



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

October 25, 2023
AGENDA ITEM #11

Discuss and consider approving an agreement with Deloitte Consulting LLP for enhancement development of the Mobility Authority's Data Platform System

Strategic Plan Relevance:	Innovation
Department:	Operations
Contact:	Greg Mack, Director of Information Technology
Associated Costs:	Not to exceed \$500,000
Funding Source:	FY24 Capital Budget
Action Requested:	Consider and act on draft resolution

Project Description/Background: To provide more flexibility in the future, in March 2021, the Mobility Authority awarded a contract to Deloitte Consulting LLP (Deloitte) to develop a system wherein all toll transaction processing and data management capabilities after the point of transaction creation are advanced to a Mobility Authority-managed solution. The Data Platform System (DPS) is the next step in the agency's evolution to a mature toll entity that controls transaction pricing and revenue recognition timing. The DPS will also provide the Authority with more insight into its transactional data, providing the ability to make better informed decisions regarding collection initiatives, transportation improvements, and other planning efforts.

The objective of the DPS is to transition all toll transaction data processing and data management capabilities after the point of transaction creation to a Mobility Authority-managed solution. Kapsch and ETC, the Authority's lane vendors, will collect the toll transaction at the roadside and forward the transaction and vehicle images to the DPS. Business logic will then consume the transaction and route the data to either the Central United States Interoperability (CUSIOP) Hub or the Pay by Mail (PBM) vendor for payment. The payment status is ultimately passed back to the DPS allowing complete reconciliation of all the Authority's toll transactions.

Development for the first two project releases was completed September 2021 on schedule. These releases created the base code as well as the routing and exchange processes. Release 3 supports development for pricing and billing transactions, defining how data governance is handled in the new processing schema, and identifying the suite of reports necessary to account for the agency's revenue and monitor performance. Release 3 is anticipated to be completed this month. The DPS went live in August 2023, and has been running in parallel to the current system since that time.

The Mobility Authority desires additional development services as the system matures. Enhancements to DPS would include new functionality that is not covered in the Operations and Maintenance scope of work. Today's action is directly related to the engagement of resources for such development.

Previous Actions & Brief History of the Program/Project: An initial contract for the development of DPS Releases 1 & 2 was awarded to Deloitte in February 2021; the contract was subsequently approved in March 2021. A contract for the development of Release 3 was awarded to Deloitte in September 2021. The initial one-year O&M contract was awarded to Deloitte in June 2022; three amendments to that contract have been issued to provide services through September 2023.

Financing: FY24 Capital Budget

Action requested/Staff Recommendation: Staff recommends approving an agreement with Deloitte Consulting LLP for consulting services for enhancement development of the Mobility Authority's Data Platform System.

Backup provided:

- Draft Resolution
- CTRMA TOMS Enhancements Statement of Work (dated 9/15/23)
- DIR Public Records Act Agreement – Deloitte Consulting Enhancements Statement of Work
- DIR Vendor Agreement – Deloitte Consulting O&M Enhancements

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

RESOLUTION NO. 23-0XX

**APPROVING AN AGREEMENT WITH DELOITTE CONSULTING LLP FOR
ENHANCEMENT DEVELOPMENT OF THE MOBILITY AUTHORITY'S DATA
PLATFORM SYSTEM**

WHEREAS, as of August 1, 2023, the Mobility Authority has been utilizing its own data platform for all toll transaction data processing and data management capabilities after the point of transaction creation (the "Data Platform System"); and

WHEREAS, the Data Platform System also supports 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, the Mobility Authority staff desires additional enhancements to the Data Platform System to add new capabilities and improve functionality; and

WHEREAS, the Executive Director has negotiated a scope of work with Deloitte Consulting LLP in an amount not to exceed \$500,000 for additional development services and enhancements to the Data Platform System which is attached hereto as Exhibit A; and

WHEREAS, pursuant to Texas Government Code Section 2054.0565 and Mobility Authority Policy Code Section 401.008, the Mobility Authority may utilize procedures established by the Texas Department of Information Resources (DIR) to procure goods and services through DIR cooperative contracts; and

WHEREAS, the Executive Director recommends entering into an agreement with Deloitte Consulting LLP for additional development services and enhancements to the Data Platform System in an amount not to exceed \$500,000 through their DIR cooperative contract.

NOW THEREFORE BE IT RESOLVED that the Board of Directors hereby approves the scope of work for additional development services and enhancements to the Data Platform System which is attached hereto as Exhibit A; and

BE IT FURTHER RESOLVED, that the Executive Director is authorized to enter into an agreement with Deloitte Consulting LLP in an amount not to exceed \$500,000 through their cooperative contract with the Texas Department of Information Resources for additional development services and enhancements to the Data Platform System.

Adopted by the Board of Directors of the Central Texas Regional Mobility Authority on the 25th day of October 2023.

Submitted and reviewed by:

Approved:

James M. Bass
Executive Director

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

Exhibit A



CENTRAL TEXAS REGIONAL
MOBILITY AUTHORITY

Statement of Work

Tolling Operations Management Solution (TOMS)

2023 – 2024 Enhancements

October 25, 2023

Contents

1. Statement of Work Purpose and Overview.....	3
1.1. Term.....	3
2. Scope of Services	3
2.1. Requirements Services	3
2.2. Design Services	4
2.3. Development Services	4
2.4. Testing Services	4
2.5. User Acceptance Testing (UAT) Services	5
2.6. Release Services	5
2.7. Warranty Services.....	5
3. Deliverables	6
3.1. Description	6
3.2. Vendor Deliverables & Payment Allocation	7
3.3. Invoices.....	7
3.4. Acceptance Management.....	7
4. Project Governance	9
4.1. Project Issues Management	9
4.2. Change Process.....	9
4.3. Unforeseen Conditions and Events	10
4.4. Delays and Extensions	10
5. Additional Terms and Conditions	11
6. Compliance with CTRMA Information Security Guidelines	12
7. CTRMA Provided Services.....	12
7.1. Location of Work, Hours and Conditions	12
Appendix A: CTRMA Information Security Policy	13

1. Statement of Work Purpose and Overview

The Tolling Operations Management Solution (“TOMS”) is an aggregate of multiple integrated solutions that support the CTRMA transaction to cash lifecycle. TOMS fully or partially automates business processes across several operational domains including Transaction Management, Product Management, Payment Path Management, Discount Management, Billing Management, Data Exchange Management, and Reporting & Analytics Management.

The purpose of this Statement of Work (“SOW”) is to define a suite of services necessary to support the development and implementation of requested enhancements to components of the existing TOMS Ecosystem. This SOW is intended to serve as a basis of understanding between CTRMA and a 3rd party Vendor (“Vendor”) for the services contracted.

1.1. Term

The Effective Date of this Contract is October 1, 2023, or the date on which this Contract is fully executed and approved according to applicable laws, rules, and regulations, whichever is later. This Contract terminates on June 30, 2024, unless otherwise terminated or extended in accordance with its terms.

2. Scope of Services

Vendor will provide the following services to CTRMA (Vendor Deliverables are noted in ***bold Italics***):

2.1. Requirements Services

CTRMA will define and document the business requirements for each scoped and prioritized feature. The business requirements will describe the expected functionality and may also include supporting artifacts such as logical models, information flow diagrams, and annotated wireframes. CTRMA will document all business requirements artifacts within the appropriate CTRMA Jira project.

In some instances, CTRMA may provide screenshots or other representations of current state for reference but are not to be considered as future state requirements.

Vendor and CTRMA will collectively review the documented business requirements and address any required clarifications.

Vendor will develop a rough order of magnitude (ROM) cost and estimated timeline for the scoped feature and present to CTRMA. Vendor and CTRMA will iteratively review and discuss the cost and estimations. If CTRMA approves the cost and estimated schedule, the feature will be moved into the Design phase. Should CTRMA decide not to proceed, the feature will be moved out of scope and placed into an appropriate backlog.

2.1.1. Vendor Requirements Services & Deliverables

- Review and analyze requirements documentation provided by CTRMA
- Identify risks and/or constraints and present feedback to CTRMA on documented requirements
- Develop cost and estimated schedule to deliver the scoped requirements
- Present rough order of magnitude (ROM) solution costs and estimated schedule to CTRMA for review and approval to proceed.

2.2. Design Services

Vendor will develop one or more designs that will provide functionality meeting the requirements defined as in scope. The initial design(s) will be presented to CTRMA for iterative review and input with the Vendor updating the initial design(s) as required. Vendor will present a final design to CTRMA that includes a revised cost and estimated schedule. If CTRMA approves the cost and estimated schedule, the feature will be moved into the Development phase. Should CTRMA decide not to proceed, the feature will be moved out of scope and placed into an appropriate backlog.

2.2.1. Vendor Design Services & Deliverables

- Create one or more recommended application designs to satisfy the documented requirements
- Create visual representations of proposed solution design(s) and risks/constraints associated with each
- Include modular and scalable solution design and architecture in recommended design(s)
- Present and review draft solution design(s), costs and estimated schedule with risk and constraints to CTRMA
- Develop revised cost and estimated schedule to deliver CTRMA selected design(s), if necessary
- ☑ ***Present final design, cost and estimated schedule to CTRMA for review and acceptance***

2.3. Development Services

Vendor will manage and complete all required solution development activities. Once completed, Vendor will present a development retrospective to CTRMA. Once accepted by CTRMA, the feature will be moved into the Testing phase.

2.3.1. Vendor Development Services & Deliverables

- Provide all application development services necessary to build the CTRMA selected design(s)
- Coordinate with CTRMA TOMS O&M Support to stand-up any/all necessary sandbox, development, and testing environments
- Manage Vendor application development resources, approach and planning
- Include modular, scalable, and/or re-usable code in all development where possible
- ☑ ***Present development retrospective including summary of modular, scalable, or re-usable code applied to CTRMA for review and acceptance***

2.4. Testing Services

Vendor will develop the testing plan and facilitate all required testing for the feature. Vendor will document the tests to be completed, expected outcomes, and actual outcomes. Vendor will document, track and manage all issues identified during testing as defects through resolution. Once all testing has been successfully completed and documented, Vendor will provide a demo of the testing results and accompanying test and defect documentation to CTRMA. After CTRMA acceptance, the feature will move into the UAT phase.

2.4.1. Vendor Testing Services & Deliverables

- Provide all testing services necessary to ensure quality assurance for developed solution(s)
- Document test cases including test scenarios, expected outcomes and actual outcomes
- ☑ ***Present documented test cases to CTRMA for review and acceptance***

- Complete all necessary smoke, unit, integration, functional, and performance testing to ensure solution quality assurance
- Coordinate with CTRMA TOMS O&M Support team to perform any/all necessary regression testing
- Document, track and manage all defects identified during testing using CTRMA Jira procedures
- ☑ ***Present a testing retrospective including documented test cases and defect resolution summary to CTRMA for review and acceptance***

2.5. User Acceptance Testing (UAT) Services

CTRMA will define the UAT scripts and facilitate any required user acceptance testing. Issues identified during UAT will be documented by CTRMA and reviewed with the Vendor. For any identified issues, CTRMA will work with the Vendor to determine if the issue is a Defect or new Requirement Specification.

For issues identified as a new Requirement Specification, CTRMA will document the requirements and add them to the TOMS Backlog for future enhancement consideration.

Issues identified as Defects will be addressed by the Vendor and are considered required for final feature acceptance. All Defects will be tracked in the CTRMA Jira system in accordance with CTRMA Jira policies and procedures. Once all Defects have been resolved and any additional UAT completed, Vendor will present a retrospective and accompanying Defect documentation to CTRMA for acceptance. Accepted features will then be moved to the Release phase.

2.5.1. Vendor Services & Deliverables

- Document, track and manage all defects identified during UAT using CTRMA Jira procedures
- ☑ ***Present a UAT retrospective with accompanying defect summary to CTRMA for review and acceptance***

2.6. Release Services

Vendor will work with the CTRMA TOMS O&M Support team to incorporate the feature into a Release Plan. Once the feature has been released to the production environment, Vendor will notify CTRMA in writing and the feature has moved into the Warranty phase.

2.6.1. Vendor Release Services & Deliverables

- Coordinate with the CTRMA TOMS O&M Support team to assign the solution to an appropriate production release
- ☑ ***Provide written notice to CTRMA that the solution has been moved into the production environment***

2.7. Warranty Services

Unless otherwise mutually agreed, the Warranty Period shall be 60 calendar days starting from the date the feature was released into production. For issues identified as Defects during the Warranty Period, the Vendor shall, at no additional charge to CTRMA, furnish such materials and services necessary to correct any Defects related to the released feature. Once the Warranty Period has ended and all Defects identified during the Warranty Period have been resolved, Vendor will present a retrospective and accompanying Warranty Period Defect summary documentation to CTRMA for acceptance.

2.7.1. Vendor Warranty Services & Deliverables

- Document, track and manage all defects identified during the Warranty Period using CTRMA Jira procedures.
- Provide all Development Services as defined in section 2.3 to resolve all defect(s) identified during the Warranty Period
- Provide all Testing Services as defined in section 2.4 to resolve all defect(s) identified during the Warranty Period
- Provide all UAT Services as defined in section 2.5 to resolve all defect(s) identified during the Warranty Period
- ☑ ***Present a Warranty Period retrospective with accompanying defect resolution summary to CTRMA for review and acceptance***

3. Deliverables

3.1. Description

“Deliverables” means all materials, documents, software (if any) and any other items set forth in this Agreement that are in scope and are originally created, developed, or produced by Vendor specifically for delivery to CTRMA.

The detailed Acceptance Criteria for each Deliverable or Service will be determined and agreed to with CTRMA, prior to the commencement of work on any Deliverable or Service. Changes to this list of Deliverables and/or Acceptance Criteria, or the definition or content of such Deliverables as described by Vendor’s management and delivery methods, or the party responsible for a Deliverable will be managed via the Change Process as defined in Section 4.2.

Both parties shall agree upon Acceptance Criteria consistent with the “SMART” Method of defining acceptance criteria, i.e., Specific, Measurable, Achievable, Relevant, and Time-bound. Notwithstanding the Vendor’s commencement or completion of any Deliverable under this Agreement, the Vendor will not submit any Deliverable or Service to CTRMA for review and CTRMA will be under no obligation to review, Accept or Reject any Deliverable or Service until the Acceptance Criteria for that Deliverable has been defined and agreed to by both parties.

Further, the Vendor is not obligated to start work on a specific Deliverable or Work Product until the parties have agreed in writing on the Acceptance Criteria for that Deliverable or Work Product, nor is the Vendor responsible for any delays caused by a failure of CTRMA to timely agree on the Acceptance Criteria.

Formal Acceptance by CTRMA of the Deliverables and Services is the sole indication that the Deliverables or Services have been completed in accordance with this Agreement. Neither party may unreasonably withhold Formal Acceptance where the agreed upon Acceptance Criteria for the Deliverable or Service have been satisfied.

3.2. Vendor Deliverables & Payment Allocation

For each scoped and prioritized feature, the Vendor will deliver the following as Deliverables as defined in Section 2: Scope of Services:

Phase	Deliverable	Payment Allocation
Design	Present final design, cost, and estimated schedule to CTRMA for review and acceptance.	20%
Development	Present development retrospective including summary of modular, scalable, or re-usable code applied to CTRMA for review and acceptance.	20%
Testing	Present documented test cases to CTRMA for review and acceptance. Present a testing retrospective including documented test cases and defect resolution summary to CTRMA for review and acceptance.	20%
UAT	Present a UAT retrospective with accompanying defect summary to CTRMA for review and acceptance.	30%
Release	Provide written notice to CTRMA that the solution has been moved into the production environment.	-
Warranty	Present a Warranty Period retrospective with accompanying defect resolution summary to CTRMA for review and acceptance.	10%

3.3. Invoices

The Vendor may invoice CTRMA after each Payment Deliverable is accepted. CTRMA will not make partial payments for deliverable subtasks.

This pricing is subject to and governed by the DBITS terms and conditions as set forth in DBITS # DIR-CPO-4919. CTRMA will purchase any additional required software, hardware, and hosting in support of the agreed upon Scope of Work. All Google Cloud Platform services are available on Texas DIR contract # DIR-TSO-4162, via Google Cloud’s exclusive government distributor, Carahsoft Technology Corporation.

3.4. Acceptance Management

Acceptance by CTRMA of the project’s Services and Deliverables means that the Services and Deliverables have been completed in accordance with this Agreement.

Vendor and CTRMA will agree upon acceptance criteria for the Services and each Deliverable. Acceptance criteria must be documented prior to the commencement of work on any Deliverable or Service. The parties agree to the following Acceptance Management process:

The respective Project Manager will submit a Deliverable and Service Acceptance form for each completed Deliverable or Service to the designated Approver.

1. The following Acceptance Definitions apply to this SOW:

- a. **Accepted:** The deliverable is approved 'As Is' and is considered complete.
 - b. **Rejected:** Does not meet Acceptance criteria and is returned for remediation (see below requirements for Rejected).
 - c. **Conditional Acceptance:** Is considered Accepted (for invoicing purposes only) under the condition that minor modifications and or updates that do not impact the holistic content of the Deliverable (See below requirements for Conditional Acceptance)
2. CTRMA approver will Accept (by written notice of Acceptance or Conditional Acceptance) or reject the Services and/or Deliverable within five (5) business days from the receipt of the acceptance form from the Vendor Project Manager.
 3. If CTRMA approver does not accept or reject the Deliverables and/or Services within five (5) business days from the receipt of the acceptance form from the Vendor Project Manager and does not communicate a reasonable timeframe in which a decision will be made, the Deliverables and Services will be considered accepted.
 - a. Work will progress to maintain the established project schedule, with the understanding that any changes to an Accepted Deliverable or Service may constitute a change in scope, and for any change that is determined to be a change in scope the parties will invoke the Escalation Process (See Issues Management).
 - b. A Change Order may result if modifications to the Accepted Deliverable or Service are required, and those modifications affect Accepted or in-progress project work.
 4. If CTRMA approver Conditionally Accepts a Deliverable or Service, the cause for the Conditional Acceptance and any known defects CTRMA wants to be addressed will be documented by CTRMA and provided to the Vendor in a notice of Conditional Acceptance as set forth above. The Vendor will correct or revise the Deliverable or Service, as applicable, and resubmit to CTRMA for review within five (5) business days from the receipt of CTRMA's notice of Conditional Acceptance or such other time as agreed upon in writing between the parties, unless the Vendor is not in agreement with the Conditional Acceptance, in which case the parties will invoke the Escalation Process as set forth in this Amendment. A Deliverable or Service is deemed complete when CTRMA has formally Accepted the Service or Deliverable under the process set forth in this section.
 5. If CTRMA rejects any Services or Deliverable, the cause for rejection and all non-conformities and defects to be addressed must be documented by CTRMA and provided to Vendor for Vendor to correct or revise. The Vendor will correct or revise the Deliverable or Service, as applicable, and resubmit to CTRMA for review withing five (5) business days from receipt of CTRMA's notice of Rejection or such other time as agreed upon in writing between the parties, unless the Vendor is not in agreement with the Rejection, in which case the parties will invoke the Escalation Process set forth in this Amendment. Any Services and Deliverables are deemed complete upon re-performance and/or resubmission of the corrected or revised Services or Deliverable by Vendor to CTRMA.

The following person(s) has been designated as the CTRMA approver of Deliverables and Services for the project:

Name: *Greg Mack*
 Title: *Director of Information Technology*

4. Project Governance

4.1. Project Issues Management

Throughout the Term of the Agreement, issues may arise requiring further information or a decision for resolution. The project team’s objective is to resolve all issues at the lowest level possible. When an issue cannot be resolved at the project team level, the following escalation path will be followed. Each contact shall have the amount of time indicated in the “Response Time” column for bringing resolution to the issue, prior to the issue being escalated to the next contact level.

Table 1: Escalation Contacts

Tier	Vendor	CTRMA	Response Time
First Level Contact	<i>Name, Title</i>	Name, Title	Three (3) business days
Second Level Contact	<i>Name, Title</i>	Name, Title	Three (3) business days
Third Level Contact	<i>Name, Title</i>	Name, Title	Three (3) business days

Should no resolution be reached after following this escalation path, either party may terminate this Agreement as a termination for convenience subject to the Early Termination provisions defined herein, and/or to the dispute resolution process defined in the Agreement, if any, and exercise any other rights and remedies available at law or in equity.

4.2. Change Process

The following Change Process will be used to manage all alterations to this Agreement. Examples of alterations include but are not limited to changes in scope, to Deliverables (including accepted Deliverables), to the schedule and to costs occurring for any reason, including failure of CTRMA to fulfill its roles and responsibilities, unforeseen events, delays caused by CTRMA, and inaccurate assumptions and dependencies. Vendor will not perform services not described in this Agreement until a Change Order has been approved.

4.2.1. Change Order Process

1. Either party shall notify the other of requested changes by completing a “**Change Order**” (“**CO**”) form that provides justification for the change and the proposed impact to the scope, schedule, and cost.
2. If CTRMA initiates the CO, Vendor will respond to the CO with the impact to the scope, schedule, and cost, also referred to as a CO in this process.

3. The CTRMA approver will approve or reject the requested Change Order within five (5) business days from the receipt of the CO form.
4. If the CTRMA approver does not approve or reject the requested Change Order within five (5) business days from the receipt of the CO form and does not communicate a reasonable timeframe in which a decision will be made, the requested Change Order will be considered deferred:
 - a. The CO status will be logged, tracked, and managed as a 'deferred' request.
 - b. Services will progress without incorporating the requested change into the work plan.
 - c. Where an approval or rejection decision is necessary for the Services under this Agreement to progress, Vendor and CTRMA will use the Issues Management process above.
5. For COs outside the stated project scope, CTRMA will authorize budget allowance and payment, on a time and materials basis, for Vendor to perform the initial analysis of a requested change.
6. Vendor shall coordinate any changes in hardware, network, software, configuration, or Services with CTRMA. CTRMA may defer the change based on impact to business operations.
7. Vendor and CTRMA shall work in good faith to resolve disputes regarding the In-Scope or Out-of-Scope classification of work, using the Issues Management process above.

4.2.2. Change Order Approvals

The following persons are responsible for obtaining signature approval of Change Orders for the engagement:

Vendor		CTRMA
Name	Uday Katira	Greg Mack
Role	Managing Director	IT Manager

4.3. Unforeseen Conditions and Events

If unforeseen conditions are discovered or unforeseen events occur that materially affect the original scope of work, Vendor will work with CTRMA to adjust the scope, cost and schedule of this Agreement using the above Change Process or to terminate this Agreement without penalty.

4.4. Delays and Extensions

Vendor has a limited ability to mitigate the impact of delays caused by CTRMA or by events outside Vendor's control. Vendor's rates, prices, and schedules do not include a contingency for the cost and schedule impacts of such delays.

Vendor will notify CTRMA promptly upon discovery of any delay caused by CTRMA or caused by events outside CTRMA's or Vendor's control and Vendor will work with CTRMA to mitigate the cost and schedule impacts;

however, Vendor will be entitled to adjust the schedule accordingly and shall inform CTRMA of any charges for additional work caused by such delays. Vendor will submit a Change Order for required cost and schedule adjustments. Vendor reserves the right to amend any Change Order to address the cumulative impacts of subsequent delays.

5. 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.

6. Compliance with CTRMA Information Security Guidelines

The Vendor shall become familiar with and adhere to CTRMA's Information Security policies, provided that such Information Security Policies (i) do not expand the scope of such services (absent a corresponding change pursuant to the change process herein), (ii) shall not apply to security controls on Vendor's computers, equipment, information systems or networks, (iii) are applicable to Vendor in performance of the services, (iv) do not conflict with or modify the terms of this Contract, or Vendor's own policies, and (v) shall not be deemed to permit CTRMA to conduct and audit, inspection or testing of Vendor's systems, equipment or facilities. 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 A).

7. 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

7.1. 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.

Appendix A: 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

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

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 important 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.

4.13 Treat 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 and 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 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 used to secure sensitive data and hence, compromise of the data. While users may understand it's important to encrypt certain documents and electronic communications, they may not be familiar with minimum standards for protecting 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 CTRMA issued 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

Free Use Disclaimer: *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

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 products 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 policies that will preempt normal CTRMA policies for the duration of a declared pandemic. These policies 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 posture 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 your 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 OPSS\$ 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 is 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.