CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

September 29, 2021
AGENDA ITEM #9

Discuss and consider approving a contract with Deloitte Consulting LLP for continued development of the data platform and associated transaction routing and system interfaces to support toll transaction management

Strategic Plan Relevance:	Explore and Invest in Transformative Technology and Adopt Industry Best Practices; Deliver Multi-faceted Mobility Solutions; Invest in Effort that Extends Beyond Roadways
Department:	Operations
Contact:	Tracie Brown, Director of Operations
Associated Costs:	$2,069,364
Funding Source:	183A Phase III Other Project funds
Action Requested:	Consider and act on draft resolution

Project Description/Background: Toll transaction management is a critical business process area within a tolling agency. The process begins when a vehicle travelling on a toll agency maintained and operated toll road passes through a toll gantry. Equipment at the toll gantry captures a suite of data that uniquely identifies the toll transaction. This data includes an image of the license plate used to extract the license plate number and state, vehicle axles, or class, date/time, location, and transponder device information. The resulting data set serves as inputs necessary to determine the toll amount, the individual responsible for paying the toll, and the payment path used to submit a request for payment. Additionally, toll transaction data is used for traffic and customer pattern analysis, monitoring and validation of toll system performance and accuracy, revenue and financial analysis, and other data points for the toll agency to make informed business decisions.

The Mobility Authority currently uses an outsourced solution developed by Kapsch TrafficCom to handle the end-to-end toll transaction management processes and workflow. To provide more flexibility in the future, in March 2021, the Mobility

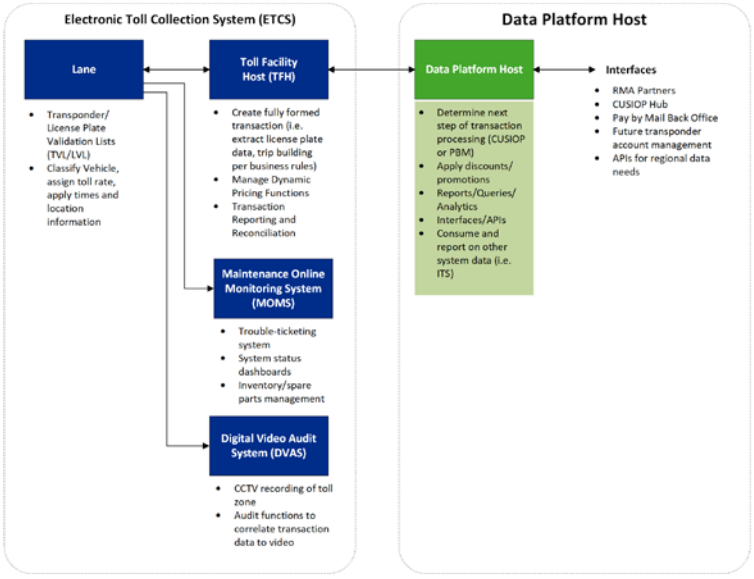
Authority awarded a contract to Deloitte Consulting LLP to begin development of the data platform to move to a stratagem wherein all toll transaction processing and data management capabilities after the point of transaction creation is advanced to a Mobility Authority-managed solution. A third-party vendor would continue to collect and create the toll transaction data set at the roadside, then pass the toll transaction data to the data platform within the Mobility Authority's network. The new approach gives the Mobility Authority more control of the data which will lead to better informed decision-making.

The Data Platform Project Explained

The objective of the data platform project is to transition all toll transaction data processing and data management capabilities after the point of transaction creation to a Mobility Authority-managed solution. A third-party vendor will continue to collect and create the toll transaction at the roadside, then pass the fully formed toll transaction to the data platform. Business logic and rules will then consume the transaction and route the payment request to either the Central United States Interoperability (CUSIOP) Hub or the Pay by Mail (PBM) vendor.

The Mobility Authority-managed data platform will also support additional business capabilities such as external reporting and internal data analytics. A connection to the Texas Department of Motor Vehicles' datasets will enable the Mobility Authority to better understand its customer base and their travel habits. Future development could include adding promotions and discount program logic.

This new configuration is depicted below.



The Data Platform Project is a component of the Mobility Authority's *Roadway Technology Plan*. The *Roadway Technology Plan* is part of a larger initiative to modernize the Mobility Authority's toll and roadway technology systems, and to thoughtfully expand the use of technology to maximize road capacity. The *Roadway Technology Plan* was first presented to the Mobility Authority's Board at its February 2020 meeting.

The Solution Approach

To achieve the new transaction processing arrangement, the Mobility Authority defined a multi-faceted strategic plan to implement an end-to-end scalable tolling transaction system to meet current and future business capabilities. This architecture design provides solutions for:

- Centralized, secure, and redundant data hosting for all data entities owned by the Mobility Authority and necessary for toll transaction processing;
- External data exchange points that provide flexible structured transaction data transmissions to and from third parties such as service providers, universities, or research institutions;
- Multi-step modular pricing and discounting business logic;
- Auditable data governance and security;
- User driven self-service data updates and business process administration; and
- Public, external, and internal reporting.

The Mobility Authority has chosen a modular approach to complete the Data Platform Project. Development for Release 1 and 2 will complete in September 2021 on schedule. The current recommendation is related to development for Release 3.

- Release 1 established the platform.
- Release 2 created the routing and exchange processes.
- Release 3 supports development for pricing and billing transactions, defines how data governance is handled in the new processing schema, and will identify the suite of reports necessary to account for the agency's revenue and monitor performance.
- Release 4 will define promotions and discount programs, and provide reporting and analytics for secure internal and external data access.

A Statement of Work (SOW) for Data Platform Release 3 was developed, in a format matching that outlined by Texas Department of Information Resources (DIR), and released to Deloitte Consulting LLP in July 2021. Deloitte responded to the SOW in August 2021. After additional discussions, Deloitte submitted an updated response in September 2021.

The total not to exceed cost for development of Releases 3 is $2,069,364. This includes a 10% project contingency as outlined below.

Release 3	$ 1,881,240
Project Contingency	$188,124
TOTAL PROJECT COST	**$ 2,069,364**

Previous Actions & Brief History of the Program/Project:

The initial contract with Deloitte was awarded by the Mobility Authority's Board of Directors in February 2021; the contract with Deloitte was approved by the Board of Directors in March 2021. Completion of the work provided by Deloitte related to Releases 1 and 2 is planned to complete on time on September 17, 2021. The purchase of additional software, hardware and hosting in support of the agreed upon scope has been estimated and partially completed.

Financing: 183A Phase III Other Project funds

Action requested/Staff Recommendation: Staff recommends contracting with Deloitte Consulting LLP for continued development of a data platform with the scope identified as Release 3 through their contract with the Texas Department of Information Resources. Pursuant to Government Code Section 2054.0565 and the Mobility Authority Policy Code, use of the DIR contract with Deloitte Consulting LLP satisfies all competitive purchasing requirements.

Backup provided: Draft Resolution
Deloitte Consulting Release 3 Response
Data Platform Release 3 Scope of Work

GENERAL MEETING OF THE BOARD OF DIRECTORS
OF THE
CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY

RESOLUTION NO. 21-0XX

APPROVING A CONTRACT WITH DELOITTE CONSULTING LLP FOR CONTINUED DEVELOPMENT OF A DATA PLATFORM AND ASSOCIATED TRANSACTION ROUTING AND SYSTEM INTERFACES TO SUPPORT TOLL TRANSACTION MANAGEMENT

WHEREAS, Mobility Authority staff is developing a data platform to transition all toll transaction data processing and data management capabilities after the point of transaction creation from a third-party vendor to the Mobility Authority (the "Data Platform Project"); and

WHEREAS, a Mobility Authority managed data platform will support new business capabilities such as external reporting, data analytics and a connection to the Texas Department of Motor Vehicles' datasets to allow better informed agency decision making; and

WHEREAS, by Resolution No. 21-018, dated March 31, 2021, the Board of Directors approved a contract with Deloitte Consulting LLP for the first phase of the Data Platform Project to establish the data platform and create the routing and exchange processes; and

WHEREAS, the Executive Director has negotiated a scope of work for the next phase of the Data Platform Project to support development for pricing and billing transactions, define how data governance is handled in the new processing schema, and identify the suite of reports necessary to account for the Mobility Authority's revenue and monitor performance which is attached hereto as Exhibit A; and

WHEREAS, Deloitte Consulting LLP has submitted pricing for the next phase of the Data Platform Project which is attached hereto as Exhibit B; and

WHEREAS, Deloitte Consulting LLP currently provides services to the State of Texas through Texas Department of Information Resources (DIR) Contract No. #DIR-TSO-431

WHEREAS, pursuant to Texas Government Code Section 2054.0565 and Mobility Authority Policy Code Section 401.008, the Mobility Authority may use the DIR contract with Deloitte Consulting LLP to implement the next phase of the Data Platform Project; and

WHEREAS, the Executive Director recommends entering into an agreement with Deloitte Consulting LLP for continued development of the Data Platform Project in a total amount not to exceed $2,069,364, including contingency, through their DIR cooperative contract.

NOW THEREFORE BE IT RESOLVED that the Board of Directors hereby approves the scope of work and pricing for the next phase of the Data Platform Project which are attached hereto as Exhibit A and Exhibit B, respectively; and

BE IT FURTHER RESOLVED, that the Executive Director is authorized to enter into an agreement with Deloitte Consulting LLP in a total amount not to exceed $2,069,364, including contingency, through their contract with the Texas Department of Information Resources for continued development of the Data Platform Project.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 29th day of September 2021.

Submitted and reviewed by:

_____

Geoffrey Petrov, General Counsel

Approved:

_____

Robert W. Jenkins, Jr.
Chairman, Board of Directors

Exhibit A

Statement of Work

Data Platform Release 3 Requirements

Technology Upgrade/Migration Transformation

July 6, 2021

List of Figures

List of Tables

List of Appendices

1. Introduction

The Central Texas Regional Mobility Authority (CTRMA) seeks Texas Department of Information Resources (TxDIR) Vendors or teams (individually or collectively, the Vendors) to provide data platform services included in Data Platform Release 3 Requirements, as more fully described in Section 3. This Statement of Work (SOW) does not include items in the Electronic Toll Collections System (ETCS).

The delineation of services is shown in Figure 1-1 below.

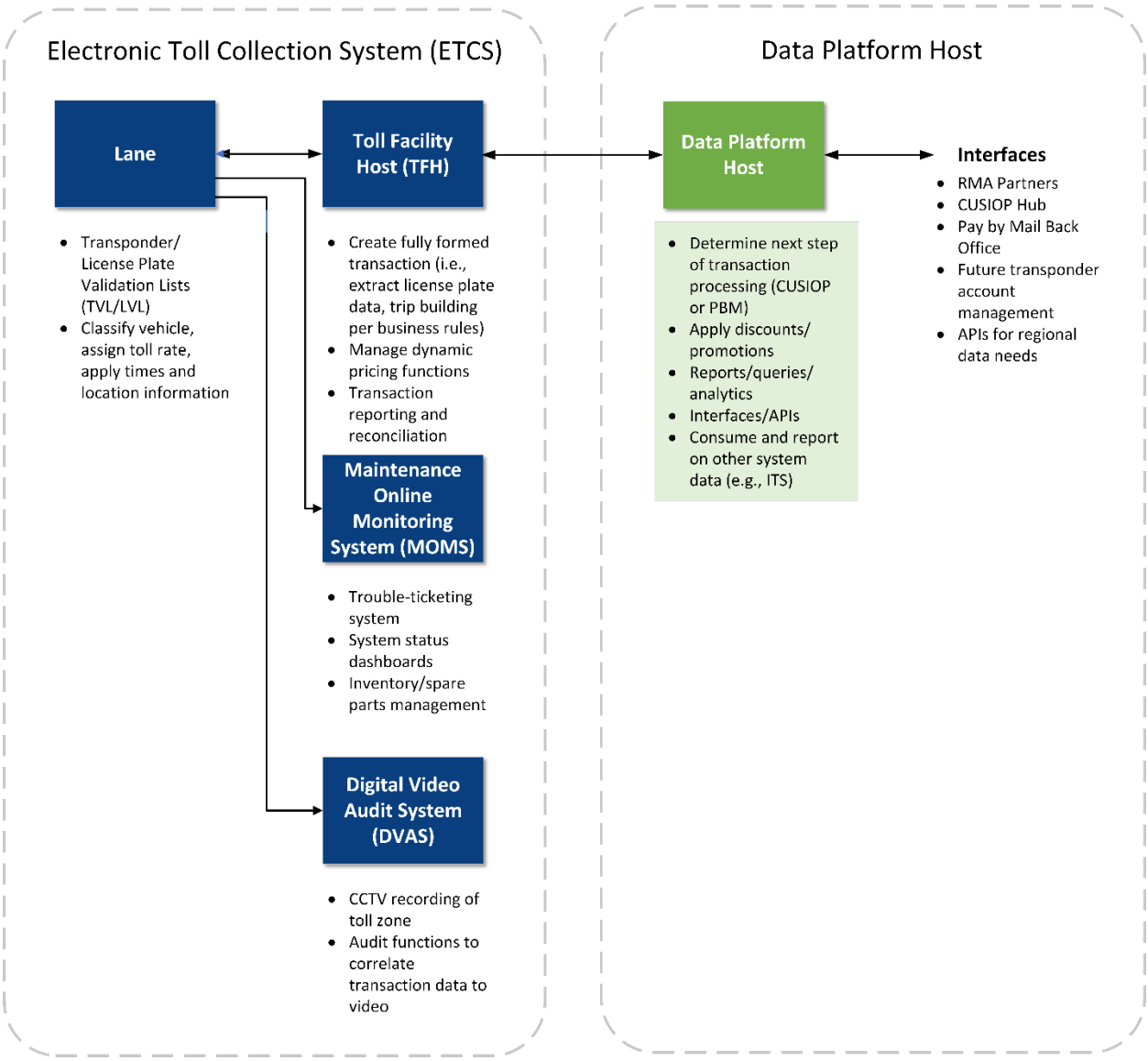


Figure 1-1: ETCS vs. Data Platform Host

2. Background

Toll transaction management is a critical business process area within a tolling agency. The process is triggered when a vehicle travelling on a toll agency maintained and operated toll road passes through a toll gantry. Equipment at the toll gantry captures a suite of data that uniquely identifies the toll transaction. This data includes an image of the license plate used to extract the license plate number and state, vehicle axles, or class, date/time, location, and Automatic Vehicle Identification (AVI) transponder device information. The resulting data set serves as inputs necessary to determine the toll amount, the individual responsible for paying the toll and the payment path used to submit a request for payment. Additionally, toll transaction data is used for traffic and customer pattern analysis, monitoring and validation of toll system performance and accuracy, revenue and financial analysis, and other data points for the toll agency to make informed business decisions.

In the current-state, CTRMA has deployed an outsourced solution to handle the end-to-end toll transaction management processes and workflow. The objective of this program is to transition all toll transaction data processing and data management capabilities after the point of toll transaction creation to a CTRMA-managed solution. A third-party vendor will continue to collect and create the toll transaction data set at the roadside, then pass the toll transaction data to a data platform within the CTRMA network. CTRMA business logic and rules will then consume the transaction data to price and route the payment request. The data platform will require additional data sets such as the Texas Department of Motor Vehicles (Texas DMV) database and the Central United States Interoperability Hub (CUSIOP Hub) data to properly route the toll transaction and complete the process. The resulting CTRMA-managed data platform will also support additional business capabilities such as external reporting and internal data analytics.

To achieve this objective, CTRMA has defined a multi-faceted strategic plan to implement an end-to-end scalable tolling transaction system to meet current and future business capabilities. Using a Service Oriented Architecture (SOA) approach, the CTRMA developed a back-office architecture design that provides solutions for:

- Centralized, secure, and redundant data hosting for all data entities necessary for toll transaction processing
- External data exchange points that provide flexible structured transaction data transmissions to and from third parties
- Multi-step modular pricing and discounting business logic
- Auditable data governance and security
- UX/UI-driven data and business process administration
- Public, external, and internal fixed reporting and cached data access

Figure 2-1: Strategic Goals

Key Features:

Data Platform

- Design and deployment of all internally managed data sources (master record)
- Send and receive data exchanges (flat file and API solutions)
- Data Governance (Use, Retention, Recovery)

Routing and Exchanges

- Automated Payor identification and transaction payment request routing

Reporting and Analytics

- Public, Internal and External tools, and files

Invoicing and Pricing

- Adjusted and Discount rate design and automation

To accomplish this objective, CTRMA has chosen to scope the releases to support a modular approach. Figure 2-2 below illustrates the linear process in scope and the planned release number for each capability area.

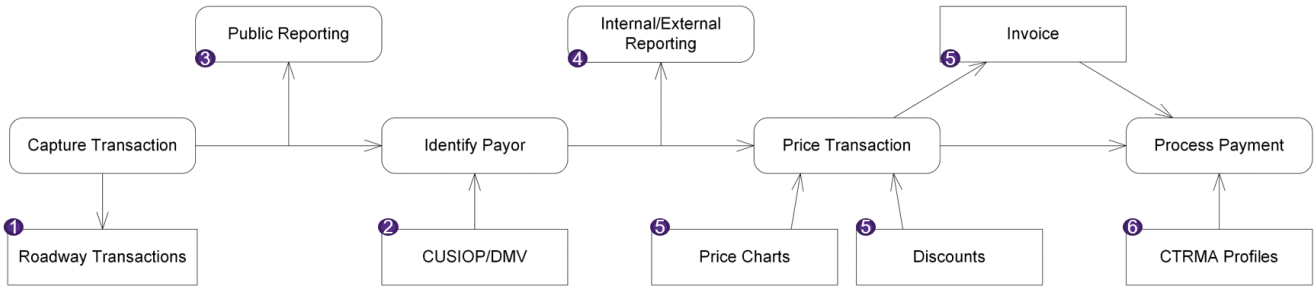


Figure 2-2: Data Platform Modular Approach

2.1. Roadmap

CTRMA has organized the program into multiple releases spanning several calendar years. The current program includes a total of four (4) releases in scope. This SOW is scoped to include Data Platform Release 3 Requirements.

Release	**Release 1 & 2 (Combined)**		**Release 3**		**Release 4**
Portfolios	**1 Establish Platform**	**2 Routing & Exchanges**	**3 Pricing & Invoicing**	**4 Data Governance**	**5 Reporting**
Work Streams	• Roadway Transaction Data • Data Transformation • Periodic SLA Review	• CUSIOP DB & TCS • Transaction Routing • Transaction Exchanges	• Product Management • Discount Program • Pricing & Invoicing	• Reporting Data Cache • Data Governance • DMV	• External Reporting • Internal Reporting • Reporting & Analytics
Projects	• Data Platform Solution • Toll Transaction Database(s) • Roadway Transaction Data • Data Transformation • Roadway Data SLA Monitoring	• CUSIOP Database(s) • Source Data Exchange & Transformation • Exemp. Vets. Habits. datasources & (UI/UX) • Transaction Routing Logic, Rules, & Price Adjustments • IOP Exchange • PBM Exchange • Current TCS Exchange • Future TCS Exchange	• Transaction Operations Management Solution (TOMS) • Product Management Strategy • Product Database(s) • Product Pricing Process • Discount Program Strategy • Discount Program Database(s) • Discount Pricing Process • Discount Program Marketing & Communication • Invoice Database(s) • Automated Invoicing Logic • Invoice Data Exchanges	• DMV DB • DMV Exchange • Reporting Cache Platform Solution • Public Reporting Data Exchanges • Public Report Generation • Public Data Reporting • Data Governance - Strategy • Data Governance Solution – Data Use • Data Governance – Availability • Data Governance - Policies & Education	• External Data Reporting Database(s) • Internal Data Reporting Database(s) • External Reporting Data Exchanges • Report Generation • Internal & External Data Exchange • Internal Reporting & Analytics Tool(s)
Key Outcomes	• Data Platform Environment • Internal Roadway Transaction Data • SLA-driven quality	• Transaction & Payment Path routing • IOP Exchange • PBM Exchange • Tolling Exchange (TCS) • Other Exchanges	• Internal pricing controls • Transaction Operations Management • Discount programs • Consistent invoicing • Transaction Processing Independence	• Fixed & Dynamic Reporting* • Data governance • SOC 2 Compliance	• Internal & external data access* • Data Governance • Public data availability

3. Data Platform Release 3 Requirements Scope

3.1. Tolling Product Management

3.1.1. Development and deployment of Product database(s) and relationships

3.1.2. Design and development of automated Product Management process(es)

3.1.1.1. Manage Tolling Product Types

3.1.1.2. Manage Tolling Products

3.1.1.3. Manage Tolling Product Items

3.1.1.4. Manage Tolling Product Pricing (Base Price, Price Window Hierarchy, and Business Rules)

3.1.3. Development of automated business process(es) for payor ID and payment path routing logic

3.1.2.1. Manage Tolling Price Adjustments

3.2. Discount Management

3.2.1. Development and deployment of Discount database(s) and relationships

3.2.2. Design and development of automated Discount Management process(es)

3.1.3.1. Manage Tolling Discount Types (Active & Passive)

3.1.3.2. Manage Tolling Discount Programs (Veterans, Student, Frequency, Members, Holiday, et al)

3.1.3.3. Manage Tolling Discounts (Discount Price, Discount Window Hierarchy, and Business Rules)

3.2.3. Integration of Discount Management with Product Management processes

3.3. Invoice Management

3.3.1. Development and deployment of Invoice database(s) and relationships

3.3.2. Design and development of automated Invoice Management process(es)

3.1.4.1. Manage Invoices

3.3.3. Integration of Invoice Management with Product and Discount Management

3.4. Data Exchange Management

3.4.1. Design, development, and testing for Pay by Mail('PBM') Invoice data exchange modifications (Fixed file, API, XML, JSON)

3.4.2. Design, development, and testing for IOP Hub Invoice data exchange modifications (Fixed file, API, XML, JSON)

3.4.3. Development of DMV Hub database(s) and relationships

3.4.4. Design, development, and testing for external DMV Hub data exchanges (Fixed file, API, XML, JSON)

3.4.5. Design, development, and testing for Public Reporting data exchange (Fixed file, API, XML, JSON, GitHub)

3.5. Reporting Cache & Reporting Management

- 3.5.1. Development of Reporting Cache data platform
- 3.5.2. Development of Public Reporting database(s) and relationships
- 3.5.3. Implementation and testing of Public Reporting data push from master data source to Reporting Cache
  - 3.5.3.1. Manage Reporting Cache
- 3.5.4. Development of automated Public Report(s) generation
  - 3.5.4.1. Manage Public Reporting
- 3.5.5. End-to-end testing of Reporting Cache and Public Reporting exchange solutions
  - 3.5.5.1. Manage Public Reporting Data Exchange(es) (API, Fixed File, GitHub)

3.6. Data Governance & SOC 2 Compliance

- 3.6.1. SOC 2 Risk Objectives, Control Objectives, and Policies
- 3.6.2. SOC 2 Compliance Processes & Procedures
- 3.6.3. Support for establishment of Data Governance strategy and approach
- 3.6.4. Definition of Data Use criteria
- 3.6.5. Automation of Data Governance process(es) including Certification and Attestation for data use
- 3.6.6. Documentation of Data Use Governance Policies & Procedures
- 3.6.7. Development of Data Governance Awareness training, compliance, and certification
- 3.6.8. Declaration and implementation of Data Governance Audit(s)

3.7. IT Enterprise Management

- 3.7.1. Policies & Procedures documentation
- 3.7.2. Revision of Source Data Entity Catalog
- 3.7.3. Data Platform IT Service Catalog(s) and Service Level definition & documentation

4. Deliverables

Deliverables must be provided on the dates specified in Section 13.3. Any changes to the delivery date must have prior approval (in writing) by the Data Platform Program Manager or designee. All deliverables must be submitted in a format approved by the Data Platform Program Manager.

If the deliverable cannot be provided within the scheduled timeframe, the Vendor is required to contact the Data Platform Program Manager in writing with a reason for the delay and the proposed revised schedule. The request for a revised schedule must include the impact on related tasks and the overall project.

A request for a revised schedule must be reviewed and approved by the Data Platform Program Manager before placed in effect. Contract Terms and Conditions may dictate remedies, costs, and other actions based on the facts related to the request for a revised schedule. CTRMA will complete a review of each submitted deliverable within fourteen (14) days from the date of receipt.

The required *Production-Ready* deliverables for Data Platform Release 3 Requirements include:

- Development and deployment of Product database(s) and relationships
- Design and development of automated Product Management process(es)
- Development of automated business process(es) for payor ID and payment path routing logic
- Development and deployment of Discount database(s) and relationships
- Design and development of automated Discount Management process(es)
- Integration of Discount Management with Product Management processes
- Development and deployment of Invoice database(s) and relationships
- Design and development of automated Invoice Management process(es)
- Integration of Invoice Management with Product and Discount Management
- Design, development, and testing for Pay by Mail('PBM') Invoice data exchange modifications (Fixed file, API, XML, JSON)
- Design, development, and testing for IOP Hub Invoice data exchange modifications (Fixed file, API, XML, JSON)
- Development of DMV Hub database(s) and relationships
- Design, development, and testing for external DMV Hub data exchanges (Fixed file, API, XML, JSON)
- Design, development, and testing for Public Reporting data exchange (Fixed file, API, XML, JSON, GitHub)
- Development of Reporting Cache data platform
- Development of Public Reporting database(s) and relationships
- Implementation and testing of Public Reporting data push from master data source to Reporting Cache
- Development of automated Public Report(s) generation
- End-to-end testing of Reporting Cache and Public Reporting exchange solutions
- SOC 2 Risk Objectives, Control Objectives, and Policies
- SOC 2 Compliance Processes & Procedures
- Support for establishment of Data Governance strategy and approach
- Definition of Data Use criteria
- Automation of Data Governance process(es) including certification and affirmation for data use
- Documentation of Data Governance Policies & Procedures
- Development of Data Governance Awareness training, compliance, and certification
- Declaration and implementation of Data Governance Audit(s)
- Policies & Procedures documentation
- Revision of Source Data Entity Catalog
- Data Platform IT Service Catalog(s) and Service Level definition & documentation

5. Project Management Requirements

Vendor personnel will ordinarily perform services under the direction of the CTRMA Data Platform Program Manager. Such interaction will normally be limited to ensuring that deliverables meet the requirements, periods of Releases, reviewing and approving of all invoices, contract compliance, and coordinating the Vendor's access to needed CTRMA resources and information.

The Vendor shall ensure that the Release is effectively and efficiently managed to the mutual benefit of the Vendor and CTRMA. Vendor shall employ as necessary the personnel, personnel hours, tools, and systems to properly manage and deliver the project.

CTRMA considers an effective project management program to be capable of identifying and addressing program issues at the earliest opportunity to minimize or eliminate Change Orders and changes to the project plan or schedule. It is

therefore incumbent upon the Vendor to have an established and fully effective project management program in place at the initiation of the contract and be implemented for each Release.

For each Release, the Vendor shall designate a Project Manager (consistent Project Management Institute – Project Management Body of Knowledge (PMI-PMBOK) practices), subject to CTRMA approval, who shall be responsive to the needs of CTRMA as required by the contract. The Project Manager shall ensure that the project tasks are completed on time and within budget. The Project Manager shall keep CTRMA fully informed of the status of the project, shall promptly, and regularly notify CTRMA of any problems or difficulties that may affect the timely or effective completion of the task, milestone, or project. The Project Manager shall have full authority to assign task priority as required to meet the requirements of the Release project.

The Project Manager shall be competent and fully qualified in all aspects of the Release project. Removal or replacement of the Project Manager(s) by the Vendor shall only be with prior approval of CTRMA.

A Project Management Plan shall be submitted as part of each Release. The plan shall include a description of the management techniques, including the overall management, staffing, and measurable controls, used to meet the Data Platform Release 3 Requirements scope. The plan shall be reviewed and modified as necessary during the execution of the contract.

The CTRMA Data Platform Program Manager will determine the intervals and form for status reports at the time a Release is negotiated and occasionally may be requested ad-hoc. Each Release status report shall consist of a brief description of the project, progress, any problems, concerns or other issues that need to be addressed, expected activities during the next reporting period, and any other information deemed appropriate and relevant by the Vendor or requested by the CTRMA Data Platform Program Manager. It is anticipated weekly status meeting with the CTRMA Data Platform Manager will be required.

6. Acceptance Criteria

For any Release assignment requiring hardware/software integration, development and/or installation, the Vendor shall develop an acceptance test plan and procedure to verify intended functionality, the completion of the deliverable milestones provided by the Vendor. Approval from CTRMA project management is required before proceeding.

Vendor shall work with CTRMA to perform the acceptance testing. Should any problems arise during the testing, the Vendor shall be responsible to make necessary corrections before CTRMA acceptance of the work. If the Vendor determines the problem is not caused by the Vendor supplied work, it shall provide CTRMA a detailed description of the problem and the reason why it is not caused by the Vendor's work. If CTRMA agrees the problem lies elsewhere, then CTRMA will provide the correction. After the correction, the acceptance test will be restarted until successful completion.

For deliverable milestones where production readiness is identified, the work product is fully developed, tested, and in the production environment. This includes any and all CTRMA policy requirements such as vulnerability scanning.

7. Period of Performance

Data Platform Services Release 3 Requirements is expected to occur during Fall 2021 to early Summer 2022.

8. Invoices

The Vendor should invoice the CTRMA after each Payment Deliverable Milestone is accepted. CTRMA will not make partial payments for deliverable milestone subtasks. Payments will be made in accordance with Appendix A of the Contract.

9. CTRMA Provided Services

If required, CTRMA will provide the following for Vendor staff working onsite:

- Desk and workspace
- Desk phone
- Security access to required physical areas
- Access to subject matter experts available during normal work hours
- Laptop or desktop computers with required network and Internet access
- CTRMA will not provide a cell phone, smart phone, tablet or other personal electronic equipment
- System access will be provided by CTRMA

10. Location of Work, Hours and Conditions

Given the dynamic health advisory climate, where possible, project work will be performed at the Vendor's resource center. Depending upon the nature of a particular deliverable, CTRMA may supply access to Vendor resources and temporary on-site workspace and/or access to facilities required for performing assigned tasks. Space will be provided for Vendors with staff working on-site. CTRMA's normal work hours on the Project are a standard 5-day workweek, excluding US National holidays.

11. Additional Terms and Conditions

CTRMA reserves the rights with respect to this SOW to:

1. Modify, withdraw, or cancel this SOW in whole or in part at any time prior to the execution of the Contract by CTRMA, without incurring any costs obligations or liabilities.
2. Issue a new SOW after withdrawal of this SOW.
3. Accept or reject any and all submittals and responses received at any time.
4. Modify dates set or projected in this SOW.
5. Terminate evaluations of responses received at any time.
6. Require confirmation of information furnished by a Vendor, require additional information from a Vendor concerning its response, and require additional evidence of qualifications to perform the work described in this SOW.
7. Seek or obtain data from any source that has the potential to improve the understanding and evaluation of the responses to this SOW.
8. Waive any weaknesses, informalities, irregularities or omissions in a response, permit corrections, and seek and receive clarifications to a response.
9. Accept other than the lowest priced response.
10. Issue addenda, supplements, and modifications to this SOW.
11. Disqualify any Vendor that changes its response without CTRMA approval.
12. Modify the SOW process (with appropriate notice to Vendors).
13. Establish a competitive range, hold discussions and/or request BAFOs.

14. Approve or disapprove changes to the Vendor teams.
15. Revise and modify, at any time before the submission deadline, the factors it will consider in evaluating Vendors, and to otherwise revise or expand its evaluation methodology. If such revisions or modifications are made, CTRMA shall circulate an addendum to all Vendors setting forth the changes to the evaluation criteria or methodology. CTRMA may extend the submission deadline if such changes are deemed by CTRMA, in its sole discretion, to be material and substantive.
16. Hold meetings, conduct discussions, and communicate with one or more of the Vendors responding to this SOW to seek an improved understanding and evaluation of the response.
17. Add or delete work to/from the scope of services.
18. Negotiate with one or more Vendors concerning its response and/or the Contract.
19. Suspend and/or terminate negotiations at any time, elect not to commence negotiations with any responding Vendor and engage in negotiations with other than the highest ranked Vendor.
20. Retain ownership of all materials submitted in hard-copy and/or electronic format.
21. Exercise any other right reserved or afforded to CTRMA under this SOW.
22. Vendor responses received become the property of CTRMA.

This SOW does not commit CTRMA to enter into a contract or proceed with the procurement described herein. CTRMA assumes no obligations, responsibilities, and liabilities, fiscal or otherwise, to reimburse all or part of the costs incurred or alleged to have been incurred by parties responding to this SOW. All such costs shall be borne solely by the Vendor. In no event shall CTRMA be bound by, or liable for, any obligations with respect to the procurement until such time (if at all) as a Contract, in form and substance satisfactory to CTRMA, has been authorized and executed by CTRMA and, then, only to the extent set forth herein. CTRMA makes no representation that the Contract will be awarded based on the requirements of this SOW. Vendors are advised that CTRMA may modify the procurement documents at any time.

11.1. Development and Testing Environments

Vendor shall be responsible for providing all development, sandbox, testing and pre-production environments during the duration of each release.

11.2. Compliance with CTRMA Information Security Guidelines

The Vendor shall become familiar with and adhere to CTRMA's Information Security policies. Consultants that have access to CTRMA IT environments will be required to sign a user acknowledgement and agree to comply with the CTRMA Information Security Policy (Appendix C).

12. Process Details

The procurement process outlined herein is in accordance with CTRMA's Policy Code and all other applicable rules and laws.

12.1. Submittal Format

All Responses must be responsive to the general format and guidelines outlined within this SOW. A responsive submittal is one that:

- Follows the general guidelines of this SOW,
- Includes all documentation requested,
- Is submitted following the general format outlined herein,
- Displays sound justification for recommendations,

- Is submitted by the deadline, and
- Has the appropriate signatures as may be required.

Failure to comply may result in the Response being deemed non-responsive.

12.2. Page Limits/Fonts

Responses must not exceed page limits listed in Section 13 (8.5 x 11 inches with 1-inch margins from all sides), type font size not less than 11 points, and printed on one side. Response shall be submitted as a bound document and printed single-sided on standard 8½" x 11" paper. Graphics, charts, photographs, and/or exhibits may be on 11" x 17" paper but must be folded to the standard size; foldout pages count as one page.

The page limit does not include the cover letter (limited to one (1) page), front/back cover sheets, dividers, table of contents, résumés (limited to two (2) pages each), the Conflict of Interest Disclosure Statement (provided as Appendix B), or other items requested to be included in an appendix. Font sizes in graphics or attachments can be less than the body of the SOW Response but should be reasonably legible.

Materials submitted exceeding the page limits specified in Section 13 will not be reviewed.

12.3. Section Headings

Vendors should follow the outline in Section 13, using section headings and subheadings. Vendors should clearly identify each request being addressed and answer each specifically and succinctly. Please provide a response to every question or request for information identified. If no response is given, clearly explain why.

12.4. Contact Information

In the cover letter, include the name, phone number, and email address of the Vendor's designated point of contact.

13. Vendor Response

CTRMA will select the Vendor(s) that offers the best value as determined by the information provided in the Vendor's Response. The following information shall be provided in the Vendor's Response:

13.1. Staff Capabilities

a. Brief history of the responding firm.
b. Personnel and team. Vendor must demonstrate key personnel and staff roles possess the skills necessary to perform services outlined in this SOW.
    i. For key personnel in leadership positions, provide the names and résumés of the consultants that Vendor is committing to this engagement.
    ii. For staff roles, provide resume(s) of representative consulting resources that would staff each role should your firm be awarded this project.
c. Corporate address.
d. Other office locations and addresses.
e. A summary of the firm's experience providing services for governmental entities for 2017, 2018, 2019, and to date.
f. This section may not exceed ten (10) pages, excluding Vendor resumes.

13.2. Relevant Experience and References

a. Provide a listing of at least three (3) relevant projects to substantiate the qualifications and experience requirements for similar services completed for three (3) years within the past five (5) years, including the following:
    i. Project name and location
    ii. Firm(s) and key staff who worked on the project
    iii. Name, address, and telephone number of client contact. [The Vendor unconditionally authorizes CTRMA to contact and confer with the indicated client contact(s) and other current or past employees of that client. Input received may be considered as part of the scoring. A reasonable effort will be made to contact all references.]
    iv. Relevant projects must be of similar size and scale. Similar size and scale is defined as demonstrated knowledge of transaction processing systems with a minimum of 50 million records and/or transactions processed annually.
b. Provide a listing of any transaction processing contracts won in the last three (3) years with scheduled go-live dates and status of each project.
c. This section may not exceed six (6) pages.

13.3. Project Work Plan

Vendor shall provide a draft high-level project work plan addressing the tasks specified in the SOW, which shall include:

a. A description of key activities and milestones.
b. Any assumptions and dependencies of the project.
c. A detailed methodology description of the Vendor's approach to analyze, assess, validate, document and complete each deliverable milestone.
d. A description of the resources necessary from CTRMA to support the process, including estimates of time needed from CTRMA's subject matter experts and high-level analysis of data gathering requirements.
e. Provide estimated due dates for each deliverable specified in Section 4.
f. All key activities, milestones and methodologies must be phrased in terms and language that can be easily understood by non-technical personnel (e.g., laypersons without subject matter expertise).
g. This section may not exceed twenty (20) pages.

13.4. Additional Considerations

a. Vendor shall indicate their agreement to comply with the Conflict of Interest Disclosure Statement (provided as Appendix B).
b. All items of this agreement shall be done in accordance with the Acceptance Criteria.
c. CTRMA will schedule an oral presentation and interview date.

13.5. Trust Services Criteria

As part of a larger SOC Compliance initiative within CTRMA, the enterprise solution for the scope within this SOW must meet the AICPA Trust Service Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy where applicable. Vendors should include in their response to this SOW an understanding of the five (5) criteria areas and any relevant client experience that included the development of policies that govern systems and data with respect to the five (5) Trust Services Criteria areas. [See Appendix D - Trust Services Criteria]

This section may not exceed five (5) pages.

13.6. Financial Ability to Implement Project

To demonstrate the Vendor possesses the adequate financial resources necessary for this project, each Vendor shall deliver to CTRMA, at the time of submission of its response, a complete set of the Vendor's then previous three (3) years of consolidated financial statements, including, without limitation, balance sheet and income statements, and notes related thereto. Financial statements should demonstrate positive cash flow from operating activities for the then previous three (3) years. If an audited financial statement for the prior year is not available, an unaudited financial statement may be provided.

Financial statements may be retrieved following the announcement of contract award. Financial statements submitted that have not been retrieved within five business (5) days of the announcement of contract award will be destroyed.

By submitting a response, each Vendor, if awarded the SOW, agrees to deliver to CTRMA, current and updated financial statements, certified as true, complete, and accurate by the Vendor's Chief Financial Officer, reasonably requested by CTRMA from time to time.

Financial statements must be included separately and be clearly marked. This information does not count toward any page limit.

14. Pricing

The main purpose of this section is to detail the pricing for the deliverables-based services. Vendor should also provide a summary of any assumptions and exclusions. The Vendor must provide a separate price for each Milestone Deliverable in this SOW based on expected hours and hourly rates by position as approved in the Vendor's current TxDIR contract. An example representation of this price breakdown can be found in Appendix E.

15. Schedule of Events and Response Guidelines

The following dates represent the CTRMA's desired schedule of events associated with this SOW inquiry. CTRMA reserves the right to modify these dates at any time, with appropriate notice to prospective Vendors.

Table 15-1: Planned Schedule of Events

SOW Issue Date	**July 6, 2021**
Deadline for Intent to Respond	July 13, 2021
Deadline for SOW Questions submitted to CTRMA	July 19, 2021
Responses by CTRMA to SOW Questions received by deadline	July 26, 2021
Deadline for Submitting Responses to this SOW	**August 4, 2021**
Presentation and Interview Dates	August 10, 2021
Anticipated Selection Date – CTRMA Board Approval	September 22, 2021
Anticipated Selected Team Notice to Proceed Date	**October 2021**

15.1. Questions and Answers

An emailed confirmation of the Vendor's intent to respond to this SOW is required by July 13, 2021.

All questions regarding the SOW must be submitted in writing. Informal verbal inquiries are not allowed. Written questions concerning this SOW must be submitted via DataPlatform@CTRMA.org.

The deadline for receipt of questions is **July 19, 2021 4:00 p.m. C.S.T.** Absent any change to deadlines evidenced through a subsequently issued addenda to this SOW, no questions will be accepted after this deadline.

CTRMA anticipates that it will post responses to questions received before the deadline on **July 26, 2021.** Responses will be emailed to all potential Vendors.

CTRMA reserves the right to contact the person submitting a question to clarify the question received, if necessary. CTRMA further reserves the right to modify, summarize or otherwise alter the content of a question to protect the identity of the requestor and to provide responses that CTRMA believes will best inform interested parties of potentially relevant information. CTRMA further reserves the right to decline to answer questions.

Each clarification, supplement, or addenda to this SOW, if any, will be emailed to all Vendors.

16. Response Submission Requirements

Responses must be received in the offices of CTRMA by or before **August 4, 2021 4:00 p.m. C.S.T.**, to be eligible for consideration. Responses must meet the format requirements set forth in Section 13, and the following submittal requirements:

Table 16-1: SOW Response Submittal Requirements

Number of Hard Copies	Two (2) bound copies of the SOW Response. One (1) of the two (2) copies of the Responses must be marked "original" and bear all the original signatures.
Number of Electronic Copies	One (1) electronic copy of the SOW Response emailed to DataPlatform@CTRMA.org. The file must be labeled as follows: DP2021-SOW_Firm Name.pdf Example: "DP2021-SOW _DP-R3 *Firm*.pdf"
Mailing Address	Central Texas Regional Mobility Authority 3300 N IH-35, Suite 300 Austin, TX 78705
Attention	Labelled, "Attention: Greg Mack"
Package Label	Data Platform Services <Firm Name> <Date>

In the event of a discrepancy/conflict between a hard copy and electronic version, the hardcopy version will govern. SOW Responses may be hand delivered to the address noted above.

Responses must be provided in a sealed envelope or package with the package label and the firm's name and address clearly visible on the outside of the envelope or package. *Responses received after the deadline will not be considered*.

The responsibility for submitting an SOW Response to CTRMA on or before the stated time and date will be solely and strictly the responsibility of the Vendor. CTRMA will in no way be responsible for delays caused by the United States mail delivery, common carrier, or by any other occurrence.

CTRMA reserves the right to request additional information or clarifications from any Vendors or to allow corrections of errors or omissions.

If the size of the SOW Response exceeds either CTRMA's 20MB email limit or Vendor email limits, the Vendor must provide a location, e.g. an FTP site, where the SOW Response may be accessed by CTRMA.

APPENDIX A

Table of Acronyms

AICPA	American Institute of CPAs
API	Application Programming Interface
AVI	Automatic Vehicle Identification
CTRMA	Central Texas Regional Mobility Authority
CUSIOP	Central United States Interoperability Hub
DMV	Texas Department of Motor Vehicles
ERD	Entity Relationship Diagram
ETCS	Electronic Toll Collection System
ICD	Interface Control Document
IOP	Interoperability
JSON	JavaScript Object Notion
PMI-PMBOK	Project Management Institute – Project Management Body of Knowledge
SOA	Service Oriented Architecture
SOC	Service Organization Control
SOW	Statement of Work
SQL	Structured Query Language
TSP	Trust Services Protocol
TxDIR	Texas Department of Information Resources
UI	User Interface
UX	User Experience
XML	eXtensible Markup Language

Appendix B

Conflict of Interest Disclosure Statement

This Disclosure Statement outlines potential conflicts of interest as a result of a previous or current business relationship between the undersigned individual (and/or the firm for which the individual works) and an individual or firm submitting a Proposal or otherwise under consideration for a contract associated with _____. Section I of this Disclosure Statement Form describes the potential conflicts of interest. Section II of this Disclosure Statement Form describes the proposer's management plan for dealing with the potential conflicts of interest as described in Section I of this form. This Disclosure Statement is being submitted in compliance with the Central Texas Regional Mobility Authority's Conflict of Interest Policy for Consultants. The undersigned acknowledges that approval of the proposed management plan is within the sole discretion of the Central Texas Regional Mobility Authority.

SECTION I. Description of Potential Conflicts of Interest.

_____
_____
_____
_____
_____

SECTION II. Management Plan for Dealing with Potential Conflicts of Interest.

_____
_____
_____
_____
_____

SIGNED: _____ DATE: _____

NAME AND TITLE: _____

REPRESENTING: _____

APPROVED BY THE CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY:

SIGNED: _____ DATE: _____

NAME AND TITLE: _____

Appendix C

CTRMA Information Security Policy

Acceptable Encryption Policy

1. Overview

See Purpose.

2. Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

3. Scope

This policy applies to all CTRMA employees and affiliates.

4. Policy

4.1 Algorithm Requirements

4.1.1 Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalog, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

4.1.2 Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

4.1.3 Signature Algorithms

Algorithm	Key Length (min)	Additional Comment
ECDSA	P-256	Cisco Legal recommends RFC6090 compliance to avoid patent infringement.
RSA	2048	Must use a secure padding scheme. PKCS#7 padding scheme is recommended. Message hashing required.
LDWM	SHA256	Refer to LDWM Hash-based Signatures Draft

4.2 Hash Function Requirements

In general, CTRMA adheres to the NIST Policy on Hash Functions.

4.3 Key Agreement and Authentication

4.3.1 Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

4.3.2 End points must be authenticated prior to the exchange or derivation of session keys.

4.3.3 Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

4.3.4 All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

4.3.5 All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

4.4 Key Generation

4.4.1 Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

4.4.2 Key generation must be seeded from an industry standard random number generator (RNG). For examples, see NIST Annex C: Approved Random Number Generators for FIPS PUB 140-2.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

National Institute of Standards and Technology (NIST) publication FIPS 140-2,

NIST Policy on Hash Functions

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Proprietary Encryption

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Acceptable Use Policy

6. Overview

Infosec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to CTRMA's established culture of openness, trust and integrity. Infosec is committed to protecting CTRMA's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of CTRMA. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every CTRMA employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

7. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at CTRMA. These rules are in place to protect the employee and CTRMA. Inappropriate use exposes CTRMA to risks including virus attacks, compromise of network systems and services, and legal issues.

8. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct CTRMA business or interact with internal networks and business systems, whether owned or leased by CTRMA, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at CTRMA and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with CTRMA policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at CTRMA, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by CTRMA.

9. Policy

a. General Use and Ownership

i. CTRMA proprietary information stored on electronic and computing devices whether owned or leased by CTRMA, the employee or a third party, remains the sole property of CTRMA. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

ii. You have a responsibility to promptly report the theft, loss or unauthorized disclosure of CTRMA proprietary information.

iii. You may access, use or share CTRMA proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

iv. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

v. For security and network maintenance purposes, authorized individuals within CTRMA may monitor equipment, systems and network traffic at any time, per Infosec's *Audit Policy*.

vi. CTRMA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

b. Security and Proprietary Information

i. All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.

ii. System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

iii. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

iv. Postings by employees from a CTRMA email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CTRMA, unless posting is in the course of business duties.

v. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

c. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of CTRMA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CTRMA-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

i. System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CTRMA.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CTRMA or the end user does not have an active license is strictly prohibited.

3. Accessing data, a server or an account for any purpose other than conducting CTRMA business, even if you have authorized access, is prohibited.

4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

7. Using a CTRMA computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

8. Making fraudulent offers of products, items, or services originating from any CTRMA account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.

12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

13. Circumventing user authentication or security of any host, network or account.

14. Introducing honeypots, honeynets, or similar technology on the CTRMA network.

15. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

17. Providing information about, or lists of, CTRMA employees to parties outside CTRMA.

ii. Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the company. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within CTRMA's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CTRMA or connected via CTRMA's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

iii. Blogging and Social Media

1. Blogging by employees, whether using CTRMA's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of CTRMA's systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate CTRMA's policy, is not detrimental to CTRMA's best interests, and does not interfere with an employee's regular work duties. Blogging from CTRMA's systems is also subject to monitoring.

2. CTRMA's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>'s Confidential Information policy when engaged in blogging.

3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of CTRMA and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by CTRMA's *Non-Discrimination and Anti-Harassment* policy.

4. Employees may also not attribute personal statements, opinions or beliefs to CTRMA when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of CTRMA. Employees assume any and all risk associated with blogging.

5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, CTRMA's trademarks, logos and any other CTRMA intellectual property may also not be used in connection with any blogging activity

10. Policy Compliance

a. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

b. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

c. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

11. Related Standards, Policies and Processes

- Data Classification Policy
- Data Protection Standard
- Social Media Policy
- Minimum Access Policy
- Password Policy

12. Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Blogging
- Honeypot
- Honeynet
- Proprietary Information
- Spam

13. Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format

Clean Desk Policy

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated June 2014*

14. Overview

A clean desk policy can be an import tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. Such a policy can also increase employee's awareness about protecting sensitive information.

15. Purpose

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property, our customers and our vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

16. Scope

This policy applies to all CTRMA employees and affiliates.

17. Policy

4.1 Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.

4.2 Computer workstations must be locked when workspace is unoccupied.

4.3 Computer workstations must be shut completely down at the end of the work day.

4.4 Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.

4.5 File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

4.6 Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.

4.7 Laptops must be either locked with a locking cable or locked away in a drawer.

4.8 Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.

4.9 Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

4.10 Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.

4.11 Whiteboards containing Restricted and/or Sensitive information should be erased.

4.12 Lock away portable computing devices such as laptops and tablets.

4.13Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up. **Things to Consider:** *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

4.14

18. Policy Compliance

8.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

8.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

8.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9 Related Standards, Policies and Processes

None.

10 Definitions and Terms

None.

11 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

<ORGANIZATION NAME> Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how <ORGANIZATION NAME>'s established culture of openness, trust and integrity should respond to such activity. <ORGANIZATION NAME> Information Security is committed to protecting <ORGANIZATION NAME>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.1 Background

This policy mandates that any individual who suspects that a theft, breach or exposure of <ORGANIZATION NAME> Protected data or <ORGANIZATION NAME> Sensitive data has occurred must immediately provide a description of what occurred via e-mail to Helpdesk@<ORGANIZATION NAME>.org, by calling 555-1212, or through the use of the help desk reporting web page at http://<ORGANIZATION NAME>. This e-mail address, phone number, and web page are monitored by the <ORGANIZATION NAME>'s Information Security Administrator. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

2.0 Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information

(PHI) of <ORGANIZATION NAME> members. Any agreements with vendors will contain language similar that protects the fund.

3.0 Policy Confirmed theft, data breach or exposure of <ORGANIZATION NAME> Protected data or <ORGANIZATION NAME> Sensitive data

As soon as a theft, data breach or exposure containing <ORGANIZATION NAME> Protected data or <ORGANIZATION NAME> Sensitive data is identified, the process of removing all access to that resource will begin.

The Executive Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Infrastructure
- IT Applications
- Finance (if applicable)
- Legal
- Communications
- Member Services (if Member data is affected)
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Executive Director

Confirmed theft, breach or exposure of <ORGANIZATION NAME> data

The Executive Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

As provided by <ORGANIZATION NAME> cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a communication plan.

Work with <ORGANIZATION NAME> communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

3.2 Ownership and Responsibilities

Roles & Responsibilities:

- Sponsors - Sponsors are those members of the <ORGANIZATION NAME> community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any <ORGANIZATION NAME> Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Information Security Administrator is that member of the <ORGANIZATION NAME> community, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the <ORGANIZATION NAME> community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

4.0 Enforcement

Any < ORGANIZATION NAME > personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

5.0 Definitions

Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;

Plain text – Unencrypted data.

Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

Protected Health Information (PHI) - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered

Protected data - See PII and PHI

Information Resource - The data and information assets of an organization, department or unit.

Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

Sensitive data - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

6.0 Revision History

Version	Date of Revision	Author	Description of Changes
1.0	August 17, 2016	SANS Institute	Initial version

1.0			

Digital Signature Acceptance Policy

19. Overview

See Purpose.

20. Purpose

The purpose of this policy is to provide guidance on when digital signatures are considered accepted means of validating the identity of a signer in CTRMA electronic documents and correspondence, and thus a substitute for traditional "wet" signatures, within the organization. Because communication has become primarily electronic, the goal is to reduce confusion about when a digital signature is trusted.

21. Scope

This policy applies to all CTRMA employees and affiliates.

This policy applies to all CTRMA employees, contractors, and other agents conducting CTRMA business with a CTRMA-provided digital key pair. This policy applies only to intra-organization digitally signed documents and correspondence and not to electronic materials sent to or received from non-CTRMA affiliated persons or organizations.

22. Policy

A digital signature is an acceptable substitute for a wet signature on any intra-organization document or correspondence, with the exception of those noted on the site of the Chief Financial Officer (CFO) on the organization's intranet: <CFO's Office URL>

The CFO's office will maintain an organization-wide list of the types of documents and correspondence that are not covered by this policy.

Digital signatures must apply to individuals only. Digital signatures for roles, positions, or titles (e.g. the CFO) are not considered valid.

4.1 Responsibilities

Digital signature acceptance requires specific action on both the part of the employee signing the document or correspondence (hereafter the *signer*), and the employee receiving/reading the document or correspondence (hereafter the *recipient*).

4.2 Signer Responsibilities

4.2.1 Signers must obtain a signing key pair from <Company Name identity management group>. This key pair will be generated using CTRMA's Public Key Infrastructure

(PKI) and the public key will be signed by the CTRMA's Certificate Authority (CA), <CA Name>.

4.2.2 Signers must sign documents and correspondence using software approved by CTRMA IT organization.

4.2.3 Signers must protect their private key and keep it secret.

4.2.4 If a signer believes that the signer's private key was stolen or otherwise compromised, the signer must contact CTRMA Identity Management Group immediately to have the signer's digital key pair revoked.

4.3 Recipient Responsibilities

4.3.1 Recipients must read documents and correspondence using software approved by CTRMA IT department.

4.3.2 Recipients must verify that the signer's public key was signed by the CTRMA's Certificate Authority (CA), <CA Name>, by viewing the details about the signed key using the software they are using to read the document or correspondence.

4.3.3 If the signer's digital signature does not appear valid, the recipient must not trust the source of the document or correspondence.

4.3.4 If a recipient believes that a digital signature has been abused, the recipient must report the recipient's concern to CTRMA Identity Management Group.

23. Policy Compliance

11.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

11.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

11.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

12 Related Standards, Policies and Processes

None.

13 References

Note that these references were used only as guidance in the creation of this policy template. We highly recommend that you consult with your organization's legal counsel, since there may be federal, state, or local regulations to which you must comply. Any other PKI-related policies your organization has may also be cited here.

American Bar Association (ABA) Digital Signature Guidelines
http://www.abanet.org/scitech/ec/isc/dsgfree.html

Minnesota State Agency Digital Signature Implementation and Use
http://mn.gov/oet/policies-and-standards/business/policy-pages/standard_digital_signature.jsp

Minnesota Electronic Authentication Act
https://www.revisor.leg.state.mn.us/statutes/?id=325K&view=chapter_-stat.325K.001

City of Albuquerque E-Mail Encryption / Digital Signature Policy
http://mesa.cabq.gov/policy.nsf/WebApprovedX/4D4D4667D0A7953A87256E7B004F6720?OpenDocument

West Virginia Code §39A-3-2: Acceptance of electronic signature by governmental entities in satisfaction of signature requirement. http://law.justia.com/westvirginia/codes/39a/wvc39a-3-2.html

14 Definitions and Terms

None.

15 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Disaster Recovery Plan Policy

24. Overview

Since disasters happen so rarely, management often ignores the disaster recovery planning process. It is important to realize that having a contingency plan in the event of a disaster gives CTRMA a competitive advantage. This policy requires management to financially support and diligently attend to disaster contingency planning efforts. Disasters are not limited to adverse weather conditions. Any event that could likely cause an extended delay of service should be considered. The Disaster Recovery Plan is often part of the Business Continuity Plan.

25. Purpose

This policy defines the requirement for a baseline disaster recovery plan to be developed and implemented by CTRMA that will describe the process to recover IT Systems, Applications and Data from any type of disaster that causes a major outage.

26. Scope

This policy is directed to the IT Management Staff who is accountable to ensure the plan is developed, tested and kept up-to-date. This policy is solely to state the requirement to have a disaster recovery plan, it does not provide requirement around what goes into the plan or sub-plans.

27. Policy

4.1 Contingency Plans

The following contingency plans must be created:

- Computer Emergency Response Plan: Who is to be contacted, when, and how? What immediate actions must be taken in the event of certain occurrences?
- Succession Plan: Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data Study: Detail the data stored on the systems, its criticality, and its confidentiality.
- Criticality of Service List: List all the services provided and their order of importance.
- It also explains the order of recovery in both short-term and long-term timeframes.
- Data Backup and Restoration Plan: Detail which data is backed up, the media to which it is saved, where that media is stored, and how often the backup is done. It should also describe how that data could be recovered.
- Equipment Replacement Plan: Describe what equipment is required to begin to provide services, list the order in which it is necessary, and note where to purchase the equipment.
- Mass Media Management: Who is in charge of giving information to the mass media?
- Also provide some guidelines on what data is appropriate to be provided.

After creating the plans, it is important to practice them to the extent possible. Management should set aside time to test implementation of the disaster recovery plan. Table top exercises should be conducted annually. During these tests, issues that may cause the plan to fail can be discovered and corrected in an environment that has few consequences.

The plan, at a minimum, should be reviewed an updated on an annual basis.

28. Policy Compliance

15.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

15.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

15.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

16 Related Standards, Policies and Processes

None.

17 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Disaster

18 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Email Policy

29. Overview

Electronic email is pervasively used in almost all industry verticals and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.

30. Purpose

The purpose of this email policy is to ensure the proper use of CTRMA email system and make users aware of what CTRMA deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within CTRMA Network.

31. Scope

This policy covers appropriate use of any email sent from a CTRMA email address and applies to all employees, vendors, and agents operating on behalf of CTRMA.

32. Policy

4.1 All use of email must be consistent with CTRMA policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

4.2 CTRMA email account should be used primarily for CTRMA business-related purposes; personal communication is permitted on a limited basis, but non-CTRMA related commercial uses are prohibited.

4.3 All CTRMA data contained within an email message or an attachment must be secured according to the *Data Protection Standard*.

4.4 Email should be retained only if it qualifies as a CTRMA business record. Email is a CTRMA business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.

4.5 Email that is identified as a CTRMA business record shall be retained according to CTRMA Record Retention Schedule.

4.6 The CTRMA email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any CTRMA employee should report the matter to their supervisor immediately.

4.7 Users are prohibited from automatically forwarding CTRMA email to a third party email system (noted in 4.8 below). Individual messages which are forwarded by the user must not contain CTRMA confidential or above information.

4.8 Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct CTRMA business, to create or memorialize any binding transactions, or to store or retain email on behalf of CTRMA. Such communications and transactions should be conducted through proper channels using CTRMA-approved documentation.

4.9 Using a reasonable amount of CTRMA resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a CTRMA email account is prohibited.

4.10 CTRMA employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.

4.11 CTRMA may monitor messages without prior notice. CTRMA is not obliged to monitor email messages.

33. Policy Compliance

18.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

18.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

18.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

19 Related Standards, Policies and Processes

- Data Protection Standard

20 Definitions and Terms

None.

21 Revision History

Date of Change	Responsible	Summary of Change
Dec 2013	SANS Policy Team	Updated and converted to new format.

End User Encryption Key Protection Policy

34. Overview

Encryption Key Management, if not done properly, can lead to compromise and disclosure of private keys use to secure sensitive data and hence, compromise of the data. While users may understand it's important to encryption certain documents and electronic communications, they may not be familiar with minimum standards for protection encryption keys.

35. Purpose

This policy outlines the requirements for protecting encryption keys that are under the control of end users. These requirements are designed to prevent unauthorized disclosure and subsequent fraudulent use. The protection methods outlined will include operational and technical controls, such as key backup procedures, encryption under a separate key and use of tamper-resistant hardware.

36. Scope

This policy applies to any encryption keys listed below and to the person responsible for any encryption key listed below. The encryption keys covered by this policy are:

- encryption keys issued by CTRMA
- encryption keys used for CTRMA business

- encryption keys used to protect data owned by CTRMA

The public keys contained in digital certificates are specifically exempted from this policy.

37.Policy

All encryption keys covered by this policy must be protected to prevent their unauthorized disclosure and subsequent fraudulent use.

4.1 Secret Key Encryption Keys

Keys used for secret key encryption, also called symmetric cryptography, must be protected as they are distributed to all parties that will use them. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest key length for that algorithm authorized in CTRMA's *Acceptable Encryption Policy.* If the keys are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different key that is the longest key length authorized and the each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key.

Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.

4.2 Public Key Encryption Keys

Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to the end user to whom the corresponding digital certificate is issued.

4.2.1 CTRMA's Public Key Infrastructure (PKI) Keys

The public-private key pairs used by the CTRMA's public key infrastructure (PKI) are generated on the tamper-resistant smart card issued to an individual end user. The private key associated with an end user's identity certificate, which are only used for digital signatures, will never leave the smart card. This prevents the Infosec Team from escrowing any private keys associated with identity certificates. The private key associated with any encryption certificates, which are used to encrypt email and other documents, must be escrowed in compliance with
CTRMA policies.

Access to the private keys stored on a CTRMAissued smart card will be protected by a personal identification number (PIN) known only to the individual to whom the smart card is issued. The smart card software will be configured to require entering the PIN prior to any private key contained on the smart card being accessed.

4.2.2 Other Public Key Encryption Keys

Other types of keys may be generated in software on the end user's computer and can be stored as files on the hard drive or on a hardware token. If the public-private key pair is generated on smartcard, the

requirements for protecting the private keys are the same as those for private keys associated with <Company Name's> PKI. If the keys are generated in software, the end user is required to create at least one backup of these keys and store any backup copies securely. The user is also required to create an escrow copy of any private keys used for encrypting data and deliver the escrow copy to the local Information Security representative for secure storage.

The Infosec Team shall not escrow any private keys associated with identity certificates. All backups, including escrow copies, shall be protected with a password or passphrase that is compliant with CTRMA *Password Policy*. Infosec representatives will store and protect the escrowed keys as described in the CTRMA *Certificate Practice Statement Policy.*

4.2.2.1 Commercial or Outside Organization Public Key Infrastructure (PKI) Keys

In working with business partners, the relationship may require the end users to use public-private key pairs that are generated in software on the end user's computer. In these cases, the public-private key pairs are stored in files on the hard drive of the end user. The private keys are only protected by the strength of the password or passphrase chosen by the end user. For example, when an end user requests a digital certificate from a commercial PKI, such as VeriSign or Thawte, the end user's web browser will generate the key pair and submit the public key as part of the certificate request to the CA. The private key remains in the browser's certificate store where the only protection is the password on the browser's certificate store. A web browser storing private keys will be configured to require the user to enter the certificate store password anytime a private key is accessed.

4.2.2.2 PGP Key Pairs

If the business partner requires the use of PGP, the public-private key pairs can be stored in the user's key ring files on the computer hard drive or on a hardware token, for example, a USB drive or a smart card. Since the protection of the private keys is the passphrase on the secret keying, it is preferable that the public-private keys are stored on a hardware token. PGP will be configured to require entering the passphrase for every use of the private keys in the secret key ring.

4.3 Hardware Token Storage

Hardware tokens storing encryption keys will be treated as sensitive company equipment, as described in CTRMA's *Physical Security policy*, when outside company offices. In addition, all hardware tokens, smartcards, USB tokens, etc., will not be stored or left connected to any end user's computer when not in use. For end users traveling with hardware tokens, they will not be stored or carried in the same container or bag as any computer.

4.4 Personal Identification Numbers (PINs), Passwords and Passphrases

All PINs, passwords or passphrases used to protect encryption keys must meet complexity and length requirements described in CTRMA's *Password Policy.*

4.5 Loss and Theft

The loss, theft, or potential unauthorized disclosure of any encryption key covered by this policy must be reported immediately to The Infosec Team. Infosec personnel will direct the end user in any actions that will be required regarding revocation of certificates or public-private key pairs.

38. Policy Compliance

21.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

21.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

21.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

22 Related Standards, Policies and Processes

- Acceptable Encryption Policy
- Certificate Practice Statement Policy
- Password Policy
- Physical Security policy

23 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Certificate authority (CA)
- Digital certificate
- Digital signature
- Key escrow
- Plaintext
- Public key cryptography

Ethics Policy

Things to Consider: *Please consult the Things to Consider FAQ for additional guidelines and suggestions for personalizing the SANS policies for your organization.*

Last Update Status: *Updated June 2014*

39. Overview

CTRMA is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When CTRMA addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

CTRMA will not tolerate any wrongdoing or impropriety at any time. CTRMA will take the appropriate measures act quickly in correcting the issue if the ethical code is broken.

40. Purpose

The purpose of this policy is to establish a culture of openness, trust and to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct. Effective ethics is a team effort involving the participation and support of every CTRMA employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

41. Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at CTRMA, including all personnel affiliated with third parties.

42. Policy

4.1 Executive Commitment to Ethics

- 4.1.1 Senior leaders and executives within CTRMA must set a prime example. In any business practice, honesty and integrity must be top priority for executives.

- 4.1.2 Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.

- 4.1.3 Executives must disclose any conflict of interests regard their position within CTRMA.

4.2 Employee Commitment to Ethics

- 4.2.1 CTRMA employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

- 4.2.2 Every employee needs to apply effort and intelligence in maintaining ethics value.

- 4.2.3 Employees must disclose any conflict of interests regard their position within CTRMA.

- 4.2.4 Employees will help CTRMA to increase customer and vendor satisfaction by providing quality product s and timely response to inquiries.

- 4.2.5 Employees should consider the following questions to themselves when any behavior is questionable:

- Is the behavior legal?
- Does the behavior comply with all appropriate CTRMA policies?
- Does the behavior reflect CTRMA values and culture?
- Could the behavior adversely affect company stakeholders?
- Would you feel personally concerned if the behavior appeared in a news headline?
- Could the behavior adversely affect CTRMA if all employees did it?

4.3 Company Awareness

4.3.1 Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

4.3.2 CTRMA will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.4 Maintaining Ethical Practices

4.4.1 CTRMA will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.

4.4.2 Employees at CTRMA should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

4.4.3 CTRMA has established a best practice disclosure committee to make sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

4.4.4 Employees are required to recertify their compliance to Ethics Policy on an annual basis.

4.5 Unethical Behavior

4.5.1 CTRMA will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

4.5.2 CTRMA will not tolerate harassment or discrimination.

4.5.3 Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.

4.5.4 CTRMA will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

4.5.5 CTRMA employees will not use corporate assets or business relationships for personal use or gain.

43. Policy Compliance

23.1 Compliance Measurement

The <Employee Resource Team> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback.

23.2 Exceptions

None.

23.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

24 Related Standards, Policies and Processes

None.

25 Definitions and Terms

None.

26 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Pandemic Response Planning Policy

44. Overview

This policy is intended for companies that do not meet the definition of critical infrastructure as defined by the federal government. This type of organization may be requested by public health officials to close their offices to non-essential personnel or completely during a worst-case scenario pandemic to limit the spread of the disease. Many companies would run out of cash and be forced to go out of business after several weeks of everyone not working. Therefore, developing a response plan in advance that addresses who can work remotely, how they will work and identifies what other issues may be faced will help the organization survive at a time when most people will be concerned about themselves and their families.

Disasters typically happen in one geographic area. A hurricane or earthquake can cause massive damage in one area, yet the worst damage is usually contained within a few hundred miles. A global pandemic,

such as the 1918 influenza outbreak which infected 1/3 of the world's population, cannot be dealt with by failing over to a backup data center. Therefore, additional planning steps for IT architecture, situational awareness, employee training and other preparations are required.

45. Purpose

This document directs planning, preparation and exercises for pandemic disease outbreak over and above the normal business continuity and disaster recovery planning process. The objective is to address the reality that pandemic events can create personnel and technology issues outside the scope of the traditional DR/BCP planning process as potentially 25% or more of the workforce may be unable to come to work for health or personal reasons.

46. Scope

The planning process will include personnel involved in the business continuity and disaster recovery process, enterprise architects and senior management of CTRMA. During the implementation of the plan, all employees and contractors will need to undergo training before and during a pandemic disease outbreak.

47. Policy

CTRMA will authorize, develop and maintain a Pandemic Response Plan addressing the following areas:

4.1 The Pandemic Response Plan leadership will be identified as a small team which will oversee the creation and updates of the plan. The leadership will also be responsible for developing internal expertise on the transmission of diseases and other areas such as second wave phenomenon to guide planning and response efforts. However, as with any other critical position, the leadership must have trained alternates that can execute the plan should the leadership become unavailable due to illness.

4.2 The creation of a communications plan before and during an outbreak that accounts for congested telecommunications services.

4.3 An alert system based on monitoring of World Health Organization (WHO) and other local sources of information on the risk of a pandemic disease outbreak.

4.4 A predefined set of emergency polices that will preempt normal CTRMA policies for the duration of a declared pandemic. These polices are to be organized into different levels of response that match the level of business disruption expected from a possible pandemic disease outbreak within the community. These policies should address all tasks critical to the continuation of the company including:

a) How people will be paid
b) Where they will work – including staying home with or bringing kids to work.
c) How they will accomplish their tasks if they cannot get to the office

4.5 A set of indicators to management that will aid them in selecting an appropriate level of response bringing into effect the related policies discussed in section 4.4—for the organization. There should be a graduated level of response related to the WHO pandemic alert level or other local indicators of a disease outbreak.

4.6 An employee training process covering personal protection including:

a) Identifying symptoms of exposure
b) The concept of disease clusters in day cares, schools or other gathering places

c) Basic prevention - limiting contact closer than 6 feet, cover your cough, hand washing
d) When to stay home
e) Avoiding travel to areas with high infection rates

4.7 A process for the identification of employees with first responders or medical personnel in their household. These people, along with single parents, have a higher likelihood of unavailability due to illness or child care issues.

4.8 A process to identify key personnel for each critical business function and transition their duties to others in the event they become ill.

4.9 A list of supplies to be kept on hand or pre-contracted for supply, such as face masks, hand sanitizer, fuel, food and water.

4.10 IT related issues:

a) Ensure enterprise architects are including pandemic contingency in planning
b) Verification of the ability for significantly increased telecommuting including bandwidth, VPN concentrator capacity/licensing, ability to offer voice over IP and laptop/remote desktop availability
c) Increased use of virtual meeting tools – video conference and desktop sharing
d) Identify what tasks cannot be done remotely
e) Plan for how customers will interact with the organization in different ways

4.11 The creation of exercises to test the plan.

4.12 The process and frequency of plan updates at least annually.

4.13 Guidance for auditors indicating that any review of the business continuity plan or enterprise architecture should assess whether they appropriately address the CTRMA Pandemic Response Plan.

48. Policy Compliance

26.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

26.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

26.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

27 Related Standards, Policies and Processes

World Health Organization

28 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Pandemic

29 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Password Protection Policy

49. Overview

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of CTRMA's resources. All users, including contractors and vendors with access to CTRMA systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

50. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

51. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any CTRMA facility, has access to the CTRMA network, or stores any non-public CTRMA information.

52. Policy

4.1 Password Creation

4.1.1 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

4.1.2 Users must not use the same password for CTRMA accounts as for other non-CTRMA access (for example, personal ISP account, option trading, benefits, and so on).

4.1.3 Where possible, users must not use the same password for various CTRMA access needs.

4.1.4 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.

4.1.5 Where Simple Network Management Protocol (SNMP) is used, the community strings

must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in interactively. SNMP community strings must meet password construction guidelines.

4.2 Password Change

4.2.1 All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

4.2.2 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.

4.2.3 Password cracking or guessing may be performed on a periodic or random basis by the Infosec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4.3 Password Protection

4.3.1 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential CTRMA information. Corporate Information Security recognizes that legacy applications do not support proxy systems in place. Please refer to the technical reference for additional details.

4.3.2 Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication.

4.3.3 Passwords must not be revealed over the phone to anyone.

4.3.4 Do not reveal a password on questionnaires or security forms.

4.3.5 Do not hint at the format of a password (for example, "my family name").

4.3.6 Do not share CTRMA passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members.

4.3.7 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

4.3.8 Do not use the "Remember Password" feature of applications (for example, web browsers).

4.3.9 Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

4.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

4.4.1 Applications must support authentication of individual users, not groups.

4.4.2 Applications must not store passwords in clear text or in any easily reversible form.

4.4.3 Applications must not transmit passwords in clear text over the network.

4.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.5 Use of Passwords and Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

53. Policy Compliance

29.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

29.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

29.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

30 Related Standards, Policies and Processes

- Password Construction Guidelines

31 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Simple Network Management Protocol (SNMP)

32 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Security Response Plan Policy

54. Overview

A Security Response Plan (SRP) provides the impetus for security and business teams to integrate their efforts from the perspective of awareness and communication, as well as coordinated response in times of crisis (security vulnerability identified or exploited). Specifically, an SRP defines a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines. By requiring business units to incorporate an SRP as part of their business continuity operations and as new products or services are developed and prepared for release to consumers, ensures that when an incident occurs, swift mitigation and remediation ensues.

55. Purpose

The purpose of this policy is to establish the requirement that all business units supported by the Infosec team develop and maintain a security response plan. This ensures that security incident management team has all the necessary information to formulate a successful response should a specific security incident occur.

56. Scope

This policy applies any established and defined business unity or entity within the CTRMA.

4 Policy

The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the specific business unit for whom the SRP is being developed in cooperation with the Infosec Team. Business units are expected to properly facilitate the SRP for applicable to the service or products they are held accountable. The business unit security coordinator or champion is further expected to work with the <organizational information security unit> in the development and maintenance of a Security Response Plan.

4.1 Service or Product Description

The product description in an SRP must clearly define the service or application to be deployed with additional attention to data flows, logical diagrams, architecture considered highly useful.

4.2 Contact Information

The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to customer. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

4.3 Triage

The SRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

4.4 Identified Mitigations and Testing

The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

4.5 Mitigation and Remediation Timelines

The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

5 Policy Compliance

5.1 Compliance Measurement

Each business unit must be able to demonstrate they have a written SRP in place, and that it is under version control and is available via the web. The policy should be reviewed annually.

5.2 Exceptions

Any exception to this policy must be approved by the Infosec Team in advance and have a written record.

5.3 Non-Compliance

Any business unit found to have violated (no SRP developed prior to service or product deployment) this policy may be subject to delays in service or product release until such a time as the SRP is developed and approved. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur in the absence of an SRP

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

None.

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Public key pairs

- Symmetric cryptography

33 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Acquisition Assessment Policy

1. Overview

The process of integrating a newly acquired company can have a drastic impact on the security poster of either the parent company or the child company. The network and security infrastructure of both entities may vary greatly and the workforce of the new company may have a drastically different culture and tolerance to openness. The goal of the security acquisition assessment and integration process should include:

- Assess company's security landscape, posture, and policies
- Protect both CTRMA and the acquired company from increased security risks
- Educate acquired company about CTRMA policies and standard
- Adopt and implement CTRMA Security Policies and Standards
- Integrate acquired company
- Continuous monitoring and auditing of the acquisition

2. Purpose

The purpose of this policy is to establish Infosec responsibilities regarding corporate acquisitions, and define the minimum security requirements of an Infosec acquisition assessment.

3. Scope

This policy applies to all companies acquired by CTRMA and pertains to all systems, networks, laboratories, test equipment, hardware, software and firmware, owned and/or operated by the acquired company.

4. Policy

4.1 General

Acquisition assessments are conducted to ensure that a company being acquired by CTRMA does not pose a security risk to corporate networks, internal systems, and/or confidential/sensitive information. The Infosec Team will provide personnel to serve as active members of the acquisition team throughout the entire acquisition process. The Infosec role is to detect and evaluate information security risk, develop a remediation plan with the affected parties for the identified risk, and work with the acquisitions team to implement solutions for any identified security risks, prior to allowing connectivity to CTRMA's networks. Below are the minimum requirements that the acquired company must meet before being connected to the CTRMA network.

4.2 Requirements

4.2.1 Hosts

4.2.1.1 All hosts (servers, desktops, laptops) will be replaced or re-imaged with a CTRMA standard image or will be required to adopt the minimum standards for end user devices.

4.2.1.2 Business critical production servers that cannot be replaced or re-imaged must be audited and a waiver granted by Infosec.

4.2.1.3 All PC based hosts will require CTRMA approved virus protection before the network connection.

4.2.2 Networks

4.2.2.1 All network devices will be replaced or re-imaged with a CTRMA standard image.

4.2.2.2 Wireless network access points will be configured to the CTRMA standard.

4.2.3 Internet

4.2.3.1 All Internet connections will be terminated.

4.2.3.2 When justified by business requirements, air-gapped Internet connections require Infosec review and approval.

4.2.4 Remote Access

4.2.4.1 All remote access connections will be terminated.

4.2.4.2 Remote access to the production network will be provided by CTRMA.

4.2.5 Labs

4.2.5.1 Lab equipment must be physically separated and secured from non-lab areas.

4.2.5.2 The lab network must be separated from the corporate production network with a firewall between the two networks.

4.2.5.3 Any direct network connections (including analog lines, ISDN lines, T1, etc.) to external customers, partners, etc., must be reviewed and approved by the Lab Security Group (LabSec).

4.2.5.4 All acquired labs must meet with LabSec lab policy, or be granted a waiver by LabSec.

4.2.5.5 In the event the acquired networks and computer systems being connected to the corporate network fail to meet these requirements, the CTRMA Chief Information Officer (CIO) must acknowledge and approve of the risk to CTRMA's networks

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Business Critical Production Server

8 Revision History

Date of Change	Responsible	Summary of Change

Bluetooth Baseline Requirements Policy

6. Overview

Bluetooth enabled devices are exploding on the Internet at an astonishing rate. At the range of connectivity has increased substantially. Insecure Bluetooth connections can introduce a number of potential serious security issues. Hence, there is a need for a minimum standard for connecting Bluetooth enable devices.

7. Purpose

The purpose of this policy is to provide a minimum baseline standard for connecting Bluetooth enabled devices to the CTRMA network or CTRMA owned devices. The intent of the minimum standard is to ensure sufficient protection Personally Identifiable Information (PII) and confidential CTRMA data.

8. Scope

This policy applies to any Bluetooth enabled device that is connected to CTRMA network or owned devices.

9. Policy

4.1 Version
No Bluetooth Device shall be deployed on CTRMA equipment that does not meet a minimum of Bluetooth v2.1 specifications without written authorization from the Infosec Team. Any Bluetooth

equipment purchased prior to this policy must comply with all parts of this policy except the Bluetooth version specifications.

4.2 Pins and Pairing

When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area where you PIN can be compromised.

If your Bluetooth enabled equipment asks for you to enter your pin after you have initially paired it, you must refuse the pairing request and report it to Infosec, through your Help Desk, immediately.

4.3 Device Security Settings

- All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.
- Use a minimum PIN length of 8. A longer PIN provides more security.
- Switch the Bluetooth device to use the hidden mode (non-discoverable)
- Only activate Bluetooth only when it is needed.
- Ensure device firmware is up-to-date.

4.4 Security Audits

The Infosec Team may perform random audits to ensure compliancy with this policy. In the process of performing such audits, Infosec Team members shall not eavesdrop on any phone conversation.

4.5 Unauthorized Use

The following is a list of unauthorized uses of CTRMA-owned Bluetooth devices:

- Eavesdropping, device ID spoofing, DoS attacks, or any form of attacking other Bluetooth enabled devices.
- Using CTRMA-owned Bluetooth equipment on non-CTRMA-owned Bluetooth enabled devices.
- Unauthorized modification of Bluetooth devices for any purpose.

4.6 User Responsibilities

- It is the Bluetooth user's responsibility to comply with this policy.
- Bluetooth mode must be turned off when not in use.
- PII and/or CTRMA Confidential or Sensitive data must not be transmitted or stored on Bluetooth enabled devices.
- Bluetooth users must only access CTRMA information systems using approved Bluetooth device hardware, software, solutions, and connections.
- Bluetooth device hardware, software, solutions, and connections that do not meet the standards of this policy shall not be authorized for deployment.
- Bluetooth users must act appropriately to protect information, network access, passwords, cryptographic keys, and Bluetooth equipment.
- Bluetooth users are required to report any misuse, loss, or theft of Bluetooth devices or systems immediately to Infosec.

10. Policy Compliance

8.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

8.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

8.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9 Related Standards, Policies and Processes

None.

10 Definitions and Terms

None.

11 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Remote Access Policy

11. Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Hypergolic Reactions, LLC policy, we must mitigate these external risks the best of our ability.

12. Purpose

The purpose of this policy is to define rules and requirements for connecting to CTRMA's network from any host. These rules and requirements are designed to minimize the potential exposure to CTRMA from damages which may result from unauthorized use of CTRMA resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical CTRMA internal systems, and fines or other financial liabilities incurred as a result of those losses.

13. Scope

This policy applies to all CTRMA employees, contractors, vendors and agents with a CTRMA-owned or personally-owned computer or workstation used to connect to the CTRMA network. This policy applies to remote access connections used to do work on behalf of CTRMA, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to CTRMA networks.

14. Policy

It is the responsibility of CTRMA employees, contractors, vendors and agents with remote access privileges to CTRMA's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to CTRMA.

General access to the Internet for recreational use through the CTRMA network is strictly limited to CTRMA employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the CTRMA network from a personal computer, Authorized Users are responsible for preventing access to any CTRMA computer resources or data by non-Authorized Users. Performance of illegal activities through the CTRMA network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the *Acceptable Use Policy*.

Authorized Users will not use CTRMA networks to access the Internet for outside business interests.

For additional information regarding CTRMA's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website (company url).

4.1 Requirements

4.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the *Acceptable Encryption Policy* and the *Password Policy*.

4.1.2 Authorized Users shall protect their login and password, even from family members.

4.1.3 While using a CTRMA-owned computer to remotely connect to CTRMA's corporate network, Authorized Users shall ensure the remote host is not connected to any other

network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.1.4 Use of external resources to conduct CTRMA business must be approved in advance by InfoSec and the appropriate business unit manager.

4.1.5 All hosts that are connected to CTRMA internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.

4.1.6 Personal equipment used to connect to CTRMA's networks must meet the requirements of CTRMA-owned equipment for remote access as stated in the *Hardware and Software Configuration Standards for Remote Access to CTRMA Networks*.

15. Policy Compliance

11.1 Compliance Measurement

The Infosec Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

11.2 Exceptions

Any exception to the policy must be approved by Remote Access Services and the Infosec Team in advance.

11.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

12 Related Standards, Policies and Processes

Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of CTRMA's network:

- *Acceptable Encryption Policy*
- *Acceptable Use Policy*
- *Password Policy*
- *Third Party Agreement*
- *Hardware and Software Configuration Standards for Remote Access to CTRMA Networks*

13 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.
April 2015	Christopher Jarko	Added an Overview; created a group term for company employees, contractors, etc. ("Authorized Users"); strengthened the policy by explicitly limiting use of company resources to Authorized Users only; combined Requirements when possible, or eliminated Requirements better suited for a Standard (and added a reference to that Standard); consolidated list of related references to end of Policy.

Remote Access Tools Policy

16. Overview

Remote desktop software, also known as remote access tools, provide a way for computer users and support staff alike to share screens, access work computer systems from home, and vice versa. Examples of such software include LogMeIn, GoToMyPC, VNC (Virtual Network Computing), and Windows Remote Desktop (RDP). While these tools can save significant time and money by eliminating travel and enabling collaboration, they also provide a back door into the CTRMA network that can be used for theft of, unauthorized access to, or destruction of assets. As a result, only approved, monitored, and properly controlled remote access tools may be used on CTRMA computer systems.

17. Purpose

This policy defines the requirements for remote access tools used at <Company Name

18. Scope

This policy applies to all remote access where either end of the communication terminates at a CTRMA computer asset

19. Policy

All remote access tools used to communicate between CTRMA assets and other systems must comply with the following policy requirements.

4.1 Remote Access Tools

CTRMA provides mechanisms to collaborate between internal users, with external partners, and from non-CTRMA systems. The approved software list can be obtained from <link-to-

approved-remote-access-software-list>. Because proper configuration is important for secure use of these tools, mandatory configuration procedures are provided for each of the approved tools.

The approved software list may change at any time, but the following requirements will be used for selecting approved products:

a) All remote access tools or systems that allow communication to CTRMA resources from the Internet or external partner systems must require multi-factor authentication. Examples include authentication tokens and smart cards that require an additional PIN or password.
b) The authentication database source must be Active Directory or LDAP, and the authentication protocol must involve a challenge-response protocol that is not susceptible to replay attacks. The remote access tool must mutually authenticate both ends of the session.
c) Remote access tools must support the CTRMA application layer proxy rather than direct connections through the perimeter firewall(s).
d) Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the CTRMA network encryption protocols policy.
e) All CTRMA antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

All remote access tools must be purchased through the standard CTRMA procurement process, and the information technology group must approve the purchase.

20. Policy Compliance

13.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

13.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

13.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

14 Related Standards, Policies and Processes

None.

15 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- Application layer proxy

16 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Router and Switch Security Policy

21. Overview

See Purpose.

22. Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of CTRMA.

23. Scope

All employees, contractors, consultants, temporary and other workers at Cisco and its subsidiaries must adhere to this policy. All routers and switches connected to Cisco production networks are affected.

24. Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentication.
2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.
3. The following services or features must be disabled:
    a. IP directed broadcasts
    b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
    c. TCP small services
    d. UDP small services
    e. All source routing and switching
    f. All web services running on router

    g. Cisco discovery protocol on Internet connected interfaces
    h. Telnet, FTP, and HTTP services
    i. Auto-configuration
4. The following services should be disabled unless a business justification is provided:
    a. Cisco discovery protocol and other discovery protocols
    b. Dynamic trunking
    c. Scripting environments, such as the TCL shell
5. The following services must be configured:
    a. Password-encryption
    b. NTP configured to a corporate standard source
6. All routing updates shall be done using secure routing updates.
7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
9. Access control lists for transiting the device are to be added as business needs arise.
10. The router must be included in the corporate enterprise management system with a designated point of contact.
11. Each router must have the following statement presented for all forms of login whether remote or local:

    "UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.
14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
    a. IP access list accounting
    b. Device logging
    c. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped

d. Router console and modem access must be restricted by additional security controls

25. Policy Compliance

16.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

16.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

16.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

17 Related Standards, Policies and Processes

None.

18 Definitions and Terms

None.

19 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Wireless Communication Policy

26. Overview

With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors.

27. Purpose

The purpose of this policy is to secure and protect the information assets owned by CTRMA. CTRMA provides computer devices, networks, and other electronic information systems to meet

missions, goals, and initiatives. CTRMA grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to CTRMA network. Only **those** wireless infrastructure devices that meet the standards **specified in** this policy or are granted an exception by the Information Security Department are approved for connectivity to a CTRMA network.

28. Scope

All employees, contractors, consultants, temporary and other workers at CTRMA, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of CTRMA must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a CTRMA network or reside on a CTRMA site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

29. Policy

4.1 General Requirements

All wireless infrastructure devices that reside at a CTRMA site and connect to a CTRMA network, or provide access to information classified as CTRMA Confidential, or above must:

- Abide by the standards specified in the *Wireless Communication Standard*.
- Be installed, supported, and maintained by an approved support team.
- Use CTRMA approved authentication protocols and infrastructure.
- Use CTRMA approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

4.2 Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to CTRMA Confidential or above, must adhere to section 4.1 above. Lab and isolated wireless devices that do not provide general network connectivity to the CTRMA network must:

- Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the *Lab Security Policy*.
- Not interfere with wireless access deployments maintained by other support organizations.

4.3 Home Wireless Device Requirements

4.3.1 Wireless infrastructure devices that provide direct access to the CTRMA corporate network, must conform to the Home Wireless Device Requirements as detailed in the *Wireless Communication Standard*.

4.3.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be installed in a manner that prohibits direct access to the CTRMA corporate network. Access to the CTRMA corporate network through this device must use standard remote access authentication.

30. Policy Compliance

19.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

19.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

19.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

20 Related Standards, Policies and Processes

- Lab Security Policy
- Wireless Communication Standard

21 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- MAC Address

22 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Wireless Communication Standard

31. Overview

See Purpose.

32. Purpose

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a CTRMA network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the InfoSec Team are approved for connectivity to a CTRMA network.

Network devices including, but not limited to, hubs, routers, switches, firewalls, remote access devices, modems, or wireless access points, must be installed, supported, and maintained by an Information Security (Infosec) approved support organization. Lab network devices must comply with the *Lab Security Policy*.

33. Scope

All employees, contractors, consultants, temporary and other workers at CTRMA and its subsidiaries, including all personnel that maintain a wireless infrastructure device on behalf of CTRMA, must comply with this standard. This standard applies to wireless devices that make a connection the network and all wireless infrastructure devices that provide wireless connectivity to the network.

Infosec must approve exceptions to this standard in advance.

34. Standard

4.1 General Requirements
All wireless infrastructure devices that connect to a CTRMA network or provide access to CTRMA Confidential, CTRMA Highly Confidential, or CTRMA Restricted information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.
- All Bluetooth devices must use Secure Simple Pairing with encryption enabled.

4.2 Lab and Isolated Wireless Device Requirements

- Lab device Service Set Identifier (SSID) must be different from CTRMA production device SSID.
- Broadcast of lab device SSID must be disabled.

4.3 Home Wireless Device Requirements

All home wireless infrastructure devices that provide direct access to a CTRMA network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

- Enable WiFi Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS
- When enabling WPA-PSK, configure a complex shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Disable broadcast of SSID
- Change the default SSID name
- Change the default login and password

35. Policy Compliance

22.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

22.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

22.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

23 Related Standards, Policies and Processes

- Lab Security Policy

24 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- AES
- EAP-FAST
- EAP-TLS
- PEAP

- SSID
- TKIP
- WPA-PSK

25 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Database Credentials Coding Policy

1. Overview

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

2. Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of CTRMA's networks.

Software applications running on CTRMA's networks may require access to one of the many internal database servers. In order to access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

3. Scope

This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on the CTRMA Network. This policy applies to all software (programs, modules, libraries or APIS that will access a CTRMA, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they don't always use sanitized information.

4. Policy

General

In order to maintain the security of CTRMA's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

Specific Requirements

Storage of Data Base User Names and Passwords

- Database user names and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.
- Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.
- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication

may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.

- Database credentials may not reside in the documents tree of a web server.
- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.
- Passwords or pass phrases used to access a database must adhere to the *Password Policy*.

Retrieval of Database User Names and Passwords

- If stored in a file that is not source code, then database user names and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the user name and password must be released or cleared.

- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

- For languages that execute from source code, the credentials' source file must not reside in the same browseable or executable file directory tree in which the executing body of code resides.

Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the *Password Policy*.
- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the *Password Policy*. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

Coding Techniques for implementing this policy

[Add references to your site-specific guidelines for the different coding languages such as Perl, JAVA, C and/or Cpro.]

5. Policy Compliance

5.1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

5.1. Exceptions
Any exception to the policy must be approved by the Infosec team in advance.

5.2. Non-Compliance
An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with CTRMA.

Any program code or application that is found to violate this policy must be remediated within a 90 day period.

6. Related Standards, Policies and Processes

- Password Policy

7. Definitions and Terms

- Credentials
- Executing Body
- Hash Function
- LDAP
- Module

8. Revision History

Date of Change	**Responsible**	**Summary of Change**
June 2014	SANS Policy Team	Formatted into new template and made minor wording changes.

Information Logging Standard

9. Overview

Logging from critical systems, applications and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint.

10. Purpose

The purpose of this document attempts to address this issue by identifying specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with an enterprise's log management function.

The intention is that this language can easily be adapted for use in enterprise IT security policies and standards, and also in enterprise procurement standards and RFP templates. In this way, organizations can ensure that new IT systems, whether developed in-house or procured, support necessary audit logging and log management functions.

11. Scope

This policy applies to all production systems on CTRMA Network.

12. Standard

4.1 General Requirements

All systems that handle confidential information, accept network connections, or make access control (authentication and authorization) decisions shall record and retain audit-logging information sufficient to answer the following questions:

1. What activity was performed?
2. Who or what performed the activity, including where or on what system the activity was performed from (subject)?
3. What the activity was performed on (object)?
4. When was the activity performed?
5. What tool(s) was the activity was performed with?
6. What was the status (such as success vs. failure), outcome, or result of the activity?
7.

4.2 Activities to be Logged

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

1. Create, read, update, or delete confidential information, including confidential authentication information such as passwords;
2. Create, update, or delete information not covered in #1;
3. Initiate a network connection;
4. Accept a network connection;
5. User authentication and authorization for activities covered in #1 or #2 such as user login and logout;

6. Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
7. System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
8. Application process startup, shutdown, or restart;
9. Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and
10. Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

4.3 Elements of the Log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term “indirectly” means unambiguously inferred.

1. Type of action – examples include authorize, create, read, update, delete, and accept network connection.
2. Subsystem performing the action – examples include process or transaction name, process or transaction identifier.
3. Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
4. Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
5. Before and after values when action involves updating a data element, if feasible.
6. Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
7. Whether the action was allowed or denied by access-control mechanisms.
8. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

4.4 Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include but are not limited to the following:

1. Microsoft Windows Event Logs collected by a centralized log management system;

2. Logs in a well-documented format sent via *syslog*, *syslog-ng*, or *syslog-reliable* network protocols to a centralized log management system;
3. Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and
4. Other open logging mechanisms supporting the above requirements including those based on CheckPoint OpSec, ArcSight CEF, and IDMEF.

13. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6 Related Standards, Policies and Processes

None.

7 Definitions and Terms

None.

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Lab Security Policy

14. Overview

See Purpose.

15. Purpose

This policy establishes the information security requirements to help manage and safeguard lab resources and CTRMA networks by minimizing the exposure of critical infrastructure and information assets to threats that may result from unprotected hosts and unauthorized access.

16. Scope

This policy applies to all employees, contractors, consultants, temporary and other workers at CTRMA and its subsidiaries must adhere to this policy. This policy applies to CTRMA owned and managed labs, including labs outside the corporate firewall (DMZ).

17. Policy

4.1 General Requirements

4.1.1 Lab owning organizations are responsible for assigning lab managers, a point of contact (POC), and a back-up POC for each lab. Lab owners must maintain up-to-date POC information with InfoSec and the Corporate Enterprise Management Team. Lab managers or their backup must be available around-the-clock for emergencies, otherwise actions will be taken without their involvement.

4.1.2 Lab managers are responsible for the security of their labs and the lab's impact on the corporate production network and any other networks. Lab managers are responsible for adherence to this policy and associated processes. Where policies and procedures are undefined lab managers must do their best to safeguard CTRMA from security vulnerabilities.

4.1.3 Lab managers are responsible for the lab's compliance with all CTRMA security policies.

4.1.4 The Lab Manager is responsible for controlling lab access. Access to any given lab will only be granted by the lab manager or designee, to those individuals with an immediate business need within the lab, either short-term or as defined by their ongoing job function. This includes continually monitoring the access list to ensure that those who no longer require access to the lab have their access terminated.

4.1.5 All user passwords must comply with CTRMA's *Password Policy*.

4.1.6 Individual user accounts on any lab device must be deleted when no longer authorized within three (3) days. Group account passwords on lab computers (Unix, windows, etc) must be changed quarterly (once every 3 months).

4.1.7 PC-based lab computers must have CTRMA's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free.

4.1.8 Any activities with the intention to create and/or distribute malicious programs into CTRMA's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

4.1.9 No lab shall provide production services. Production services are defined as ongoing and shared business critical services that generate revenue streams or provide customer capabilities. These should be managed by a <proper support> organization.

4.1.10 In accordance with *the Data Classification Policy*, information that is marked as CTRMA Highly Confidential or CTRMA Restricted is prohibited on lab equipment.

4.1.11 Immediate access to equipment and system logs must be granted to members of InfoSec and the Network Support Organization upon request, in accordance with the *Audit Policy*.

4.1.12 InfoSec will address non-compliance waiver requests on a case-by-case basis and approve waivers if justified.

4.2 Internal Lab Security Requirements

4.2.1 The Network Support Organization must maintain a firewall device between the corporate production network and all lab equipment.

4.2.2 The Network Support Organization and/or InfoSec reserve the right to interrupt lab connections that impact the corporate production network negatively or pose a security risk.

4.2.3 The Network Support Organization must record all lab IP addresses, which are routed within CTRMA networks, in Enterprise Address Management database along with current contact information for that lab.

4.2.4 Any lab that wants to add an external connection must provide a diagram and documentation to InfoSec with business justification, the equipment, and the IP address space information. InfoSec will review for security concerns and must approve before such connections are implemented.

4.2.5 All traffic between the corporate production and the lab network must go through a Network Support Organization maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and production networks.

4.2.6 Original firewall configurations and any changes thereto must be reviewed and approved by InfoSec. InfoSec may require security improvements as needed.

4.2.7 Labs are prohibited from engaging in port scanning, network auto-discovery, traffic spamming/flooding, and other similar activities that negatively impact the corporate network and/or non-CTRMA networks. These activities must be restricted within the lab.

4.2.8 Traffic between production networks and lab networks, as well as traffic between separate lab networks, is permitted based on business needs and as long as the traffic does not negatively impact on other networks. Labs must not advertise network services that may compromise production network services or put lab confidential information at risk.

4.2.9 InfoSec reserves the right to audit all lab-related data and administration processes at any time, including but not limited to, inbound and outbound packets, firewalls and network peripherals.

4.2.10 Lab owned gateway devices are required to comply with all CTRMA product security advisories and must authenticate against the Corporate Authentication servers.

4.2.11 The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with CTRMA's *Password Policy*. The password will only be provided to those who are authorized to administer the lab network.

4.2.12 In labs where non-CTRMA personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no CTRMA confidential information can reside on any computer equipment in these labs. Connectivity for authorized personnel from these labs can be allowed to the corporate production network only if authenticated against the Corporate Authentication servers, temporary access lists (lock and key), SSH, client VPNs, or similar technology approved by InfoSec.

4.2.13 Lab networks with external connections are prohibited from connecting to the corporate production network or other internal networks through a direct connection, wireless connection, or other computing equipment.

4.3 DMZ Lab Security Requirements

4.3.1 New DMZ labs require a business justification and VP-level approval from the business unit. Changes to the connectivity or purpose of an existing DMZ lab must be reviewed and approved by the InfoSec Team.

4.3.2 DMZ labs must be in a physically separate room, cage, or secured lockable rack with limited access. In addition, the Lab Manager must maintain a list of who has access to the equipment.

4.3.3 DMZ lab POCs must maintain network devices deployed in the DMZ lab up to the network support organization point of demarcation.

4.3.4 DMZ labs must not connect to corporate internal networks, either directly, logically (for example, IPSEC tunnel), through a wireless connection, or multi-homed machine.

4.3.5 An approved network support organization must maintain a firewall device between the DMZ lab and the Internet. Firewall devices must be configured based on least privilege access principles and the DMZ lab business requirements. Original firewall configurations and subsequent changes must be reviewed and approved by the InfoSec Team. All traffic between the DMZ lab and the Internet must go through the approved firewall. Cross-connections that bypass the firewall device are strictly prohibited.

4.3.6 All routers and switches not used for testing and/or training must conform to the DMZ Router and Switch standardization documents.

4.3.7 Operating systems of all hosts internal to the DMZ lab running Internet Services must be configured to the secure host installation and configuration standards published the InfoSec Team.

4.3.8 Remote administration must be performed over secure channels (for example, encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.

4.3.9 DMZ lab devices must not be an open proxy to the Internet.

4.3.10 The Network Support Organization and InfoSec reserve the right to interrupt lab connections if a security concern exists.

18. Policy Compliance

8.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

8.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

8.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

9 Related Standards, Policies and Processes

- Audit Policy
- Acceptable Use Policy
- Data Classification Policy
- Password Policy

10 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- DMZ
- Firewall

11 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated, made general lab and included DMZ lab requirements, and converted to new format.

Server Security Policy

19. Overview

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

20. Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by CTRMA. Effective implementation of this policy will minimize unauthorized access to CTRMA proprietary information and technology.

21. Scope

All employees, contractors, consultants, temporary and other workers at Cisco and its subsidiaries must adhere to this policy. This policy applies to server equipment that is owned, operated, or leased by Cisco or registered under a Cisco-owned internal network domain.

This policy specifies requirements for equipment on the internal Cisco network. For secure configuration of equipment external to Cisco on the DMZ, see the Internet *DMZ Equipment Policy*.

22. Policy

4.1 General Requirements

4.1.1 All internal servers deployed at CTRMA must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by InfoSec. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures

4.1.2 For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the *Audit Policy*.

4.2 Configuration Requirements

4.2.1 Operating System configuration should be in accordance with approved InfoSec guidelines.

4.2.2 Services and applications that will not be used must be disabled where practical.

4.2.3 Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

4.2.4 The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.

4.2.5 Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

4.2.6 Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.

4.2.7 If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

4.2.8 Servers should be physically located in an access-controlled environment.

4.2.9 Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3 Monitoring

4.3.1 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.

4.3.2 Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks
- Evidence of unauthorized access to privileged accounts
- Anomalous occurrences that are not related to specific applications on the host.

23. Policy Compliance

11.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

11.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

11.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

12 Related Standards, Policies and Processes

- Audit Policy

- DMZ Equipment Policy

13 Definitions and Terms

The following definition and terms can be found in the SANS Glossary located at:
https://www.sans.org/security-resources/glossary-of-terms/

- De-militarized zone (DMZ)

14 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Software Installation Policy

24. Overview

Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on company equipment.

25. Purpose

The purpose of this policy is to outline the requirements around installation software on <Company Owned> computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within <Company Name's> computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

26. Scope

This policy applies to all CTRMA employees, contractors, vendors and agents with a CTRMA-owned mobile devices. This policy covers all computers, servers, smartphones, tablets and other computing devices operating within CTRMA.

27. Policy

- Employees may not install software on <Company Name's> computing devices operated within the CTRMA network.
- Software requests must first be approved by the requester's manager and then be made to the Information Technology department or Help Desk in writing or via email.
- Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requester's need.
- The Information Technology Department will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

28. Policy Compliance

14.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

14.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

14.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

15 Related Standards, Policies and Processes

None.

16 Definitions and Terms

None.

17 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Technology Equipment Disposal Policy

29. Overview

Technology equipment often contains parts which cannot simply be thrown away. Proper disposal of equipment is both environmentally responsible and often required by law. In addition, hard drives, USB drives, CD-ROMs and other storage media contain various kinds of CTRMA data, some of which is considered sensitive. In order to protect our constituent's data, all storage mediums must be properly erased before being disposed of. However, simply deleting or even formatting data is not considered sufficient. When deleting files or formatting a device, data is marked for deletion, but is still accessible until being overwritten by a new file. Therefore, special tools must be used to securely erase data prior to equipment disposal.

30. Purpose

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by CTRMA.

31. Scope

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within CTRMA including, but not limited to the following: personal computers, servers, hard drives, laptops, mainframes, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, typewriters, compact and floppy discs, portable storage devices (i.e., USB drives), backup tapes, printed materials.

All CTRMA employees and affiliates must comply with this policy.

32. Policy

4.1 Technology Equipment Disposal

4.1.1 When Technology assets have reached the end of their useful life they should be sent to the <Equipment Disposal Team> office for proper disposal.

4.1.2 The <Equipment Disposal Team> will securely erase all storage mediums in accordance with current industry best practices.

4.1.3 All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defense standards.

4.1.4 No computer or technology equipment may be sold to any individual other than through the processes identified in this policy (Section 4.2 below).

4.1.5 No computer equipment should be disposed of via skips, dumps, landfill etc. Electronic recycling bins may be periodically placed in locations around CTRMA. These can be used to dispose of equipment. The <Equipment Disposal Team> will properly remove all data prior to final disposal.

4.1.6 All electronic drives must be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).

4.1.7 Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes, etc.

4.1.8 The <Equipment Disposal Team> will place a sticker on the equipment case indicating the disk wipe has been performed. The sticker will include the date and the initials of the technician who performed the disk wipe.

4.1.9 Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

4.2 Employee Purchase of Disposed Equipment

4.2.1 Equipment which is working, but reached the end of its useful life to CTRMA, will be made available for purchase by employees.

4.2.2 A lottery system will be used to determine who has the opportunity to purchase available equipment.

4.2.3 All equipment purchases must go through the lottery process. Employees cannot purchase their office computer directly or "reserve" a system. This ensures that all employees have an equal chance of obtaining equipment.

4.2.4 Finance and Information Technology will determine an appropriate cost for each item.

4.2.5 All purchases are final. No warranty or support will be provided with any equipment sold.

4.2.6 Any equipment not in working order or remaining from the lottery process will be donated or disposed of according to current environmental guidelines. Information

4.2.7 Technology has contracted with several organizations to donate or properly dispose of outdated technology assets.

4.2.8 Prior to leaving CTRMA premises, all equipment must be removed from the Information Technology inventory system.

33. Policy Compliance

17.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

17.2 Exceptions

Any exception to the policy must be approved by the Infosec Team in advance.

17.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

18 Related Standards, Policies and Processes

None.

19 Definitions and Terms

None.

20 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Workstation Security (For HIPAA) Policy

34. Overview

See Purpose.

35. Purpose

The purpose of this policy is to provide guidance for workstation security for CTRMA workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

36. Scope

This policy applies to all CTRMA employees, contractors, workforce members, vendors and agents with a CTRMA-owned or personal-workstation connected to the CTRMA network.

37. Policy

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users.

3.1 Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.
3.2 CTRMA will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

3.3 Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with CTRMA *Password Policy*.
- Complying with all applicable password policies and procedures. See CTRMA *Password Policy*.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.
- Storing all sensitive information, including protected health information (PHI) on network servers
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the *Portable Workstation Encryption Policy*
- Complying with the Baseline *Workstation Configuration Standard*
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Exit running applications and close open documents
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the *Wireless Communication policy*

38. Policy Compliance

20.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

20.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

20.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

21 Related Standards, Policies and Processes

- Password Policy
- Portable Workstation Encryption Policy
- Wireless Communication policy
- Workstation Configuration Standard

HIPPA 164.210
http://www.hipaasurvivalguide.com/hipaa-regulations/164-310.php

About HIPPA
http://abouthipaa.com/about-hipaa/hipaa-hitech-resources/hipaa-security-final-rule/164-308a1i-administrative-safeguards-standard-security-management-process-5-3-2-2/

22 Definitions and Terms

None.

23 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Web Application Security Policy

1. Overview

Web application vulnerabilities account for the largest portion of attack vectors outside of malware. It is crucial that any web application be assessed for vulnerabilities and any vulnerabilities be remediated prior to production deployment.

2. Purpose

The purpose of this policy is to define web application security assessments within **CTRMA**. Web application assessments are performed to identify potential or realized weaknesses as a result of inadvertent mis-configuration, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of **CTRMA** services available both internally and externally as well as satisfy compliance with any relevant policies in place.

3. Scope

This policy covers all web application security assessments requested by any individual, group or department for the purposes of maintaining the security posture, compliance, risk management, and change control of technologies in use at **CTRMA**.

All web application security assessments will be performed by delegated security personnel either employed or contracted by **CTRMA**. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of **CTRMA** is strictly prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to the start of the assessment.

4. Policy

4.1 Web applications are subject to security assessments based on the following criteria:

a) New or Major Application Release – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
b) Third Party or Acquired Web Application – will be subject to full assessment after which it will be bound to policy requirements.
c) Point Releases – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.

d) Patch Releases – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
e) Emergency Releases – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency releases will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

4.2 All security issues that are discovered during assessments must be mitigated based upon the following risk levels. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of Medium risk level or greater.

a) High – Any high risk issue must be fixed immediately or other mitigation strategies must be put in place to limit exposure before deployment. Applications with high risk issues are subject to being taken off-line or denied release into the live environment.
b) Medium – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
c) Low – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

4.3 The following security assessment levels shall be established by the InfoSec organization or other designated organization that will be performing the assessments.

a) Full – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of any and all discovered.
b) Quick – A quick assessment will consist of a (typically) automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
c) Targeted – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

4.4 The current approved web application security assessment tools in use which will be used for testing are:

- <Tool/Application 1>
- <Tool/Application 2>

- …

Other tools and/or techniques may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

5. Policy Compliance

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Web application assessments are a requirement of the change control process and are required to adhere to this policy unless found to be exempt. All application releases must pass through the change control process. Any web applications that do not adhere to this policy may be taken offline until such time that a formal assessment can be performed at the discretion of the Chief Information Officer.

6 Related Standards, Policies and Processes

OWASP Top Ten Project

OWASP Testing Guide

OWASP Risk Rating Methodology

7 Definitions and Terms

None.

8 Revision History

Date of Change	Responsible	Summary of Change
June 2014	SANS Policy Team	Updated and converted to new format.

Appendix D

Trust Services Criteria

AICPA

TSP Section 100

2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

Includes March 2020 updates

TSP Section 100

2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

(This version includes revisions made in March 2020, as discussed in the Notice to Readers.)

Notice to Readers

The *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* presents control criteria established by the Assurance Services Executive Committee (ASEC) of the AICPA for use in attestation or consulting engagements to evaluate and report on controls over the security, availability, processing integrity, confidentiality, or privacy of information and systems (*a*) across an entire entity; (*b*) at a subsidiary, division, or operating unit level; (*c*) within a function relevant to the entity's operational, reporting, or compliance objectives; or (*d*) for a particular type of information used by the entity.

In developing and establishing these criteria, ASEC followed due process procedures, including exposure of criteria for public comment. BL section 360R, *Implementing Resolutions Under Section 3.6 Committees*, [fn 1] designates ASEC as a senior technical committee with the authority to make public statements without clearance from the AICPA council or the board of directors. Paragraph .A44 of AT-C section 105, *Concepts Common to All Attestation Engagements*, [fn 2] indicates that criteria promulgated by a body designated by the Council of the AICPA under the AICPA Code of Professional Conduct are, by definition, considered suitable.

This version of the trust services criteria has been modified by AICPA staff to include conforming changes necessary because of the issuance, in March 2020, of a new SOC examination. In a SOC for Supply Chain examination, a practitioner examines and reports on the effectiveness of controls (suitability of design and operating effectiveness) relevant to the security, availability, or processing integrity of a system or the confidentiality or privacy of information processed by a system that produces, manufactures, or distributes products.

These changes, which have been reviewed by the ASEC chair, were made to provide greater flexibility for use of the trust services criteria in a SOC for Supply Chain examination. It is important to note that these changes do not alter in any way the trust services criteria used to evaluate controls in a SOC 2®, SOC 3®, or SOC for Cybersecurity examination.

[fn 1] All BL sections can be found in AICPA *Professional Standards*.

[fn 2] All AT-C sections can be found in AICPA *Professional Standards*.

For users who want to see all conforming changes made to this version of the trust services criteria, a red-lined version is available at https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria-redline-2019.pdf.

Background

.01 The AICPA Assurance Services Executive Committee (ASEC) has developed a set of criteria (trust services criteria) to be used when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the systems at an entity, a division, or an operating unit of an entity. In addition, the trust services criteria may be used when evaluating the design and operating effectiveness of controls relevant to the security, availability, processing integrity, confidentiality or privacy of a particular type of information processed by one or more of an entity's systems or one or more systems used to support a particular function within the entity. This document presents the trust services criteria.

.02 As in any system of internal control, an entity faces risks that threaten its ability to achieve its objectives based on the trust services criteria. Such risks arise because of factors such as the following:

- The nature of the entity's operations
- The environment in which it operates
- The types of information generated, used, or stored by the entity
- The types of commitments made to customers and other third parties
- Responsibilities entailed in operating and maintaining the entity's systems and processes
- The technologies, connection types, and delivery channels used by the entity
- The use of third parties (such as service providers and suppliers), who have access to the entity's system, to provide the entity with critical raw materials or components or operate controls that are necessary, in combination with the entity's controls, to achieve the system's objectives
- Changes to the following:
    - — System operations and related controls
    - — Processing volume
    - — Key management personnel of a business unit, supporting IT, or related personnel
    - — Legal and regulatory requirements with which the entity needs to comply
- Introduction of new services, products, or technologies

An entity addresses these risks through the implementation of suitably designed controls that, if operating effectively, provide reasonable assurance of achieving the entity's objectives.

.03 Applying the trust services criteria in actual situations requires judgment. Therefore, in addition to the trust services criteria, this document presents points of focus for each criterion. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), in its *Internal Control — Integrated Framework* (the COSO framework), [fn 3] states that points of focus represent important characteristics of the criteria. Consistent with the COSO framework, the points of focus in this document may assist management when designing, implementing, and operating controls over security, availability, processing integrity, confidentiality, and privacy. In addition, the points of focus may assist both management and the practitioner when they are evaluating whether the controls were suitably designed and operated effectively to achieve the entity's objectives based on the trust services criteria.

.04 Some points of focus may not be suitable or relevant to the entity or to the engagement to be performed. In such situations, management may customize a particular point of focus or identify and consider other characteristics based on the specific circumstances of the entity. Use of the trust services criteria does not require an assessment of whether each point of focus is addressed. Users are advised to consider the facts and circumstances of the entity and its environment in actual situations when applying the trust services criteria.

Organization of the Trust Services Criteria

.05 The trust services criteria presented in this document have been aligned to the 17 criteria (known as *principles*) presented in the COSO framework, which was revised in 2013. In addition to the 17 principles, the trust services criteria include additional criteria supplementing COSO principle 12: *The entity deploys control activities through policies that establish what is expected and procedures that put policies into action* (supplemental criteria). The supplemental criteria, which apply to the achievement of the entity's objectives relevant to a trust services engagement, are organized as follows:

- *Logical and physical access controls.* The criteria relevant to how an entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access
- *System operations.* The criteria relevant to how an entity manages the operation of system(s) and detects and mitigates processing deviations, including logical and physical security deviations
- *Change management.* The criteria relevant to how an entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made
- *Risk mitigation.* The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners

.06 In addition to the 17 principles in the COSO framework, certain of the supplemental criteria are shared amongst all the trust services categories (see the section "Trust Services Categories"). For example, the

---

[fn 3]

criteria related to logical access apply to the security, availability, processing integrity, confidentiality, and privacy categories. As a result, the trust services criteria consist of

- criteria common to all five of the trust services categories (common criteria) and
- additional specific criteria for the availability, processing integrity, confidentiality, and privacy categories.

.07 The common criteria provide specific criteria for addressing the following:

- The control environment (CC1 series)
- Communication and information (CC2 series)
- Risk assessment (CC3 series)
- Monitoring of controls (CC4 series)
- Control activities related to the design and implementation of controls (CC5 series)

The common criteria are suitable for evaluating the effectiveness of controls to achieve an entity's system objectives related to security; no additional control activity criteria are needed. For the categories of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of (*a*) the common criteria and (*b*) the control activity criteria applicable to the specific trust services category or categories addressed by the engagement. The criteria for each trust services category addressed by the engagement are considered complete only if all the criteria associated with that category are addressed by the engagement.

Trust Services Category	***Common Criteria***	***Additional Category-Specific Criteria***
Security	X	N/A
Availability	X	X (A series)
Processing Integrity (Over the Provision of Services or the Production, Manufacturing, or Distribution of Goods)	X	X (PI series)
Confidentiality	X	X (C series)
Privacy	X	X (P series)

.08 The practitioner may report on any of the trust services categories of security, availability, processing integrity, confidentiality, or privacy, either individually or in combination with one or more of the other trust services categories. For each category addressed by the engagement, all criteria for that category are usually addressed. However, in limited circumstances, such as when the scope of the engagement is to report on a system and a particular criterion is not relevant to the services provided by a service organization, one or more criteria may not be applicable to the engagement. For example, when reporting on

privacy for a service organization's system, criterion P3.1, *Personal information is collected consistent with the entity's objectives related to privacy*, is not applicable for a service organization that does not directly collect personal information from data subjects.

Trust Services Categories

.09 The table in paragraph .24 presents the trust services criteria and the related points of focus. In that table, the trust services criteria are classified into the following categories:

a. *Security.* Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.

Security refers to the protection of

i. information during its collection or creation, use, processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

b. *Availability.* Information and systems are available for operation and use to meet the entity's objectives.

Availability refers to the accessibility of information used by the entity's systems as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

c. *Processing integrity (over the provision of services or the production, manufacturing, or distribution of goods).* System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation. Because of the number of systems used by an entity, processing integrity is usually only addressed at the system or functional level of an entity. In a SOC for Supply Chain examination, processing integrity refers to whether processing is complete, valid, accurate, timely, and authorized to produce, manufacture, or distribute goods that meet the products' specifications.

d. *Confidentiality.* Information designated as confidential is protected to meet the entity's objectives.

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

e. *Privacy.* Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

Although confidentiality applies to various types of sensitive information, *privacy* applies only to personal information.

The privacy criteria are organized as follows:

i. *Notice and communication of objectives.* The entity provides notice to data subjects about its objectives related to privacy.

ii. *Choice and consent.* The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.

iii. *Collection.* The entity collects personal information to meet its objectives related to privacy.

iv. *Use, retention, and disposal.* The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.

v. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.

vi. *Disclosure and notification.* The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.

vii. *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.

viii. *Monitoring and enforcement.* The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

.10 As previously stated, the trust services criteria may be used when evaluating the suitability of the design and operating effectiveness of controls relevant to the security, availability, or processing integrity of information and systems, or the confidentiality or privacy of the information processed by the entity. As such, they may be used when evaluating whether the entity's controls were effective to meet the criteria relevant to any of those categories (security, availability, processing integrity, confidentiality, or privacy), either individually or in combination with controls in other categories.

Application and Use of the Trust Services Criteria

.11 The trust services criteria were designed to provide flexibility in application and use for a variety of different subject matters. The following are the types of subject matters a practitioner may be engaged to report on using the trust services criteria:

- The effectiveness of controls within an entity's cybersecurity risk management program to achieve the entity's cybersecurity objectives using the trust services criteria relevant to security, availability, and confidentiality as *control criteria* in a SOC for Cybersecurity examination. [fn 4]

- The suitability of design and operating effectiveness of controls included in management's description of a service organization's system relevant to one or more of the trust services criteria over security, availability, processing integrity, confidentiality, or privacy throughout a specified period to achieve the entity's objectives based on those criteria in a type 2 SOC 2 engagement. A type 2 SOC 2 engagement, which includes an opinion on the operating effectiveness of controls, also includes a detailed description of tests of controls performed by the service auditor and the results of those tests. A type 1 SOC 2 engagement addresses the same subject matter as a type 2 SOC 2 engagement; however, a type 1 SOC 2 report does not contain an opinion on the operating effectiveness of controls nor a detailed description of tests of controls performed by the service auditor and the results of those tests. [fn 5]

- The design and operating effectiveness of a service organization's controls over a system relevant to one or more of the trust services criteria over security, availability, processing integrity, confidentiality, and privacy in a SOC 3 engagement. A SOC 3 report contains an opinion on the operating effectiveness of controls but does not include a detailed description of tests of controls performed by the service auditor and the results of those tests.

[fn 4] AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls* (the cybersecurity guide) provides practitioners with performance and reporting guidance for a SOC for Cybersecurity examination.

[fn 5] AICPA Guide *SOC 2® Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*, issued in 2018, contains performance and reporting guidance for SOC 2 examinations.

- The suitability of design and operating effectiveness of controls of an entity, other than a service organization, over one or more systems relevant to one or more of the trust services categories of security, availability, processing integrity, confidentiality, or privacy (for example, a SOC for Supply Chain examination).

- The suitability of the design of an entity's controls over security, availability, processing integrity, confidentiality, or privacy to achieve the entity's objectives based on the related trust services criteria. [fn 6]

.12 Practitioners generally do not use the trust services criteria when engaged to report on an entity's compliance, or on an entity's internal control over compliance with laws, regulations, rules, contracts, or grant agreements. If the practitioner is engaged to report on compliance with laws, regulations, rules, contracts, or grant agreements in connection with an examination of the design and operating effectiveness of an entity's controls (for example, in a privacy engagement performed in accordance with AT-C section 105 and AT- Csection 205, *Examination Engagements*), the compliance portion of the engagement would be performed in accordance with AT-C section 105 and AT-C section 315, *Compliance Attestation*.

.13 Many of the trust services criteria include the phrase *to meet the entity's objectives.* Because the trust services criteria may be used to evaluate controls relevant to a variety of different subject matters (see paragraph .11) in a variety of different types of engagements (see paragraphs .20–.23), interpretation of that phrase depends upon the specific circumstances of the engagement. Therefore, when using the trust services criteria, consideration is given to how the *entity's objectives* referred to in the criteria are affected by the subject matter and scope of the particular engagement.

.14 For example, consider the following engagements:

- In a SOC 2 engagement to examine and report on a service organization's controls over the security, availability, processing integrity, confidentiality, or privacy of a *system*, management is responsible for meeting its commitments to customers. Therefore, the *objectives* in a SOC 2 engagement relate *to meeting its commitments to customers and system requirements. Commitments* are the declarations made by management to customers regarding the performance of one or more of the entity's systems. Such commitments generally are included in written contracts, service level agreements, or public statements (for example, a privacy notice). Some commitments are applicable to all customers (baseline commitments), whereas others are designed to meet individual customer needs and result in the implementation of processes or controls, in addition to those required to meet the baseline commitments. *System requirements* refer to how the system should function to achieve the entity's commitments to customers, relevant laws and regulations, or guidelines of industry groups, such as trade or business associations.

[fn 6] AT-C section 9205, *Examination Engagements: Attestation Interpretations of Section 205*, addresses an engagement such as this in Interpretation No. 2, "Reporting on the Design of Internal Control" (AT-C sec. 9205 par. .04–.14). That document states that a practitioner may examine the suitability of the design of controls under AT-C section 205, *Examination Engagements*. Paragraph .10 of AT-C section 205 provides guidance on how a practitioner should report when the engagement is over controls that have not yet been implemented.

- In a SOC for Supply Chain engagement to examine and report on an entity's controls over the security, availability, processing integrity, confidentiality, or privacy of a system used to produce, manufacture, or distribute products, management is responsible for establishing principal system objectives. Such objectives are embodied in the product commitments the entity makes to customers, including producing or manufacturing a product that meets product performance specifications and other production, manufacturing, or distribution specifications. Commitments may also relate to other matters (for example, conforming with a variety of other standards and criteria such as the risk entity management framework issued by the National Institute of Standards and Technology, the cybersecurity standards issued by the International Organization for Standardization [ISO], or the Food and Drug Administration regulations on electronic records and electronic signatures included in Code of Federal Regulations, *Electronic Records; Electronic Signatures*, Title 21, Part 11).

- In an entity-wide SOC for Cybersecurity examination, the entity establishes *cybersecurity objectives. Cybersecurity objectives* are those that could be affected by cybersecurity risk and, therefore, affect the achievement of the entity's compliance, reporting, and operational objectives. The nature of an entity's cybersecurity objectives will vary depending on the environment in which the entity operates, the entity's mission and vision, the overall business objectives established by management, and other factors. For example, a telecommunication entity may have a cybersecurity objective related to the reliable functioning of those aspects of its operations that are deemed to be critical infrastructure, whereas an online dating entity is likely to regard the privacy of the personal information collected from customers to be a critical factor in achieving its operating objectives. [fn 7]

.15 As an example of how the different subject matters and engagement scopes affect the use of the trust services criteria, consider trust services criterion CC6.4:

> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

.16 In the SOC 2 engagement example discussed in paragraph .14, the phrase *to meet the entity's objectives* in CC6.4 usually would be interpreted as follows:

> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel *to meet the service organization's commitments and system requirements.*

.17 In addition, criterion CC6.4 would only be applied as it relates to controls over the trust services category(ies) relevant to the system(s) included within the scope of the SOC 2 engagement.

[fn 7] The practitioner's responsibility is similar to that in AT-C section 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*, which requires the service auditor in a SOC 1® engagement to determine whether the control objectives stated in management's description of the service organization's system are reasonable in the circumstances.

.18 In the SOC for Cybersecurity examination example in paragraph .14, the phrase *to meet the entity's objectives* in CC6.4 usually would be interpreted as follows:

> The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's cybersecurity objectives.

.19 In addition, criterion CC6.4 would be applied as it relates to controls within the cybersecurity risk management program (*a*) across an entire entity; (*b*) at a subsidiary, division, or operating unit level; (*c*) within a function relevant to the entity's operations, reporting, or compliance objectives; or (*d*) for a particular type of information used by the entity, depending on the scope of the SOC for Cybersecurity examination.

Professional Standards Governing Engagements Using the Trust Services Criteria

Attestation Engagements

.20 Examination engagements and engagements to apply agreed-upon procedures performed in accordance with the AICPA Statements on Standards for Attestation Engagements [fn 8] (SSAEs or attestation standards) may use the trust services criteria as the evaluation criteria. The attestation standards provide guidance on performing and reporting in connection with an examination, review, [fn 9] and agreed-upon procedures engagements. Under the attestation standards, the CPA performing an attestation engagement is known as a *practitioner*. In an examination engagement, the practitioner provides a report in which he or she expresses an opinion on subject matter or an assertion about the subject matter in relation to an identified set of criteria. In an agreed-upon procedures engagement, the practitioner does not express an opinion but, rather, performs procedures agreed upon by the specified parties and reports the results of those procedures. Examination engagements are performed in accordance with AT-C sections 105 and 205; agreed-upon procedures engagements are performed in accordance with AT-C section 105 and AT-C section 215, *Agreed-Upon Procedures Engagements*.

.21 According to the attestation standards, the criteria used in an attestation engagement should be suitable and available to report users. Attributes of suitable criteria are as follows: [fn 10]

[fn 8] Statement on Standards for Attestation Engagements No. 18, *Attestation Standards: Clarification and Recodification*, is effective for practitioners' reports dated on or after May 1, 2017.

[fn 9] Paragraph .07 of AT-C section 305, *Prospective Financial Information*, prohibits a practitioner from performing a review of internal control; therefore, practitioners may not perform a review engagement in accordance with the attestation standards using the trust services criteria.

[fn 10] Paragraph .25*b* of AT-C section 105, *Concepts Common to All Attestation Engagements*.

- *Relevance*. Criteria are relevant to the subject matter.
- *Objectivity*. Criteria are free from bias.
- *Measurability*. Criteria permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- *Completeness*. Criteria are complete when subject matter prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect decisions of the intended users made on the basis of that subject matter.

.22 In addition to being suitable, AT-C section 105 indicates that the criteria used in an attestation engagement must be available to users. The publication of the trust services criteria makes the criteria available to report users. Accordingly, ASEC has concluded that the trust services criteria are suitable criteria in accordance with the attestation standards.

Consulting Engagements

.23 Sometimes, the trust services criteria may be used in engagements that involve the performance of readiness services, in which a practitioner may assist management with the implementation of one or more new information systems within an organization. [fn 11] Such engagements typically are performed under the consulting standards. In a consulting engagement, the practitioner develops findings and makes recommendations for the consideration and use of management; the practitioner does not form a conclusion about or express an opinion on the subject matter of the engagement. Generally, consulting services are performed only for the use and benefit of the client. Practitioners providing such services follow CS section 100, *Consulting Services: Definitions and Standards*. [fn 12]

Trust Services Criteria

.24 The following table presents the trust services criteria and the related points of focus. In the table, criteria and related points of focus that come directly from the COSO framework are presented using a normal font. In contrast, supplemental criteria and points of focus that apply to engagements using the trust services criteria are presented in *italics*. Finally, criteria and points of focus that apply only when engagements using the trust services criteria are performed at a system level are presented in ***bold italics***.

[fn 11] When a practitioner provides information systems design, implementation, or integration services to an attest client, threats to the practitioner's independence may exist. The "Information Systems Design, Implementation, or Integration" interpretation (ET sec. 1.295.145) of the AICPA Code of Professional Conduct, provides guidance to practitioners on evaluating the effect of such threats to their independence.

All ET sections can be found in AICPA *Professional Standards*.

[fn 12] All CS sections can be found in AICPA *Professional Standards*.

	CONTROL ENVIRONMENT
CC1.1	**COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Sets the Tone at the Top — The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.
	• Establishes Standards of Conduct — The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.
	• Evaluates Adherence to Standards of Conduct — Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.
	• Addresses Deviations in a Timely Manner — Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers Contractors and Vendor Employees in Demonstrating Its Commitment — Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.*
CC1.2	**COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:

	• Establishes Oversight Responsibilities — The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
	• Applies Relevant Expertise — The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.
	• Operates Independently — The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Supplements Board Expertise — The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.*
CC1.3	**COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers All Structures of the Entity — Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.
	• Establishes Reporting Lines — Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.
	• Defines, Assigns, and Limits Authorities and Responsibilities — Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.

	Additional points of focus specifically related to all engagements using the trust services criteria:
	• *Addresses Specific Requirements When Defining Authorities and Responsibilities — Management and the board of directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy when defining authorities and responsibilities.*
	• *Considers Interactions With External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities — Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.*
CC1.4	**COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Establishes Policies and Practices — Policies and practices reflect expectations of competence necessary to support the achievement of objectives.
	• Evaluates Competence and Addresses Shortcomings — The board of directors and management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings.
	• Attracts, Develops, and Retains Individuals — The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.
	• Plans and Prepares for Succession — Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.
	Additional point of focus specifically related to all engagements using the trust services criteria:

	• *Considers the Background of Individuals — The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*
	• *Considers the Technical Competency of Individuals — The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*
	• *Provides Training to Maintain Technical Competencies — The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.*
CC1.5	**COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Enforces Accountability Through Structures, Authorities, and Responsibilities — Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.
	• Establishes Performance Measures, Incentives, and Rewards — Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.
	• Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance — Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.
	• Considers Excessive Pressures — Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.
	• Evaluates Performance and Rewards or Disciplines Individuals — Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and

	provide rewards or exercise disciplinary action, as appropriate.
	COMMUNICATION AND INFORMATION
CC2.1	**COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Identifies Information Requirements — A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.
	• Captures Internal and External Sources of Data — Information systems capture internal and external sources of data.
	• Processes Relevant Data Into Information — Information systems process and transform relevant data into information.
	• Maintains Quality Throughout Processing — Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.
CC2.2	**COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Communicates Internal Control Information — A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.
	• Communicates With the Board of Directors — Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.

	• Provides Separate Communication Lines — Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.
	• Selects Relevant Method of Communication — The method of communication considers the timing, audience, and nature of the information.
	Additional points of focus specifically related to all engagements using the trust services criteria:
	• *Communicates Responsibilities — Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.*
	• *Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters — Entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel.*
	• *Communicates Objectives and Changes to Objectives — The entity communicates its objectives and changes to those objectives to personnel in a timely manner.*
	• *Communicates Information to Improve Security Knowledge and Awareness — The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.*
	Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:
	• ***Communicates Information About System Operation and Boundaries — The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.***
	• ***Communicates System Objectives — The entity communicates its objectives to personnel to enable them to carry out their responsibilities.***

	• ***<u>Communicates System Changes</u> — System changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner.***
CC2.3	**COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• <u>Communicates to External Parties</u> — Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.
	• <u>Enables Inbound Communications</u> — Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.
	• <u>Communicates With the Board of Directors</u> — Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.
	• <u>Provides Separate Communication Lines</u> — Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.
	• <u>Selects Relevant Method of Communication</u> — The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.
	Additional point of focus that applies only to an engagement using the trust services criteria for confidentiality:
	• *<u>Communicates Objectives Related to Confidentiality and Changes to Objectives</u> — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives and changes to objectives related to confidentiality.*

	Additional point of focus that applies only to an engagement using the trust services criteria for privacy:
	• *Communicates Objectives Related to Privacy and Changes to Objectives — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives related to privacy and changes to those objectives.*
	Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:
	• ***Communicates Information About System Operation and Boundaries — The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.***
	• ***Communicates System Objectives — The entity communicates its system objectives to appropriate external users.***
	• ***Communicates System Responsibilities — External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive communications about their responsibilities and have the information necessary to carry out those responsibilities.***
	• ***Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters — External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.***
	RISK ASSESSMENT
CC3.1	**COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	Operations Objectives

	• Reflects Management's Choices — Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.
	• Considers Tolerances for Risk — Management considers the acceptable levels of variation relative to the achievement of operations objectives.
	• Includes Operations and Financial Performance Goals — The organization reflects the desired level of operations and financial performance for the entity within operations objectives.
	• Forms a Basis for Committing of Resources — Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.
	External Financial Reporting Objectives • Complies With Applicable Accounting Standards — Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.
	• Considers Materiality — Management considers materiality in financial statement presentation.
	• Reflects Entity Activities — External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.
	External Nonfinancial Reporting Objectives • Complies With Externally Established Frameworks — Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.
	• Considers the Required Level of Precision — Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.
	• Reflects Entity Activities — External reporting reflects the underlying transactions and events within a range of acceptable limits.
	Internal Reporting Objectives • Reflects Management's Choices — Internal reporting provides management with accurate and complete information regarding management's choices and information

	needed in managing the entity.
	• Considers the Required Level of Precision — Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.
	• Reflects Entity Activities — Internal reporting reflects the underlying transactions and events within a range of acceptable limits.
	Compliance Objectives • Reflects External Laws and Regulations — Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.
	• Considers Tolerances for Risk — Management considers the acceptable levels of variation relative to the achievement of operations objectives.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Establishes Sub-objectives to Support Objectives — Management identifies sub-objectives related to security, availability, processing integrity, confidentiality, and privacy to support the achievement of the entity's objectives related to reporting, operations, and compliance.*
CC3.2	**COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels — The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.
	• Analyzes Internal and External Factors — Risk identification considers both internal and external factors and their impact on the achievement of objectives.
	• Involves Appropriate Levels of Management — The entity puts into place effective

	risk assessment mechanisms that involve appropriate levels of management.
	• Estimates Significance of Risks Identified — Identified risks are analyzed through a process that includes estimating the potential significance of the risk.
	• Determines How to Respond to Risks — Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.
	Additional points of focus specifically related to all engagements using the trust services criteria:
	• *Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities — The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.*
	• *Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties — The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.*
	• *Considers the Significance of the Risk — The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.*
CC3.3	**COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers Various Types of Fraud — The assessment of fraud considers fraudulent

	reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.
	• Assesses Incentives and Pressures — The assessment of fraud risks considers incentives and pressures.
	• Assesses Opportunities — The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.
	• Assesses Attitudes and Rationalizations — The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers the Risks Related to the Use of IT and Access to Information — The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.*
CC3.4	**COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Assesses Changes in the External Environment — The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.
	• Assesses Changes in the Business Model — The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.
	• Assesses Changes in Leadership — The entity considers changes in management and respective attitudes and philosophies on the system of internal control.

	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Assesses Changes in Systems and Technology — The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.*
	• *Assesses Changes in Vendor and Business Partner Relationships — The risk identification process considers changes in vendor and business partner relationships.*
	MONITORING ACTIVITIES
CC4.1	**COSO Principle 16*:* The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers a Mix of Ongoing and Separate Evaluations — Management includes a balance of ongoing and separate evaluations.
	• Considers Rate of Change — Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.
	• Establishes Baseline Understanding — The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.
	• Uses Knowledgeable Personnel — Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.
	• Integrates With Business Processes — Ongoing evaluations are built into the business processes and adjust to changing conditions.
	• Adjusts Scope and Frequency — Management varies the scope and frequency of separate evaluations depending on risk.

	• Objectively Evaluates — Separate evaluations are performed periodically to provide objective feedback.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers Different Types of Ongoing and Separate Evaluations — Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.*
CC4.2	**COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Assesses Results — Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.
	• Communicates Deficiencies — Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.
	• Monitors Corrective Action — Management tracks whether deficiencies are remedied on a timely basis.
	CONTROL ACTIVITIES
CC5.1	**COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Integrates With Risk Assessment — Control activities help ensure that risk responses that address and mitigate risks are carried out.

	• Considers Entity-Specific Factors — Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.
	• Determines Relevant Business Processes — Management determines which relevant business processes require control activities.
	• Evaluates a Mix of Control Activity Types — Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.
	• Considers at What Level Activities Are Applied — Management considers control activities at various levels in the entity.
	• Addresses Segregation of Duties — Management segregates incompatible duties and, where such segregation is not practical, management selects and develops alternative control activities.
CC5.2	**COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls — Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.
	• Establishes Relevant Technology Infrastructure Control Activities — Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.
	• Establishes Relevant Security Management Process Controls Activities — Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.
	• Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities — Management selects and develops control activities over

	the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.
CC5.3	**COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Establishes Policies and Procedures to Support Deployment of Management's Directives — Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.
	• Establishes Responsibility and Accountability for Executing Policies and Procedures — Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.
	• Performs in a Timely Manner — Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.
	• Takes Corrective Action — Responsible personnel investigate and act on matters identified as a result of executing control activities.
	• Performs Using Competent Personnel — Competent personnel with sufficient authority perform control activities with diligence and continuing focus.
	• Reassesses Policies and Procedures — Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.
	Logical and Physical Access Controls
CC6.1	***The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Identifies and Manages the Inventory of Information Assets — The entity identifies,*

	inventories, classifies, and manages information assets.
	• *Restricts Logical Access — Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.*
	• *Identifies and Authenticates Users — Persons, infrastructure, and software are identified and authenticated prior to accessing information assets, whether locally or remotely.*
	• *Considers Network Segmentation — Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.*
	• *Manages Points of Access — Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.*
	• *Restricts Access to Information Assets — Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access-control rules for information assets.*
	• *Manages Identification and Authentication — Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure, and software.*
	• *Manages Credentials for Infrastructure and Software — New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.*
	• *Uses Encryption to Protect Data — The entity uses encryption to supplement other measures used to protect data at rest, when such protections are deemed appropriate based on assessed risk.*
	• *Protects Encryption Keys — Processes are in place to protect encryption keys during generation, storage, use, and destruction.*
CC6.2	***Prior to issuing system credentials and granting system access, the entity registers and authorizes***

	new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Controls Access Credentials to Protected Assets — Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.*
	• *Removes Access to Protected Assets When Appropriate — Processes are in place to remove credential access when an individual no longer requires such access.*
	• *Reviews Appropriateness of Access Credentials — The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.*
CC6.3	***The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Creates or Modifies Access to Protected Information Assets — Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.*
	• *Removes Access to Protected Information Assets — Processes are in place to remove access to protected information assets when an individual no longer requires access.*
	• *Uses Role-Based Access Controls — Role-based access control is utilized to support segregation of incompatible functions.*
	• *Reviews Access Roles and Rules — The appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals with access and access rules are modified as appropriate.*

CC6.4	***The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Creates or Modifies Physical Access — Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner.*
	• *Removes Physical Access — Processes are in place to remove access to physical resources when an individual no longer requires access.*
	• *Reviews Physical Access — Processes are in place to periodically review physical access to ensure consistency with job responsibilities.*
CC6.5	***The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Identifies Data and Software for Disposal — Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.*
	• *Removes Data and Software From Entity Control — Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.*
CC6.6	***The entity implements logical access security measures to protect against threats from sources outside its system boundaries.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restricts Access — The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.*

	• *Protects Identification and Authentication Credentials — Identification and authentication credentials are protected during transmission outside its system boundaries.*
	• *Requires Additional Authentication or Credentials — Additional authentication information or credentials are required when accessing the system from outside its boundaries.*
	• *Implements Boundary Protection Systems — Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.*
CC6.7	***The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restricts the Ability to Perform Transmission — Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement, and removal of information.*
	• *Uses Encryption Technologies or Secure Communication Channels to Protect Data — Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.*
	• *Protects Removal Media — Encryption technologies and physical asset protections are used for removable media (such as USB drives and backup tapes), as appropriate.*
	• *Protects Mobile Devices — Processes are in place to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets.*
CC6.8	***The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:

	• *Restricts Application and Software Installation — The ability to install applications and software is restricted to authorized individuals.*
	• *Detects Unauthorized Changes to Software and Configuration Parameters — Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.*
	• *Uses a Defined Change Control Process — A management-defined change control process is used for the implementation of software.*
	• *Uses Antivirus and Anti-Malware Software — Antivirus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.*
	• *Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software — Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.*
	System Operations
CC7.1	***To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Uses Defined Configuration Standards — Management has defined configuration standards.*
	• *Monitors Infrastructure and Software — The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.*
	• *Implements Change-Detection Mechanisms — The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.*
	• *Detects Unknown or Unauthorized Components — Procedures are in place to de-*

	tect the introduction of unknown or unauthorized components.
	• *Conducts Vulnerability Scans — The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.*
CC7.2	***The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Implements Detection Policies, Procedures, and Tools — Detection policies and procedures are defined and implemented and detection tools are implemented on infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.*
	• *Designs Detection Measures — Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.*
	• *Implements Filters to Analyze Anomalies — Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.*
	• *Monitors Detection Tools for Effective Operation — Management has implemented processes to monitor the effectiveness of detection tools.*
CC7.3	***The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:

	• *Responds to Security Incidents — Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.*
	• *Communicates and Reviews Detected Security Events — Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.*
	• *Develops and Implements Procedures to Analyze Security Incidents — Procedures are in place to analyze security incidents and determine system impact.*
	Additional points of focus that apply only in an engagement using the trust services criteria for privacy:
	• *Assesses the Impact on Personal Information — Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations.*
	• *Determines Personal Information Used or Disclosed — When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.*
CC7.4	***The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Assigns Roles and Responsibilities — Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.*
	• *Contains Security Incidents — Procedures are in place to contain security incidents that actively threaten entity objectives.*
	• *Mitigates Ongoing Security Incidents — Procedures are in place to mitigate the effects of ongoing security incidents.*

	• *Ends Threats Posed by Security Incidents — Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.*
	• *Restores Operations — Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.*
	• *Develops and Implements Communication Protocols for Security Incidents — Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.*
	• *Obtains Understanding of Nature of Incident and Determines Containment Strategy — An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.*
	• *Remediates Identified Vulnerabilities — Identified vulnerabilities are remediated through the development and execution of remediation activities.*
	• *Communicates Remediation Activities — Remediation activities are documented and communicated in accordance with the incident-response program.*
	• *Evaluates the Effectiveness of Incident Response — The design of incident-response activities is evaluated for effectiveness on a periodic basis.*
	• *Periodically Evaluates Incidents — Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.*
	Additional points of focus that apply only in an engagement using the trust services criteria for privacy:
	• *Communicates Unauthorized Use and Disclosure — Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.*
	• *Application of Sanctions — The conduct of individuals and organizations operating under the authority of the entity and involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, sanctioned in accordance*

	with entity policies and legal and regulatory requirements.
CC7.5	***The entity identifies, develops, and implements activities to recover from identified security incidents.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restores the Affected Environment — The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.*
	• *Communicates Information About the Event — Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).*
	• *Determines Root Cause of the Event — The root cause of the event is determined.*
	• *Implements Changes to Prevent and Detect Recurrences — Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.*
	• *Improves Response and Recovery Procedures — Lessons learned are analyzed and the incident-response plan and recovery procedures are improved.*
	• *Implements Incident-Recovery Plan Testing — Incident-recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.*
	Change Management
CC8.1	***The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:

	• *Manages Changes Throughout the System Life Cycle — A process for managing system changes throughout the life cycle of the system and its components (infrastructure, data, software, and procedures) is used to support system availability and processing integrity.*
	• *Authorizes Changes — A process is in place to authorize system changes prior to development.*
	• *Designs and Develops Changes — A process is in place to design and develop system changes.*
	• *Documents Changes — A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.*
	• *Tracks System Changes — A process is in place to track system changes prior to implementation.*
	• *Configures Software — A process is in place to select and implement the configuration parameters used to control the functionality of software.*
	• *Tests System Changes — A process is in place to test system changes prior to implementation.*
	• *Approves System Changes — A process is in place to approve system changes prior to implementation.*
	• *Deploys System Changes — A process is in place to implement system changes.*
	• *Identifies and Evaluates System Changes — Objectives affected by system changes are identified and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.*
	• *Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents — Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified and the change process is initiated upon identification.*
	• *Creates Baseline Configuration of IT Technology — A baseline configuration of IT*

	and control systems is created and maintained.
	• *Provides for Changes Necessary in Emergency Situations — A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent time frame).*
	Additional points of focus that apply only in an engagement using the trust services criteria for confidentiality:
	• *Protects Confidential Information — The entity protects confidential information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to confidentiality.*
	Additional points of focus that apply only in an engagement using the trust services criteria for privacy:
	• *Protects Personal Information — The entity protects personal information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to privacy.*
	Risk Mitigation
CC9.1	***The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Considers Mitigation of Risks of Business Disruption — Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes, information, and communications to meet the entity's objectives during response, mitigation, and recovery efforts.*
	• *Considers the Use of Insurance to Mitigate Financial Impact Risks — The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.*

CC9.2	***The entity assesses and manages risks associated with vendors and business partners.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Establishes Requirements for Vendor and Business Partner Engagements — The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.*
	• *Assesses Vendor and Business Partner Risks — The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.*
	• *Assigns Responsibility and Accountability for Managing Vendors and Business Partners — The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners.*
	• *Establishes Communication Protocols for Vendors and Business Partners — The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.*
	• *Establishes Exception Handling Procedures From Vendors and Business Partners — The entity establishes exception handling procedures for service or product issues related to vendors and business partners.*
	• *Assesses Vendor and Business Partner Performance — The entity periodically assesses the performance of vendors and business partners.*
	• *Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments — The entity implements procedures for addressing issues identified with vendor and business partner relationships.*
	• *Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships.*
	Additional points of focus that apply only to an engagement using the trust services criteria for confidentiality:

	• *Obtains Confidentiality Commitments from Vendors and Business Partners — The entity obtains confidentiality commitments that are consistent with the entity's confidentiality commitments and requirements from vendors and business partners who have access to confidential information.*
	• *Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements.*
	Additional points of focus that apply only to an engagement using the trust services criteria for privacy:
	• *Obtains Privacy Commitments from Vendors and Business Partners — The entity obtains privacy commitments, consistent with the entity's privacy commitments and requirements, from vendors and business partners who have access to personal information.*
	• *Assesses Compliance with Privacy Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and takes corrective action as necessary.*
	ADDITIONAL CRITERIA FOR AVAILABILITY
A1.1	***The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for availability, highlight important characteristics relating to this criterion:
	• *Measures Current Usage — The use of the system components is measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.*
	• *Forecasts Capacity — The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.*
	• *Makes Changes Based on Forecasts — The system change management process is*

	initiated when forecasted usage exceeds capacity tolerances.
A1.2	***The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services availability criteria, highlight important characteristics relating to this criterion:
	• *Identifies Environmental Threats — As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.*
	• *Designs Detection Measures — Detection measures are implemented to identify anomalies that could result from environmental threat events.*
	• *Implements and Maintains Environmental Protection Mechanisms — Management implements and maintains environmental protection mechanisms to prevent and mitigate environmental events.*
	• *Implements Alerts to Analyze Anomalies — Management implements alerts that are communicated to personnel for analysis to identify environmental threat events.*
	• *Responds to Environmental Threat Events — Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator backup subsystem).*
	• *Communicates and Reviews Detected Environmental Threat Events — Detected environmental threat events are communicated to and reviewed by the individuals responsible for the management of the system and actions are taken, if necessary.*
	• *Determines Data Requiring Backup — Data is evaluated to determine whether backup is required.*
	• *Performs Data Backup — Procedures are in place for backing up data, monitoring to detect backup failures, and initiating corrective action when such failures occur.*
	• *Addresses Offsite Storage — Backup data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environ-*

	mental threat event affecting both sets of data is reduced to an appropriate level.
	• *Implements Alternate Processing Infrastructure — Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable.*
A1.3	***The entity tests recovery plan procedures supporting system recovery to meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for availability, highlight important characteristics relating to this criterion:
	• *Implements Business Continuity Plan Testing — Business continuity plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.*
	• *Tests Integrity and Completeness of Backup Data — The integrity and completeness of backup information is tested on a periodic basis.*
	ADDITIONAL CRITERIA FOR CONFIDENTIALITY
C1.1	***The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.***
	The following points of focus, which apply only to an engagement using the trust services criteria for confidentiality, highlight important characteristics relating to this criterion:
	• *Identifies Confidential information — Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.*
	• *Protects Confidential Information From Destruction — Procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.*
C1.2	***The entity disposes of confidential information to meet the entity's objectives related to confidentiality.***

	The following points of focus, which apply only to an engagement using the trust services criteria for confidentiality, highlight important characteristics relating to this criterion:
	• *Identifies Confidential Information for Destruction — Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.*
	• *Destroys Confidential Information — Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.*
	ADDITIONAL CRITERIA FOR PROCESSING INTEGRITY (OVER THE PROVISION OF SERVICES OR THE PRODUCTION, MANUFACTURING, OR DISTRIBUTION OF GOODS)
PI1.1	***The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Identifies Information Specifications — The entity identifies information specifications required to support the use of products and services.*
	• *Defines Data Necessary to Support a Product or Service — When data is provided as part of a service or product or as part of a reporting obligation related to a product or service:* 1. *The definition of the data is available to the users of the data* 2. *The definition of the data includes the following information:* *a. The population of events or instances included in the data* *b. The nature of each element (for example, field) of the data (that is, the event or instance to which the data element relates, for example, transaction price of a sale of XYZ Corporation stock for the last trade in that stock on a given day)* *c. Source(s) of the data* *d. The unit(s) of measurement of data elements (for example, fields)* *e. The accuracy/correctness/precision of measurement* *f. The uncertainty or confidence interval inherent in each data element and in the population of those elements* *g. The date the data was observed or the period of time during which the events relevant to the data occurred* *h. The factors in addition to the date and period of time used to determine the inclusion and exclusion of items in the data elements*

	and population 3. *The definition is complete and accurate.* 4. *The description of the data identifies any information that is necessary to understand each data element and the population in a manner consistent with its definition and intended purpose (metadata) that has not been included within the data.*
	The following point of focus, which applies only to an engagement using the trust services criteria for processing integrity for a system that produces, manufactures, or distributes products, highlights important characteristics relating to this criterion:
	• *Defines Information Necessary to Support the Use of a Good or Product — When information provided by the entity is needed to use the good or product in accordance with its specifications:* 1. *The required information is available to the user of the good or product.* 2. *The required information is clearly identifiable.* 3. *The required information is validated for completeness and accuracy.*
PI1.2	***The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Defines Characteristics of Processing Inputs — The characteristics of processing inputs that are necessary to meet requirements are defined.*
	• *Evaluates Processing Inputs — Processing inputs are evaluated for compliance with defined input requirements.*
	• *Creates and Maintains Records of System Inputs — Records of system input activities are created and maintained completely and accurately in a timely manner.*
PI1.3	***The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Defines Processing Specifications — The processing specifications that are necessary to meet product or service requirements are defined.*

	• *Defines Processing Activities — Processing activities are defined to result in products or services that meet specifications.*
	• *Detects and Corrects Production Errors — Errors in the production process are detected and corrected in a timely manner.*
	• *Records System Processing Activities — System processing activities are recorded completely and accurately in a timely manner.*
	• *Processes Inputs — Inputs are processed completely, accurately, and timely as authorized in accordance with defined processing activities.*
PI1.4	***The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:
	• *Protects Output — Output is protected when stored or delivered, or both, to prevent theft, destruction, corruption, or deterioration that would prevent output from meeting specifications.*
	• *Distributes Output Only to Intended Parties — Output is distributed or made available only to intended parties.*
	• *Distributes Output Completely and Accurately — Procedures are in place to provide for the completeness, accuracy, and timeliness of distributed output.*
	• *Creates and Maintains Records of System Output Activities — Records of system output activities are created and maintained completely and accurately in a timely manner.*
PI1.5	***The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for processing integrity, highlight important characteristics relating to this criterion:

	• *Protects Stored Items — Stored items are protected to prevent theft, corruption, destruction, or deterioration that would prevent output from meeting specifications.*
	• *Archives and Protects System Records — System records are archived and archives are protected against theft, corruption, destruction, or deterioration that would prevent them from being used.*
	• *Stores Data Completely and Accurately — Procedures are in place to provide for the complete, accurate, and timely storage of data.*
	• *Creates and Maintains Records of System Storage Activities — Records of system storage activities are created and maintained completely and accurately in a timely manner.*
	ADDITIONAL CRITERIA FOR PRIVACY
P1.0	**Privacy Criteria Related to Notice and Communication of Objectives Related to Privacy**
P1.1	***The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates to Data Subjects — Notice is provided to data subjects regarding the following:* — *Purpose for collecting personal information* — *Choice and consent* — *Types of personal information collected* — *Methods of collection (for example, use of cookies or other tracking techniques)* — *Use, retention, and disposal* — *Access* — *Disclosure to third parties* — *Security for privacy*

	— *Quality, including data subjects' responsibilities for quality* — *Monitoring and enforcement* *If personal information is collected from sources other than the individual, such sources are described in the privacy notice.*
	• <u>*Provides Notice to Data Subjects*</u> *— Notice is provided to data subjects (1) at or before the time personal information is collected or as soon as practical thereafter, (2) at or before the entity changes its privacy notice or as soon as practical thereafter, or (3) before personal information is used for new purposes not previously identified.*
	• <u>*Covers Entities and Activities in Notice*</u> *— An objective description of the entities and activities covered is included in the entity's privacy notice.*
	• <u>*Uses Clear and Conspicuous Language*</u> *— The entity's privacy notice is conspicuous and uses clear language.*
P2.0	**Privacy Criteria Related to Choice and Consent**
P2.1	***The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• <u>*Communicates to Data Subjects*</u> *— Data subjects are informed (a) about the choices available to them with respect to the collection, use, and disclosure of personal information and (b) that implicit or explicit consent is required to collect, use, and disclose personal information, unless a law or regulation specifically requires or allows otherwise.*
	• <u>*Communicates Consequences of Denying or Withdrawing Consent*</u> *— When personal information is collected, data subjects are informed of the consequences of refusing to provide personal information or denying or withdrawing consent to use personal information for purposes identified in the notice.*
	• <u>*Obtains Implicit or Explicit Consent*</u> *— Implicit or explicit consent is obtained from data subjects at or before the time personal information is collected or soon there-*

	after. The individual's preferences expressed in his or her consent are confirmed and implemented.
	• *Documents and Obtains Consent for New Purposes and Uses — If information that was previously collected is to be used for purposes not previously identified in the privacy notice, the new purpose is documented, the data subject is notified, and implicit or explicit consent is obtained prior to such new use or purpose.*
	• *Obtains Explicit Consent for Sensitive Information — Explicit consent is obtained directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.*
	• *Obtains Consent for Data Transfers — Consent is obtained before personal information is transferred to or from an individual's computer or other similar device.*
P3.0	**Privacy Criteria Related to Collection**
P3.1	***Personal information is collected consistent with the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Limits the Collection of Personal Information — The collection of personal information is limited to that necessary to meet the entity's objectives.*
	• *Collects Information by Fair and Lawful Means — Methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information.*
	• *Collects Information From Reliable Sources — Management confirms that third parties from whom personal information is collected (that is, sources other than the individual) are reliable sources that collect information fairly and lawfully.*
	• *Informs Data Subjects When Additional Information Is Acquired — Data subjects are informed if the entity develops or acquires additional information about them for its use.*
P3.2	***For information requiring explicit consent, the entity communicates the need for such consent as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives re-***

	lated to privacy.
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Obtains Explicit Consent for Sensitive Information — Explicit consent is obtained directly from the data subject when sensitive personal information is collected, used, or disclosed, unless a law or regulation specifically requires otherwise.*
	• *Documents Explicit Consent to Retain Information — Documentation of explicit consent for the collection, use, or disclosure of sensitive personal information is retained in accordance with objectives related to privacy.*
P4.0	**Privacy Criteria Related to Use, Retention, and Disposal**
P4.1	***The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy.***
	The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Uses Personal Information for Intended Purposes — Personal information is used only for the intended purposes for which it was collected and only when implicit or explicit consent has been obtained, unless a law or regulation specifically requires otherwise.*
P4.2	***The entity retains personal information consistent with the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Retains Personal Information — Personal information is retained for no longer than necessary to fulfill the stated purposes, unless a law or regulation specifically requires otherwise.*
	• *Protects Personal Information — Policies and procedures have been implemented to protect personal information from erasure or destruction during the specified retention period of the information.*
P4.3	***The entity securely disposes of personal information to meet the entity's objectives related to privacy.***

	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Captures, Identifies, and Flags Requests for Deletion — Requests for deletion of personal information are captured and information related to the requests is identified and flagged for destruction to meet the entity's objectives related to privacy.*
	• *Disposes of, Destroys, and Redacts Personal Information — Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.*
	• *Destroys Personal Information — Policies and procedures are implemented to erase or otherwise destroy personal information that has been identified for destruction.*
P5.0	**Privacy Criteria Related to Access**
P5.1	***The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Authenticates Data Subjects' Identity — The identity of data subjects who request access to their personal information is authenticated before they are given access to that information.*
	• *Permits Data Subjects Access to Their Personal Information — Data subjects are able to determine whether the entity maintains personal information about them and, upon request, may obtain access to their personal information.*
	• *Provides Understandable Personal Information Within Reasonable Time — Personal information is provided to data subjects in an understandable form, in a reasonable time frame, and at a reasonable cost, if any.*
	• *Informs Data Subjects If Access Is Denied — When data subjects are denied access to their personal information, the entity informs them of the denial and the reason for the denial in a timely manner, unless prohibited by law or regulation.*

P5.2	***The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates Denial of Access Requests — Data subjects are informed, in writing, of the reason a request for access to their personal information was denied, the source of the entity's legal right to deny such access, if applicable, and the individual's right, if any, to challenge such denial, as specifically permitted or required by law or regulation.*
	• *Permits Data Subjects to Update or Correct Personal Information — Data subjects are able to update or correct personal information held by the entity. The entity provides such updated or corrected information to third parties that were previously provided with the data subject's personal information consistent with the entity's objectives related to privacy.*
	• *Communicates Denial of Correction Requests — Data subjects are informed, in writing, about the reason a request for correction of personal information was denied and how they may appeal.*
P6.0	**Privacy Criteria Related to Disclosure and Notification**
P6.1	***The entity discloses personal information to third parties with the explicit consent of data subjects and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates Privacy Policies to Third Parties — Privacy policies or other specific instructions or requirements for handling personal information are communicated to third parties to whom personal information is disclosed.*
	• *Discloses Personal Information Only When Appropriate — Personal information is disclosed to third parties only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject, unless a law or regulation specifically requires otherwise.*
	• *Discloses Personal Information Only to Appropriate Third Parties — Personal information is disclosed only to third parties who have agreements with the entity to*

	protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet the terms of the agreement, instructions, or requirements.
	• *Discloses Information to Third Parties for New Purposes and Uses — Personal information is disclosed to third parties for new purposes or uses only with the prior implicit or explicit consent of data subjects.*
P6.2	***The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy.***
	The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlights important characteristics relating to this criterion:
	• *Creates and Retains Record of Authorized Disclosures — The entity creates and maintains a record of authorized disclosures of personal information that is complete, accurate, and timely.*
P6.3	***The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy.***
	The following point of focus, which applies only to an engagement using the trust services criteria for privacy, highlights important characteristics relating to this criterion:
	• *Creates and Retains Record of Detected or Reported Unauthorized Disclosures — The entity creates and maintains a record of detected or reported unauthorized disclosures of personal information that is complete, accurate, and timely.*
P6.4	***The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Discloses Personal Information Only to Appropriate Third Parties — Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of the entity's privacy notice or other specific instructions or requirements. The entity has procedures in place to evaluate that the third parties have effective controls to meet*

	the terms of the agreement, instructions, or requirements.
	• *Remediates Misuse of Personal Information by a Third Party — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.*
P6.5	***The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident-response procedures to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Remediates Misuse of Personal Information by a Third Party — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.*
	• *Reports Actual or Suspected Unauthorized Disclosures — A process exists for obtaining commitments from vendors and other third parties to report to the entity actual or suspected unauthorized disclosures of personal information.*
P6.6	***The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Remediates Misuse of Personal Information by a Third Party — The entity takes remedial action in response to misuse of personal information by a third party to whom the entity has transferred such information.*
	• *Provides Notice of Breaches and Incidents — The entity has a process for providing notice of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy.*
P6.7	***The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.***

	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Identifies Types of Personal Information and Handling Process — The types of personal information and sensitive personal information and the related processes, systems, and third parties involved in the handling of such information are identified.*
	• *Captures, Identifies, and Communicates Requests for Information — Requests for an accounting of personal information held and disclosures of the data subjects' personal information are captured and information related to the requests is identified and communicated to data subjects to meet the entity's objectives related to privacy.*
P7.0	**Privacy Criteria Related to Quality**
P7.1	***The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Ensures Accuracy and Completeness of Personal Information — Personal information is accurate and complete for the purposes for which it is to be used.*
	• *Ensures Relevance of Personal Information — Personal information is relevant to the purposes for which it is to be used.*
P8.0	**Privacy Criteria Related to Monitoring and Enforcement**
P8.1	***The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner.***
	The following points of focus, which apply only to an engagement using the trust services criteria for privacy, highlight important characteristics relating to this criterion:
	• *Communicates to Data Subjects — Data subjects are informed about how to contact the entity with inquiries, complaints, and disputes.*
	• *Addresses Inquiries, Complaints, and Disputes — A process is in place to address*

	inquiries, complaints, and disputes.
	• *Documents and Communicates Dispute Resolution and Recourse — Each complaint is addressed and the resolution is documented and communicated to the individual.*
	• *Documents and Reports Compliance Review Results — Compliance with objectives related to privacy are reviewed and documented and the results of such reviews are reported to management. If problems are identified, remediation plans are developed and implemented.*
	• *Documents and Reports Instances of Noncompliance — Instances of noncompliance with objectives related to privacy are documented and reported and, if needed, corrective and disciplinary measures are taken on a timely basis.*
	• *Performs Ongoing Monitoring — Ongoing procedures are performed for monitoring the effectiveness of controls over personal information and for taking timely corrective actions when necessary.*

Appendix A — Glossary

.25

access to personal information. The ability to view personal information held by an organization. This ability may be complemented by an ability to update or correct the information. Access defines the intersection of identity and data, that is, who can do what to which data. Access is one of the fair information practice principles. Individuals need to be able to find out what personal information an entity has on file about them and how the information is being used. Individuals need to be able to correct erroneous information in such records.

architecture. The design of the structure of a system, including logical components, and the logical interrelationships of a computer, its operating system, a network, or other elements.

authentication. The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device) or to verify the source and integrity of data.

authorization. The process of granting access privileges to a user, program, or process by a person that has the authority to grant such access.

board or **board of directors.** Individuals with responsibility for overseeing the strategic direction of the entity and the obligations related to the accountability of the entity. Depending on the nature of the entity, such responsibilities may be held by a board of directors or supervisory board for a corporation, a board of trustees for a not-for-profit entity, a board of governors or commissioners for a government entity, general partners for a partnership, or an owner for a small business.

business partner. An individual or business (and its employees), other than a vendor, that has some degree of involvement with the entity's business dealings or agrees to cooperate, to any degree, with the entity (for example, a computer manufacturer who works with another company who supplies it with parts).

collection. The process of obtaining personal information from the individual directly (for example, through the individual's submission of an internet form or a registration form) or from another party such as a business partner.

commitments. Declarations made by management to customers regarding the performance of one or more systems that provide services or products. Commitments can be communicated in written individualized agreements, standardized contracts, service level agreements, or published statements (for example, a security practices statement). A commitment may relate to one or more trust services categories. Commitments may be made on many different aspects of the service being provided or the product, production, manufacturing, or distribution specifications.

component. One of five elements of internal control, including the control environment, risk assessment, control activities, information and communication, and monitoring activities.

compromise. Refers to a loss of confidentiality, integrity, or availability of information, including any resultant impairment of (1) processing integrity or availability of systems or (2) the integrity or availability of system inputs or outputs.

controls. Policies and procedures that are part of the entity's system of internal control. The objective of an entity's system of internal control is to provide reasonable assurance that principal system objectives are achieved.

control activity. An action established through policies and procedures that help ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

consent. This privacy requirement is one of the fair information practice objectives. Individuals must be able to prevent the collection of their personal data, unless legally required. If an individual has a choice about the use or disclosure of his or her information, consent is the individual's way of giving permission for the use or disclosure. Consent may be affirmative (for example, opting in) or implied (for example, not opting out). There are two types of consent:

- **explicit consent.** A requirement that an individual "signifies" his or her agreement with a data controller by some active communication between the parties.

- **implied consent.** When consent may reasonably be inferred from the action or inaction of the individual.

COSO. The Committee of Sponsoring Organizations of the Treadway Commission. COSO is a joint initiative of five private-sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence. (See www.coso.org.)

criteria. The benchmarks used to measure or evaluate the subject matter.

cybersecurity objectives. Objectives that address the cybersecurity risks that could affect the achievement of the entity's overall business objectives (including compliance, reporting, and operational objectives).

design. As used in the COSO definition of internal control, the internal control system design is intended to provide reasonable assurance of the achievement of an entity's objectives.

data subject. The individual about whom personal information is collected.

disclosure. The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information. Disclosure is often used interchangeably with the terms *sharing* and *onward transfer*.

disposal. A phase of the data life cycle that pertains to how an entity removes or destroys data or information.

effectiveness (of controls). Encompasses both the suitability of the design of controls and the operating effectiveness of controls to provide reasonable assurance that the entity's principal system objectives are achieved.

entity. A legal entity or management operating model of any size established for a particular purpose. A legal entity may, for example, be a business enterprise, a not-for-profit organization, a government body, or an academic institution. The management operating model may follow product or service lines, divisions, or operating units, with geographic markets providing for further subdivisions or aggregations of performance.

entity-wide. Activities that apply across the entity — most commonly in relation to entity-wide controls.

environmental. Of or having to do with the matters that can damage the physical elements of information systems (for example, fire, flood, wind, earthquake, power surges, or power outages). An entity implements controls and other activities to detect, prevent, and manage the risk of casualty damage to the physical elements of the information system from environmental elements.

external users. Users, other than entity personnel, who are authorized by entity management, customers, or other authorized persons to interact with the entity's information system.

information and systems. Refers to information in electronic form (electronic information) during its use, processing, transmission, and storage and systems that use, process, transmit or transfer, and store information or that produce, manufacture, or distribute products.

information assets. Data and the associated software and infrastructure used to process, transmit, and store information or to produce, manufacture, or distribute products.

infrastructure. The collection of physical or virtual resources that supports an overall IT environment, including the server, storage, and network elements.

internal control. A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

outsourced service providers. A service provider that performs business processes, operations, or controls on behalf of the entity when such business processes, operations, or controls are necessary to achieve the entity's objectives.

personal information. Information that is or can be about or related to an identifiable individual.

policies. Management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the bases for procedures.

practitioner. As used in this document, a CPA who performs an examination of controls within an entity's system relevant to security, availability, processing integrity, confidentiality, or privacy.

principal system objectives. System objectives that relate to the trust services category or categories addressed by the examination and that could reasonably be expected to influence the relevant decisions of intended users. (See *system objectives*.)

privacy commitments. Declarations made by management regarding the performance of a system processing personal information. Such commitments can be communicated in written agreements, standardized contracts, service level agreements, or published statements (for example, a privacy practices statement). In addition, privacy commitments may be made on many different aspects of the service being provided.

privacy notice. A written communication by entities that collect personal information, to the individuals about whom personal information is collected, about the entity's (*a*) policies regarding the nature of the information that they will collect and how that information will be used, retained, disclosed, and disposed of or anonymized and (*b*) commitment to adhere to those policies. A privacy notice also includes information about such matters as the purpose of collecting the information, the choices that individuals have related to their personal information, the security of such information, and how individuals can contact the entity with inquiries, complaints, and disputes related to their personal information. When a user entity collects personal information from individuals, it typically provides a privacy notice to those individuals.

products. Tangible or intangible goods manufactured or produced by an entity. Throughout this document, the term is used interchangeably with *goods.*

report users. Intended users of the practitioner's report in accordance with AT-C section 205, *Examination Engagements*. [fn 1] There may be a broad range of report users for a general-purpose report but only a limited number of specified parties for a report that is restricted in accordance with paragraph .64 of AT-C section 205.

retention. A phase of the data life cycle that pertains to how long an entity stores information for future use or reference.

[fn 1] All AT-C sections can be found in AICPA *Professional Standards*.

risk. The possibility that an event will occur and adversely affect the achievement of objectives.

risk response. The decision to accept, avoid, reduce, or share a risk.

security event. An occurrence, arising from actual or attempted unauthorized access or use by internal or external parties, that impairs or could impair the availability, integrity, or confidentiality of information or systems, result in unauthorized disclosure or theft of information or other assets, or cause damage to systems.

security incident. A security event that requires action on the part of an entity in order to protect information assets and resources.

senior management. The chief executive officer or equivalent organizational leader and senior management team.

service provider. A supplier (such as a service organization) engaged to provide services to the entity. Service providers include outsourced service providers as well as suppliers that provide services not associated with business functions, such as janitorial, legal, and audit services.

SOC 2 engagement. An examination engagement to report on the fairness of the presentation of management's description of the service organization's system, the suitability of the design of the controls included in the description, and, in a type 2 engagement, the operating effectiveness of those controls. This engagement is performed in accordance with the attestation standards and AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy*.

SOC 3 engagement. An examination engagement to report on the suitability of design and the operating effectiveness of an entity's controls over a system relevant to one or more of the trust services categories.

SOC for Cybersecurity examination. An examination engagement to report on whether (*a*) management's description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and (*b*) the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria. A SOC for Cybersecurity examination is performed in accordance with the attestation standards and AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*.

SOC for Supply Chain examination. An examination engagement to report on whether (*a*) the description of the entity's system is presented in accordance with the description criteria and (*b*) the controls stated in the description, which are necessary to provide reasonable assurance that the entity achieved its principal system objectives, were effective based on the applicable trust services criteria. Such an examination is based on guidance contained in AICPA Guide *SOC for Supply Chain: Reporting on an Examination of Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy in a Production, Manufacturing, or Distribution System*.

stakeholders. Parties that are affected by the entity, such as shareholders, the communities in which an entity operates, employees, customers, and suppliers.

subsequent events. Events or transactions that occur after the specified period addressed by the description but prior to the date of the practitioner's report; such events or transactions could have a significant effect on the evaluation of whether the description is presented in accordance with the description criteria or whether controls were effective to provide reasonable assurance that the entity's principal system objectives were achieved based on the applicable trust services criteria.

supplier. See definition for *vendor*.

system. Refers to the infrastructure, software, people, processes, and data that are designed, implemented, and operated to work together to achieve one or more specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements.

system boundaries. The specific aspects of an entity's infrastructure, software, people, procedures, and data necessary to perform a function (such as producing, manufacturing, or distributing a product) or provide a service. When systems for multiple functions or services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap but the boundaries of each system will differ.

system components. Refers to the individual elements of a system. System components can be classified into the following five categories: infrastructure, software, people, processes, and data.

system event. An occurrence that could lead to the loss of, or disruption to, operations, services, or functions and could result in an entity's failure to achieve its system objectives. Such an occurrence may arise from actual or attempted unauthorized access or use by internal or external parties and (*a*) impair (or potentially impair) the availability, integrity, or confidentiality of information or systems; (*b*) result in unauthorized disclosure or theft of information or other assets or the destruction or corruption of data; or (*c*) cause damage to systems. Such occurrences also may arise from the failure of the system to process data as designed or from the loss, corruption, or destruction of data used by the system.

system incident. A system event that requires action on the part of entity management to prevent or reduce the impact of a system event on the entity's achievement of its system objectives.

system objectives. The entity's objectives, established by entity management, that are embodied in the product commitments it makes to customers, including producing or manufacturing a product that meets product performance specifications and other production, manufacturing, or distribution specifications. The system objectives also include the requirements established for the functioning of the system to meet production, manufacturing, or distribution commitments.

system requirements. Specifications regarding how the system should function to (*a*) meet the entity's commitments to customers and others (such as customers' customers); (*b*) meet the entity's commitments to suppliers and business partners; (*c*) comply with relevant laws and regulations and guidelines of industry groups, such as business or trade associations; and (*d*) achieve other entity objectives that are relevant to the trust services category or categories addressed by the description. Requirements are often specified in the entity's system policies and procedures, system design documentation, contracts with customers, and government regulations.

System requirements may result from the entity's commitments relating to security, availability, processing integrity, confidentiality, or privacy. For example, a commitment to programmatically

enforce segregation of duties between data entry and data approval creates system requirements regarding user access administration.

third party. An individual or organization other than the entity and its employees. Third parties may be customers, suppliers, business partners, or others.

trust services. A set of professional attestation and advisory services based on a core set of criteria related to security, availability, processing integrity, confidentiality, or privacy.

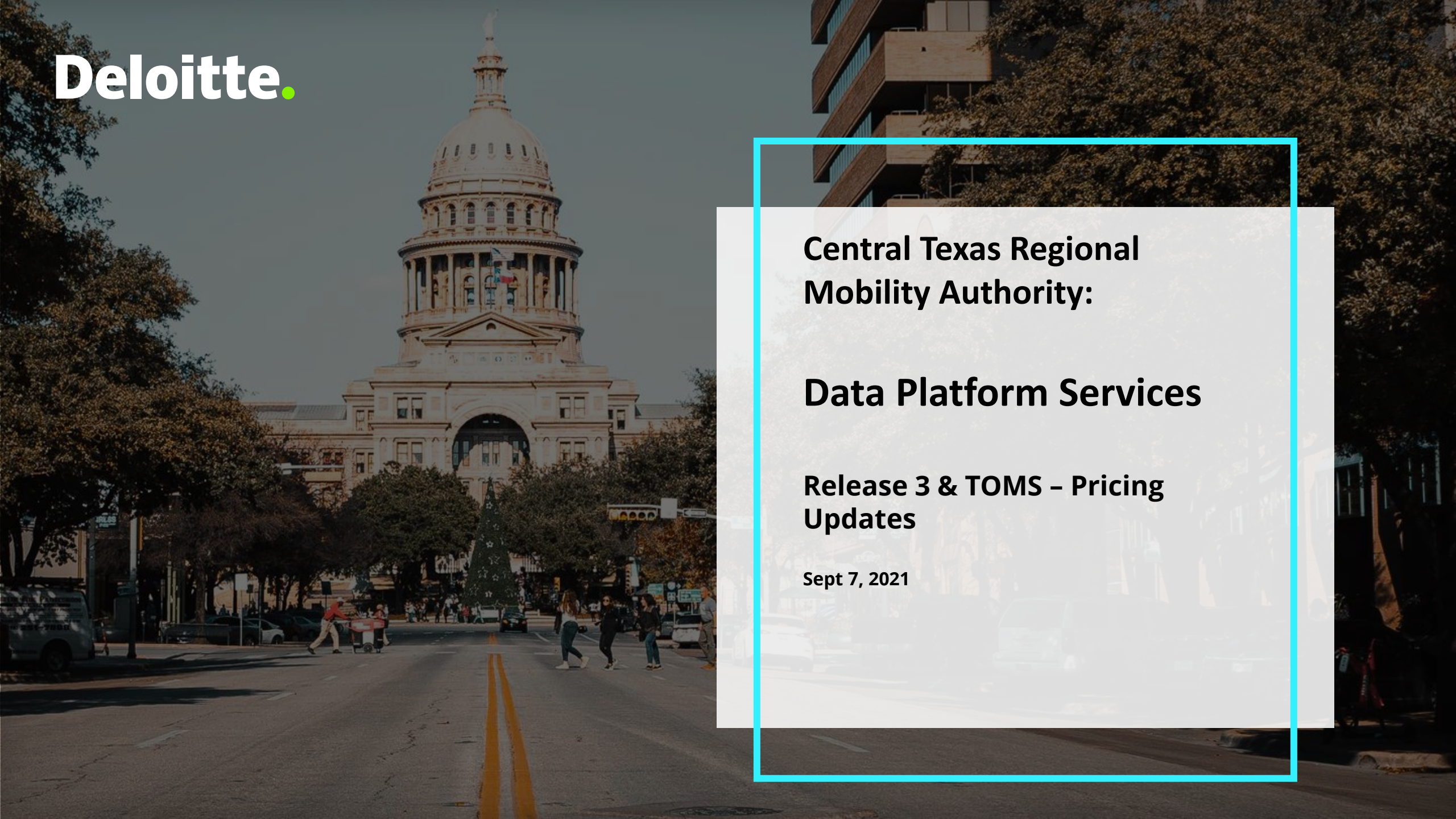
unauthorized access. Access to information or system components that (*a*) has not been approved by a person designated to do so by management and (*b*) compromises segregation of duties, confidentiality commitments, or otherwise increases risks to the information or system components beyond the levels approved by management (that is, access is inappropriate).

vendor (or supplier). An individual or business (and its employees) that is engaged to provide goods or services to the entity. Depending on the services provided (for example, if the vendor operates certain controls on behalf of the entity that are necessary to achieve the entity's objectives), it also might be a service provider.

Exhibit B

CTRMA DATA PLATFORM RELEASE 3 STATEMENT OF WORK
APPENDIX E PRICING FORM - Deloitte Consulting

Release 3 Data Platform Deliverables	Total Hrs / Price	
Tolling Product Management		
Development and deployment of Product database(s) and relationships	Hours	386
	Price	$50,055.00
Design and development of automated Product Management process(es)	Hours	386
	Price	$50,055.00
Development of automated business process(es) for payor ID and payment path routing logic	Hours	386
	Price	$50,055.00
Discount Management		
Development and deployment of Discount database(s) and relationships	Hours	386
	Price	$50,055.00
Design and development of automated Discount Management process(es)	Hours	386
	Price	$50,055.00
Integration of Discount Management with Product Management processes	Hours	386
	Price	$50,055.00
Invoice Management		
Development and deployment of Invoice database(s) and relationships	Hours	386
	Price	$50,055.00
Design and development of automated Invoice Management process(es)	Hours	386
	Price	$50,055.00
Integration of Invoice Management with Product and Discount Management	Hours	386
	Price	$50,055.00
Data Exchange Management		
Design, development, and testing for Pay by Mail('PBM') Invoice data exchange modifications (Fixed file, API, XML, JSON)	Hours	386
	Price	$50,055.00
Design, development, and testing for IOP Hub Invoice data exchange modifications (Fixed file, API, XML, JSON)	Hours	386
	Price	$50,055.00
Development of DMV Hub database(s) and relationships	Hours	386
	Price	$50,055.00
Design, development, and testing for external DMV Hub data exchanges (Fixed file, API, XML, JSON)	Hours	386
	Price	$50,055.00
Design, development, and testing for Public Reporting data exchange (Fixed file, API, XML, JSON, GitHub)	Hours	386
	Price	$50,055.00
Reporting Cache & Reporting Management		
Development of Reporting Cache data platform	Hours	386
	Price	$50,055.00
Development of Public Reporting database(s) and relationships	Hours	386
	Price	$50,055.00
Implementation and testing of Public Reporting data push from master data source to Reporting Cache	Hours	386
	Price	$50,055.00
Development of automated Public Report(s) generation	Hours	386
	Price	$50,055.00
End-to-end testing of Reporting Cache and Public Reporting exchange solutions	Hours	386
	Price	$50,055.00
Data Governance & SOC 2 Compliance		
SOC 2 Risk Objectives, Control Objectives, and Policies	Hours	386
	Price	$50,055.00
SOC 2 Compliance Processes & Procedures	Hours	386
	Price	$50,055.00
Support for establishment of Data Governance strategy and approach	Hours	386
	Price	$50,055.00
Definition of Data Use criteria	Hours	386
	Price	$50,055.00
Automation of Data Governance process(es) including Certification and Attestation for data use	Hours	386
	Price	$50,055.00
Documentation of Data Use Governance Policies & Procedures	Hours	386
	Price	$50,055.00
Development of Data Governance Awareness training, compliance, and certification	Hours	386
	Price	$50,055.00
Declaration and implementation of Data Governance Audit(s)	Hours	386
	Price	$50,055.00
IT Enterprise Management		
Policies & Procedures documentation	Hours	386
	Price	$50,055.00
Revision of Source Data Entity Catalog	Hours	386
	Price	$50,055.00
Data Platform IT Service Catalog(s) and Service Level definition & documentation	Hours	386
	Price	$50,055.00
UX/UI Approaches, Tools, and Deliverables		
Discovery and strategic road mapping for User Experience (near and long-term)	Hours	136
	Price	$18,075.71
User types/roles, tasks, and experience-based priorities	Hours	136
	Price	$18,075.71
User story generation and cataloging (features/functionality suite)	Hours	136
	Price	$18,075.71
Rapid Prototyping for UX & UI design (clickable, codeless)	Hours	136
	Price	$18,075.71
User flows, navigation models, and information flows	Hours	136
	Price	$18,075.71
UI mockups, low-fidelity wireframes, and high-fidelity wireframes	Hours	136
	Price	$18,075.71
Business rules implications, validations, and constraints	Hours	136
	Price	$18,075.71
Style standards, documentation, and controls	Hours	136
	Price	$18,075.71
Multi-workstream Agile-driven sprint release approach	Hours	136
	Price	$18,075.71
Angular v12 Components	Hours	136
	Price	$18,075.71
Feature Deliverables		
Design and development of UX/UI for Manage Roadside Vendor Data Exchange (TCS DEX)	Hours	136
	Price	$18,075.71
Design and development of UX/UI for Manage CUSIOP Hub Data Exchanges (Hub DEX)	Hours	136
	Price	$18,075.71
Design and development of UX/UI for Manage PBM Data Exchanges (PBM DEX)	Hours	136
	Price	$18,075.71
Design and development of UX/UI for Manage General Transaction Processing Day to Day needs	Hours	136
	Price	$18,075.71
Design and development of UX/UI for Product Management (View List, View Item, Create, Modify, Delete)	Hours	136
	Price	$18,075.71
Design and development of UX/UI for monitoring and reporting of automated business process(es) for payor ID and payment path routing logic	Hours	136
	Price	$18,075.71
Design and development of UX/UI for Discount Management (View List, View Item, Create, Modify, Delete)	Hours	136
	Price	$18,075.71
Design and development of UX/UI for Billing Management (View List, View Item, Create, Modify, Delete)	Hours	136
	Price	$18,075.71
Development of UX/UI for monitoring and reporting of automated business process(es) for end-to-end Transaction Pricing, Discounting & Billing process(es)	Hours	136
	Price	$18,075.71
Development of UX/UI for monitoring and reporting of automated business process(es) for Public Reporting metrics & performance	Hours	136
	Price	$18,075.71
Design and development of UX/UI for administration and facilitation of Data Governance process(es)	Hours	136
	Price	$18,075.71
	Total Hours by Role	**14,450**
	Total Price by Role	**$1,881,240**



Deloitte.

Central Texas Regional Mobility Authority:

Data Platform Services

Release 3 & TOMS – Pricing Updates

Sept 7, 2021

Agenda

- Release 3 Scope and Deliverables
- TOMS Scope, Requirements and Deliverables
- Pricing & Project Timeline Information

Deloitte.

Release 3 – Revised High-Level Scope and Assumptions

Category	Detail

High Level Scope	• **Plan & Strategy**
	  ○ Conduct up to 8 Discovery/Design Sessions
	• **Tolling Product Management**
	  ○ Design & Develop Database Model
	  ○ Design & Develop (~2) Data Processing routines for 2 active current products
	  ○ Develop/Modify required Payor ID and Payment routing Process
	• **Discount Management**
	  ○ Design & Develop Discount Database Model
	  ○ Design & Develop (~5) Discount Data Processing routines
	  ○ Integrate Product and Discount Management Process
	• **Invoice Management**
	  ○ Design & Develop Invoice Database Model
	  ○ Design & Develop (~9) automated Invoice Data Processing routines
	  ○ Integrate Product and Discount Management Process with Invoicing
	• **Data Exchange Management**
	  ○ Design & Develop (~5) Data Processing/Exchange Routines to support DMV, PBM etc.
	  ○ Modify required existing Data Exchange Routines (~10) related to CUSIOP, PBM, TCS etc.,
	• **Reporting Cache & Reporting Management**
	  ○ Create Reporting Data Model in BigQuery to support Public Reporting
	  ○ Design & Develop (~20) Data transfer routines from master data source to reporting cache
	  ○ Install and Configure GCP Looker Service tool
	  ○ Develop up to 8 Public Reports/API Services and 5 Looker Reports to support Operational Monitoring
	• **Data Governance & IT Enterprise Management**
	  ○ Define relevant SOC 2 Compliance Processes & Procedures
	  ○ Documentation of Data Governance Policies & Procedures
	  ○ Development of Data Governance Awareness training, compliance, and certification
	  ○ Declaration and implementation of Data Governance Audit(s)
	  ○ Revision of Source Data Entity Catalog
	  ○ Data Platform IT Service Catalog(s) and Service Level definition & documentation

Release 3 – Revised High-Level Scope and Assumptions

Category	Detail

High Level Scope	• **Testing and Go-Live**
	  ○ Perform end to end testing of Release 3 system changes and coordinate with CTRMA/external stakeholders for User Acceptance testing (~400 test cases)
	  ○ Transition of operations post Go-Live to Run and Operate team

Assumptions	▪ This solution is based on existing Google Cloud Platform (GCP) ▪ CTRMA will procure any additional required software licenses and services per mutual agreement ▪ GCP Cloud consumption cost is not included on the pricing ▪ CTRMA business teams and SME to be available for requirements discovery and design review sessions ▪ CTRMA payments are processed by an external third party and either of PCI-DSS Self-Assessment Questionnaire (SAQ) A or A-EP shall be applicable wherein Deloitte team shall support CTRMA in completing the questionnaire (if applicable) ▪ Deloitte will leverage existing procedures and processes wherever applicable ▪ Data governance activities will leverage DPS data dictionary and attribute list ▪ Deloitte shall update or create up to 10 procedures as a part of CTRMA Data Platform documentation ▪ Policy and procedure documentation will be limited to relevant IT, security, and compliance components in-scope for the CTRMA Data Platform ▪ Duration excludes 3 weeks of holiday break ▪ Coordinate and conduct 6 weeks of UAT with HUB and PBM vendor ▪ Scope adjusted based on active products and corresponding discounts & invoices ▪ Test scenarios/ Test cases will be provided related to production business situations/operational items ▪ CTRMA team will support with production data to verify and validate DPS codebase functionality/performance ▪ Data Use Criteria and Data Entity Catalog Deliverables will be combined ▪ Security Deliverables will be combined into one document as appropriate with sections detailing the content of stated deliverables
Out of Scope	▪ Historic Data Migration/conversion ▪ Operate and Production Support services ▪ PCI-DSS certification and SOC2 attestation ▪ Reporting for public access and viewing

TOMS – High-Level Scope and Assumptions

Category	Detail
High Level Scope	**Plan & Strategy** ▪ Conduct 1-3 discovery sessions with 4-6 key stakeholders to gather and identify design and functionality requirements* **UI/UX Features** **Data Exchange Management** ▪ Design & Development of UX/UI to manage TCS Data Exchange (TCS DEX) ▪ Design & Development of UX/UI to manage CUSIOP Hub Data Exchange (Hub DEX) ▪ Design & Development of UX/UI to manage PBM Data Exchange (PBM DEX) ▪ Design & Development of UX/UI to manage General Transactional Processing Day To Day Needs **Product Management** ▪ Design & Development of UX/UI for Product Management (View & List Items and support CRUD Ops) ▪ Design & Development of UX/UI for Monitoring Payor ID & Payment Path Routing Logic, managing Pricing Adjustments **Discount Management** ▪ Design & Development of UX/UI for Managing Discount Types, Discount Programs and Discount Pricing **Billing Management** ▪ Design & Development of UX/UI for Managing Billing (View & List Items and support CRUD Ops) ▪ Design & Development of UX/UI for Monitoring and Managing of automated processes of End-To-End Transaction Pricing, Discounting, Billing **Reporting Management** ▪ Design & Development of UX/UI for Monitoring of automated business processes for Public Reporting Metrics and Performance **Data Governance** ▪ Design & Development of UX/UI for Managing Administration and Facilitation of Data Governance processes

TOMS – Revised High-Level Scope and Assumptions

Category	Detail
High Level Scope	**UI/UX Approaches and Tools** ▪ Provide user types/roles, tasks, and experience-based priorities as needed ▪ User story generation and cataloging (features/functionality suite)***** ▪ Provide experience architecture - application map, user flows, navigation models, and key workflows ▪ Create all necessary UI screen mockups, zone diagrams & wireframes ▪ Create prototypes (clickable, codeless) as needed to demonstrate interaction design ▪ Business rules implications, validations, and constraints ▪ Develop design system guide: style standards, templates, components, and proposed governance ▪ Sprint planning: Multi-workstream Agile-driven sprint release approach ▪ Deliver code as Angular v12 Components **Testing** ▪ Conduct and facilitate design validation testing and UAT testing with CTRMA stakeholders ▪ Perform Functional Testing including accessibility/performance
Assumptions	▪ *****Any features/functionality identified as future enhancements (i.e., not to be not delivered in current phase) will be added to a future state backlog and will require additional scope to conduct a vision workshop and provide a strategic experience roadmap. ▪ QA will be required for functional / accessibility (508) testing and to help with visual QA based on front-end designs. ▪ Existing DPS UI application framework will be extended for TOMS
Out of Scope	▪ **Any internal and external reporting tied with UI/UX will be addressed in CTRMA future Release 4** ▪ DEX Reporting ▪ Product Reporting ▪ Payment Path Reporting ▪ Discount Reporting ▪ Invoice Reporting ▪ Reporting & Analytics Management ▪ Quality Management ▪ Case Management

Release 3 – Revised Deliverable Schedule

Proposed Release 3 deliverable/payment schedule information

No.	Deliverables	Estimated Sprint Schedule	Estimated Week Ending	Estimated Due Date*	Payment Amount
1	Development and deployment of Product database(s) and relationships	2	4	10/30/2021	$50,055
2	Design and development of automated Product Management process(es)	2	4	10/30/2021	$50,055
3	Development of automated business process(es) for payor ID and payment path routing logic	2	4	10/30/2021	$50,055
4	Development and deployment of Discount database(s) and relationships	4	9	12/3/2021	$50,055
5	Design and development of automated Discount Management process(es)	4	9	12/3/2021	$50,055
6	Integration of Discount Management with Product Management processes	4	9	12/3/2021	$50,055
7	Development and deployment of Invoice database(s) and relationships	5	11	12/17/2021	$50,055
8	Design and development of automated Invoice Management process(es)	5	11	12/17/2021	$50,055
9	Integration of Invoice Management with Product and Discount Management	5	11	12/17/2021	$50,055
10	Design, development, and testing for Pay by Mail('PBM') Invoice data exchange modifications (Fixed file, API, XML, JSON)	6	15	1/14/2022	$50,055
11	Design, development, and testing for IOP Hub Invoice data exchange modifications (Fixed file, API, XML, JSON)	6	15	1/14/2022	$50,055
12	Development of DMV Hub database(s) and relationships	6	15	1/14/2022	$50,055
13	Design, development, and testing for external DMV Hub data exchanges (Fixed file, API, XML, JSON)	7	17	1/28/2022	$50,055
14	Design, development, and testing for Public Reporting data exchange (Fixed file, API, XML, JSON, GitHub)	7	17	1/28/2022	$50,055
15	Development of Reporting Cache data platform	7	17	1/28/2022	$50,055
16	Development of Public Reporting database(s) and relationships	8	19	2/11/2022	$50,055
17	Implementation and testing of Public Reporting data push from master data source to Reporting Cache	8	19	2/11/2022	$50,055
18	Development of automated Public Report(s) generation	8	19	2/11/2022	$50,055
19	End-to-end testing of Reporting Cache and Public Reporting exchange solutions	9	21	2/25/2022	$50,055
20	SOC 2 Risk Objectives, Control Objectives, and Policies	9	21	2/25/2022	$50,055
21	SOC 2 Compliance Processes & Procedures	9	21	2/25/2022	$50,055
22	Support for establishment of Data Governance strategy and approach	9	21	2/25/2022	$50,055
23	Definition of Data Use criteria	9	21	2/25/2022	$50,055
24	Automation of Data Governance process(es) including certification and affirmation for data use	9	21	2/25/2022	$50,055
25	Documentation of Data Governance Policies & Procedures	9	21	2/25/2022	$50,055
26	Development of Data Governance Awareness training, compliance, and certification	10	23	3/11/2022	$50,055
27	Declaration and implementation of Data Governance Audit(s)	10	23	3/11/2022	$50,055
28	Policies & Procedures documentation	10	23	3/11/2022	$50,055
29	Revision of Source Data Entity Catalog	11	25	3/28/2022	$50,055
30	Data Platform IT Service Catalog(s) and Service Level definition & documentation	11	25	3/28/2022	$50,055
				Sub-Total	**$1,501,650**

Deloitte. * Based on project state date of 10/4/21

TOMS - Deliverable Schedule

Proposed TOMS deliverable/payment schedule information

No.	Deliverables	Estimated Sprint Schedule	Estimated Week Ending	Estimated Due Date*	Payment Amount
1	Discovery and strategic road mapping for User Experience (near and long-term)	4	9	12/3/2021	$18,075
2	User types/roles, tasks, and experience-based priorities	4	9	12/3/2021	$18,075
3	User story generation and cataloging (features/functionality suite)	4	9	12/3/2021	$18,075
4	Rapid Prototyping for UX & UI design (clickable, codeless)	5	11	12/17/2021	$18,075
5	User flows, navigation models, and information flows	5	11	12/17/2021	$18,075
6	UI mockups, low-fidelity wireframes, and high-fidelity wireframes	5	11	12/17/2021	$18,075
7	Business rules implications, validations, and constraints	6	15	1/14/2022	$18,075
8	Style standards, documentation, and controls	6	15	1/14/2022	$18,075
9	Multi-workstream Agile-driven sprint release approach	6	15	1/14/2022	$18,075
10	Angular v12 Components	7	17	1/28/2022	$18,075
11	Design and development of UX/UI for Manage Roadside Vendor Data Exchange (TCS DEX)	7	17	1/28/2022	$18,075
12	Design and development of UX/UI for Manage CUSIOP Hub Data Exchanges (Hub DEX)	7	17	1/28/2022	$18,075
13	Design and development of UX/UI for Manage PBM Data Exchanges (PBM DEX)	8	19	2/11/2022	$18,075
14	Design and development of UX/UI for Manage General Transaction Processing Day to Day needs	8	19	2/11/2022	$18,075
15	Design and development of UX/UI for Product Management (View List, View Item, Create, Modify, Delete)	8	19	2/11/2022	$18,075
16	Design and development of UX/UI for monitoring and reporting of automated business process(es) for payor ID and payment path routing logic	9	21	2/25/2022	$18,075
17	Design and development of UX/UI for Discount Management (View List, View Item, Create, Modify, Delete)	9	21	2/25/2022	$18,075
18	Design and development of UX/UI for Billing Management (View List, View Item, Create, Modify, Delete)	9	21	2/25/2022	$18,075
19	Development of UX/UI for monitoring and reporting of automated business process(es) for end-to-end Transaction Pricing, Discounting & Billing process(es)	10	23	3/11/2022	$18,075
20	Development of UX/UI for monitoring and reporting of automated business process(es) for Public Reporting metrics & performance	10	23	3/11/2022	$18,075
21	Design and development of UX/UI for administration and facilitation of Data Governance process(es)	10	23	3/11/2022	$18,090
				Sub-Total	**$379,590**
				Total	**$1,881,240**

* Based on project state date of 10/4/21

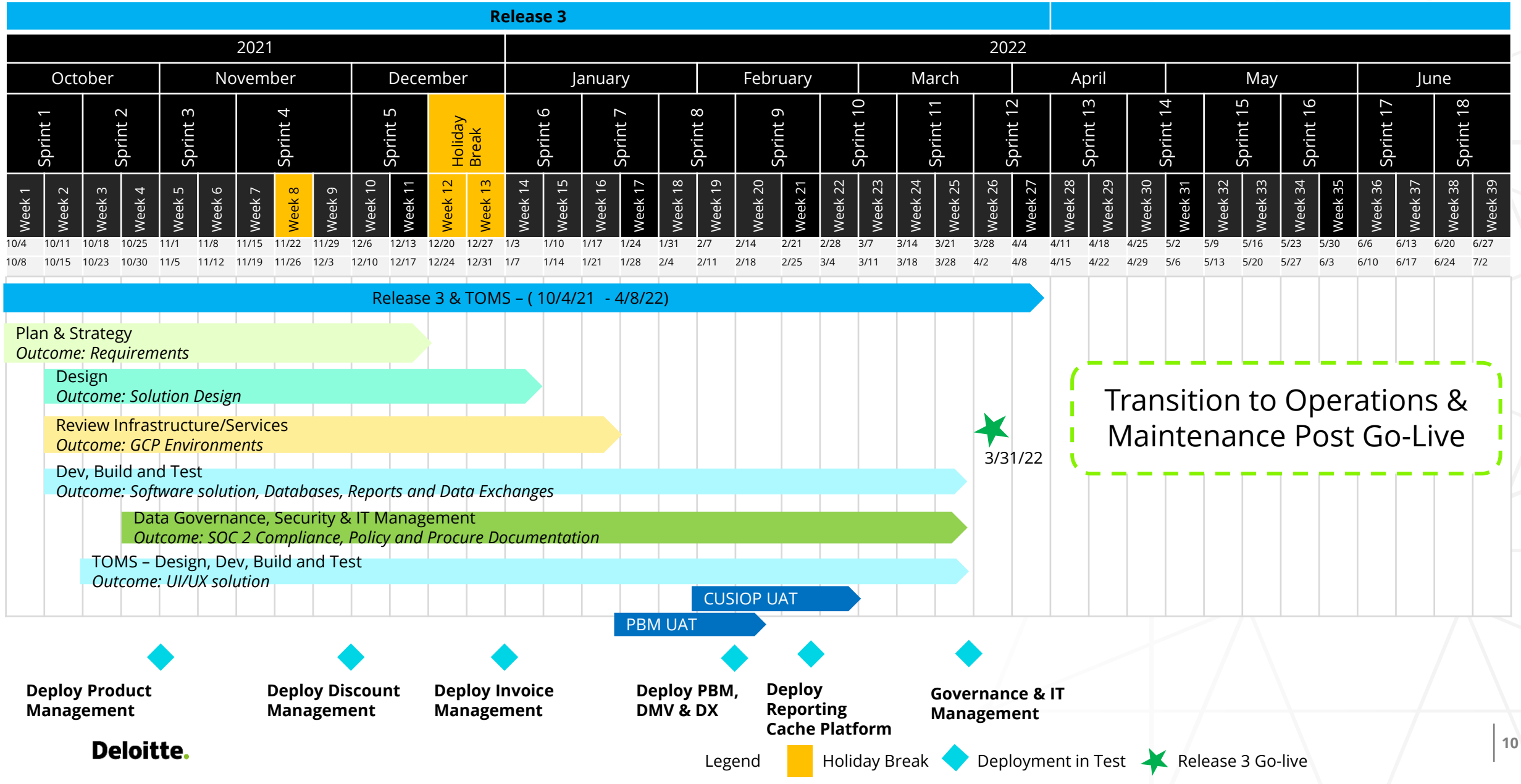
Pricing & Productivity Gain Synopsis – From Release 1 & 2 to 3

We have leveraged knowledge, experience and expertise from the execution of Release 1 & 2 to optimize delivery approach and estimates of Release 3 and TOMS

Release	No. of Deliverables	No. of Sprints	Total Fees	Fees / Deliverable
Release 1 & 2	17	12	$1,540,860	$90,639
Release 3 with TOMS	51	12	$1,881,240	$36,887
Productivity Gain / Deliverable	**Release 3 with TOMS - 59% Productivity Gain Over Release 1&2**			

Release 3 & TOMS – Timeline and Sprint Plan

Data Platform Services Release 3 Requirements and TOMS is expected to occur during Fall 2021 to early Summer 2022.



Public Records Act Agreement

Contractor acknowledges and agrees that all records, documents, drawings, plans, specifications and other materials in the Authority's possession, including materials submitted by Contractor, are subject to the provisions of the Texas Public Information Act (see Texas Government Code § 552.001). Contractor shall be solely responsible for all determinations made by it under such law, and for clearly and prominently marking each and every page or sheet of materials with "Trade Secret" or "Confidential", as it determines to be appropriate. Contractor is advised to contact legal counsel concerning such law and its application to Contractor.

If any of the materials submitted by the Contractor to the Authority are clearly and prominently labeled "Trade Secret" or "Confidential" by Contractor, the Authority will endeavor to advise Contractor of any request for the disclosure of such materials prior to making any such disclosure. Under no circumstances, however, will the Authority be responsible or liable to Contractor or any other person for the disclosure of any such labeled materials, whether the disclosure is required by law, or court order, or occurs through inadvertence, mistake or negligence on the part of the Authority or its officers, employees, contractors or consultants.

In the event of litigation concerning the disclosure of any material marked by Contractor as "Trade Secret" or "Confidential," the Authority's sole obligation will be as a stakeholder retaining the material until otherwise ordered by a court, and Contractor shall be fully responsible for otherwise prosecuting or defending any action concerning the materials at its sole cost and risk; provided, however, that the Authority reserves the right, in its sole discretion, to intervene or participate in the litigation in such manner as it deems necessary or desirable. All costs and fees, including reasonable attorneys' fees and costs, incurred by the Authority in connection with any litigation, proceeding or request for disclosure shall be reimbursed and paid by Contractor.

DELOITTE CONSULTING LLP	**CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY**
_____	_____
Uday Katira, Managing Director Deloitte Consulting LLP	James Bass Executive Director
_____	_____
Date	Date

DIR Vendor Agreement

This is to signify that the Central Texas Regional Mobility Authority and Deloitte Consulting LLP Corporation have entered into an Agreement **in an amount not to exceed $2,069,364** *(amount includes a 10% project contingency; does not include required hardware, software or software licenses)* pursuant to Texas Government Code Section 2054.0565 utilizing Texas Department of Information Resources Contract No. #DIR-TSO-4031 for the deliverable-based information technology services described in this proposal. All terms and conditions of Texas Department of Information Resources Contract No. #DIR-TSO-4031 are applicable to and made part of this agreement.

DELOITTE CONSULTING LLP	**CENTRAL TEXAS REGIONAL MOBILITY AUTHORITY**
_____	_____
Uday Katira, Managing Director Deloitte Consulting LLP	James Bass Executive Director
_____	_____
Date	Date