FACILITY-RELATED CONTROL SYSTEMS

SECURITY AUDIT PLAN (SAP) GUIDELINE

[Replace ESTCP Logo with Organization Logo]

June 20, 2017

Organization Address

City, State, Zip Code

Controlled Unclassified Information (CUI)

Table of Contents

HOW THIS DOCUMENT IS ORGANIZED 5

1.1 DEFINTION 6

1.2 POTENTIAL EVIDENCE OF A SECURITY INCIDENT ..... **Error! Bookmark not defined.**

2.1 CATEGORIES OF EVENTS/INCIDENTS ..... **Error! Bookmark not defined.**

2.2 PRIOR TO REPORTING AN EVENT/INCIDENT ..... **Error! Bookmark not defined.**

2.3 REPORTING AN INCIDENT ..... **Error! Bookmark not defined.**

3.1 ROLES AND RESPONSIBILITIES ..... **Error! Bookmark not defined.**

3.1.1.1 RESPONSIBILITIES: ..... **Error! Bookmark not defined.**

3.1.2 [ORGANIZATION] IT SUPPORT ..... **Error! Bookmark not defined.**

3.1.2.1 RESPONSIBILITIES: ..... **Error! Bookmark not defined.**

3.1.3 [ORGANIZATION] COMPUTER INCIDENT RESPONSE TEAM (CIRT) ..... **Error! Bookmark not defined.**

3.1.3.1 RESPONSIBILITIES: ..... **Error! Bookmark not defined.**

3.1.4 INFORMATION SYSTEMS SECURITY MANAGER ..... **Error! Bookmark not defined.**

3.1.4.1 RESPONSIBILITIES: ..... **Error! Bookmark not defined.**

3.1.5.1 RESPONSIBILITIES: ..... **Error! Bookmark not defined.**

3.2 US-CERT INCIDENT HANDLING FOR DIFFERENT LEVELS OF SEVERITY ..... **Error! Bookmark not defined.**

3.3 CYBERCOM INCIDENT HANDLING FOR DIFFERENT LEVELS OF SEVERITY ..... **Error! Bookmark not defined.**

3.4 INCIDENT REPORTING PROCESS FLOWCHART ..... **Error! Bookmark not defined.**

.....**Error! Bookmark not defined.**

EXECUTIVE SUMMARY

This security audit process documentation details the steps taken to verify software and hardware is functioning as intended, event and audit logs are reviewed, potential vulnerabilities are identified and addressed, patch management is current, continuous monitoring is functional and indicators of compromise or exploit are identified and appropriate action is taken in a timely manner.

The security audit process is done on a monthly basis and is compared to previous and baseline configurations to identify any systemic changes to the [ORGANIZATION] Systems. This document is used in conjunction with the IT policies and procedures and ISCP documents.

Prepared by

Identification of Organization that this Document Prepared by		
Logo	Organization Name	
	Street Address	
	Suite/Room/Building	
	City, State Zip	

Prepared for

Identification of Organization that this Document was Prepared for		
Logo	Organization Name	
	Street Address	
	Suite/Room/Building	
	City, State Zip	

Controlled Unclassified Information (CUI)

TEMPLATE REVISION HISTORY

Date	Page(s)	Description	Author
06/20/2017	All	Initial Document - The document was modeled after the NIST recommendations	Michael Chipley

ABOUT THIS DOCUMENT

This document has been developed to provide guidance and procedures for [Organization] Security Audit Plans.

HOW THIS DOCUMENT IS ORGANIZED

This document is divided into three sections. Some sections include subsections.

Section 1	Describes the introduction and provides an overview and includes the purpose of the document as well as the authorities and standards.
Section 2	Describes the Audit Trail Levels
Section 3	Describes the Audit plan roles and responsibilities
Section 4	Describes the Audit plan policy
Section 3	Provides example steps to conduct the audit

1. INTRODUCTION AND PURPOSE

1.1 SECURITY AUDIT PROCESS

The security audit review process will be done monthly by the security team which will consist of members listed within the ITCP but will include at a minimum: the ISSO, the system administrator and security coordinator(s).

1.2 REFERENCES

NIST - Special Publication 800-12: An Introduction to Computer Security - The NIST Handbook
NIST - Sample Generic Policy and High Level Procedures for Audit Trails
NIST - Special Publication 800-26: Security Self-Assessment Guide for Information Technology Systems
NIST - Special Publication 800-92: Guide to Computer Security Log Management

2. AUDIT LEVELS TRAILS

2.1 SYSTEM-LEVEL AUDIT TRAILS

If a system-level audit capability exists, the audit trail should capture, at a minimum, any attempt to log on (successful or unsuccessful), the log-on ID, date and time of each log-on attempt, date and time of each log-off, the devices used, and the function(s) performed once logged on (e.g., the applications that the user tried, successfully or unsuccessfully, to invoke). System-level logging also typically includes information that is not specifically security-related, such as system operations, cost-accounting charges, and network performance.

2.2 APPLICATION-LEVEL AUDIT TRAIL

System-level audit trails may not be able to track and log events within applications, or may not be able to provide the level of detail needed by application or data owners, the system administrator, or the computer security manager. In general, application-level audit trails monitor and log user activities, including data files opened and closed, specific actions, such as reading, editing, and deleting records or fields, and printing reports. Some applications may be sensitive enough from a data availability, confidentiality, and/or integrity perspective that a "before" and "after" picture of each modified record (or the data element(s) changed within a record) should be captured by the audit trail.

2.3 USER AUDIT TRAILS

User audit trails can usually log:

- All commands directly initiated by the user;
- All identification and authentication attempts; and
- Files and resources accessed.

It is most useful if options and parameters are also recorded from commands. It is much more useful to know that a user tried to delete a log file (e.g., to hide unauthorized actions) than to know the user merely issued the delete command, possibly for a personal data file.

3 ROLES AND RESPONSIBILITY

3.1 INFORMATION SYSTEMS SECURITY OFFICER (ISSO)

- Prepare policy guidelines on online monitoring and audit trail recording, protecting, reviewing, and reporting, and report security breaches or anomalies to the Director, ISSO.

3.2 SYSTEM ADMINISTRATOR (SA)

- Periodically monitor user activity, and
- Assist the Security Coordinator and ISSO in reconciling audit trail anomalies.

3.3 SECURITY COORDINATOR(s) (SC)

- Periodically monitor online programmer activity,
- Ensure audit trail functions are operating and reports are reviewed weekly, and
- Immediately inform the ISSO if the audit trail contains anomalies or security breaches.

4.0 AUDIT TRAIL POLICY

The following functions must be recorded:

- Log-in attempts,
- Password changes, and
- File creations, changes and/or deletions.

The audit trail event record should specify:

- Type of event,
- When the event occurred,
- User ID associated with the event, and
- Program or command used to initiate the event.

Audit trails must be reviewed monthly by the Security Coordinator or other authorized company individuals who are not regular users or who do not administer access to the [ORGANIZATION]. The ISSO must review the audit trail monthly.

Anomalies must be immediately reported to appropriate supervisory and/or ISSO for follow-up action.

All audit files shall be stored electronically with a physical hard copy backup placed in a locked room and kept for three years.

5.0 COMPLIANCE

Unauthorized personnel are not allowed to see or obtain sensitive data. The gross negligence or willful disclosure of information can result in prosecution for misdemeanor or felony resulting in fines, imprisonment, civil liability, and/or dismissal.

Step 1: Corporate IT Systems Admin Login Verification

- All system administrators log into the MS AD server console to validate credentials
- All system administrators log into the Office 365 server console to validate credentials
- All system administrators log into the firewalls and wireless access points to validate credentials
- All system administrators log into the corporate business servers to validate credentials
- All system administrators log into the corporate Electronic Security Systems servers to validate credentials

IT System	Name	Verified	
Active Directory		SysAdmin 1	No
Active Directory		SysAdmin 2	No
Remote Desktop Services (RDS 1)		SysAdmin 1	No
Remote Desktop Services (RDS 2)		SysAdmin 2	No
Server 1		SysAdmin 1	No
Server		SysAdmin 2	No
Office365		SysAdmin 1	No
Office365		SysAdmin 2	No
MS Azure		SysAdmin 1	No
MS Azure		SysAdmin 2	No
Cisco Meraki		SysAdmin 1	No
Cisco Meraki		SysAdmin 2	No
LinkSys LAPN (Corp)		SysAdmin 1	No
LinkSys LAPN (Corp)		SysAdmin 2	No
LinkSys LAPN (Guest)		SysAdmin 1	No
LinkSys LAPN (Guest)		SysAdmin 2	No
LinkSys (Voice)		SysAdmin 1	No
LinkSys (Voice)		SysAdmin 2	No
Cisco (Voice)		SysAdmin 1	No
Cisco (Voice)		SysAdmin 2	No

NAS	SysAdmin 1	No
NAS	SysAdmin 2	No
Backup 2012 Server	SysAdmin 1	No
Backup 2012 Server	SysAdmin 2	No
TalkSwitch	SysAdmin 1	No
TalkSwitch	SysAdmin 2	No
Accounting Server	SysAdmin 1	No
Accounting Server	SysAdmin 2	No
HR Server	SysAdmin 1	No
HR Server	SysAdmin 2	No
Electronic Security Systems (PACS, CCTV, IDS)	SysAdmin 1	No
Electronic Security Systems (PACS, CCTV, IDS)	SysAdmin 1	No

Step 2: Microsoft DC Verification of Devices and Accounts (Active Directory)

- Connect to Domain Controller
  - Manually verify [ORGANIZATION] admin group accounts & permissions
    - Active Directory Users and Computers -> [ORGANIZATION].com -> [ORGANIZATION] -> Admins
  - Manually verify [ORGANIZATION] power users group accounts & permissions
    - Active Directory Users and Computers ->. [ORGANIZATION].com -> [ORGANIZATION] -> Power Users
  - Manually verify [ORGANIZATION] service group (Builtin [ORGANIZATION]) accounts & permissions
    - Active Directory Users and Computers -> [ORGANIZATION].com -> Builtin [ORGANIZATION]
  - Manually verify Root Services group accounts & permissions
    - Active Directory Users and Computers -> [ORGANIZATION].com -> Root Services
  - Manually verify TBD group accounts & permissions
    - Active Directory Users and Computers -> [ORGANIZATION].[ORGANIZATION].com -> TBD
  - Manually verify no unknown devices exist in Workstation Surfaces OU & permissions

■ Active Directory Users and Computers -> [ORGANIZATION].[ORGANIZATION].com -> Workstation Surfaces

○ Manually verify no unknown devices exist in Workstation OU & permissions

■ Active Directory Users and Computers -> [ORGANIZATION].com -> Workstations

○ Manually verify no unknown devices exist in Workstation Test OU & permissions

■ Active Directory Users and Computers -> [ORGANIZATION].com -> Workstations Test

● Disable any inactive/terminated users

○ Verification through ISSO of current accounts

● If any system administrators are inactive/terminated, conduct password resets for all system administrators

Step 3: Microsoft RDS Verification of Devices and Accounts (Remote Desktop)

● Remote Desktop Server

○ Manually verify [ORGANIZATION] admin group accounts & permissions

■ Active Directory Users and Computers -> [ORGANIZATION].com -> [ORGANIZATION] -> Admins

Step 4: Microsoft [ORGANIZATION] Verification of Devices and Accounts (CAD, BIM, SKM)

● Remote Desktop Server

○ Manually verify [ORGANIZATION] admin group accounts & permissions

Step 5: Microsoft DC, RDS, [ORGANIZATION] Server2 Verification of Event Logs

● Connect to Domain Controller

○ Event viewer subscription service setup to receive logs from all domain servers.

○ Manually parse event logs to find irregularities

■ Critical events need to be considered highest severity

○ Export event logs for easier sorting and enumeration of event types and sources

■ Baselines will be created for comparison to more easily spot irregularities in event logs from month to month.

○ Irregularities will be noted and investigated

■ Example: APP Server is throwing twice as many events related to TBD in comparison with the month before

- Investigation will begin to determine the cause and resolution will occur

Step 6: Microsoft DC, RDS, Server2 Verification of Security Logs

- Connect to Domain Controller
  - WebRoot Enterprise Console receives all information relating to WebRoot from all clients
  - Review WebRoot logs and reports for irregularities
  - Produce report for WebRoot baseline month to month changes
  - EMET Verification to ensure no injections have taken place that WebRoot has missed
  - Open Executive Summary from within WebRoot
    - Preview Report
    - Print Scheduled Generated Report

Step 7: Office 365

- Office 365
  - Connect to [ORGANIZATION]'s MS Office365
  - Open TBD
  - Open Alarms
  - Verify Alarm Status is consistent

Step 8: MS Azure

- Open MS Azure Login
  - Connect to [ORGANIZATION]'s MS Azure
  - Open TBD
  - Open Alarms
  - Verify Alarm Status is consistent

Step 9: Cisco Meraki

- Open Cisco Meraki Login
  - Connect to [ORGANIZATION]'s Cisco Meraki
  - Open TBD
  - Open Alarms
  - Verify Alarm Status is consistent

Step 10: LinkSys LAPN

- Open LinkSys LAPN Login
  - Connect to [ORGANIZATION]'s LinkSys LAPN
  - Open TBD
  - Open Alarms
  - Verify Alarm Status is consistent

Step 11: LinkSys

- Open LinkSys Login
  - Connect to [ORGANIZATION]'s LinkSys
  - Open TBD
  - Open Alarms
  - Verify Alarm Status is consistent

Step 12: NAS

- Open NA Login
  - Connect to [ORGANIZATION]'s NAS
  - Open TBD
  - Open Alarms
  - Verify Alarm Status is consistent

Step 13: TalkSwitch

- Open TalkSwitch Login
  - Connect to [ORGANIZATION]'s TalkSwitch
  - Open TBD
  - Open Alarms
  - Verify Alarm Status is consistent

Step 14: Business Servers

- Open Business Servers Login
  - Connect to [ORGANIZATION]'s Business Servers
  - Open TBD
  - Open Alarms
  - Verify Alarm Status is consistent

Step 15: SCAP Report

- Run SCAP Tool on Servers, Workstations and Laptops

Step 16: SSL Reports

- Open SSLLabs (https://www.ssllabs.com/ssltest/)
  - Test [ORGANIZATION].com server
- Save Server Final Report
  - Test [ORGANIZATION] browsers (IE, Edge, Chrome, Mozilla, etc.)
- Save Browsers Final Report

Step 17: Comparison of Monthly Reports and Baseline

- Open previous months reports
  - Compare current month to previous month for anomalies
- AD Verification

- Visual verification of Admin & User groups
  - Admin Events
- Excel file
  - MS Azure Alarms
- Visual scan of manually generated alarm status
  - Connection Log
- Excel file
  - EMET Log
- Excel file
  - SSL Reports
- Visual scan of manually generated report
  - Webroot Report (or other SEIM tool; Nessus, Splunk, ForcePoint, etc.)
- Auto-generated PDF

Step 18: Patch Management

- [ORGANIZATION] Corporate IT Servers, Workstations and Laptops
  - [ORGANIZATION] Automatically applied patches (WSUS enabled) and Manual Patches
- MS Azure Servers
  - Manually apply patches on scheduled maintenance
- Printers
  - Vendor manually apply patches on scheduled maintenance
- Wireless Access Points
  - Vendor manually apply patches on scheduled maintenance
- Electronic Security Systems (PACS, CCTV, IDS)
  - Vendor manually apply patches on scheduled maintenance

Step 19: Physical Security & Backup Validation

- Manually inspect server room & storage locker

- Visitor sign-in required at main entrance
- Doors are locked and room is secured
- Alarm system/IDS is functioning
- UPS is functioning and indicator lights all green
- Ensure UPS is up to date with maintenance
- Validate backup copies in safe

Step 20: Resolve Findings

- Within 5 business days findings to be resolved and reported out with a copy to the ISSO, system administrator and security coordinator(s).
- Categorize findings as level 1, 2, 3
- Level 1: High Priority - Immediate Action/High Risk (mitigate with 5 business days)
- Level 2: Moderate Priority - Businessweek/Moderate Risk (mitigate with 30 business days)
- Level 3: Low Priority - Review for next security audit/Low Risk (mitigate when feasible/possible)
- Update POAM