

Timeline Requirements for Statewide IT Control Standards and Plan

This document contains time-based requirements in the Statewide IT Control Standards and Statewide Information Security Plan. To reduce document length, listed items solely cover the section that contains time-based criteria and **will not** include items without time requirements even if adjacent and contextual to the mentioned item, so refer to the full Standards and Plan for the complete list of requirements.

Additionally, there are multiple CIS Safeguards that contain time requirements and are related to sections within the standards. Please review the related CIS Safeguards for applicable requirements and related documents.

Standards Time Requirements

Within (Org/other defined time)

- CP-2(3) - Contingency Plan | Resume Essential Missions / Business Functions
- CP-7 - Alternate Processing Site
- CP-8 - Telecommunications Service
- CP-10 - System Recovery and Reconstruction
- PS-7 - Third-Party Personnel Security

Minute(s)

- AC-7 - Unsuccessful Logon Attempts
- AC-11 - Device Lock
- AC-12 - Session Termination
- CM-8(3) - System Component Inventory | Automated Unauthorized Component Detection
- SC-10 - Network Disconnect

Hours/Hourly

- AC-2 – Account Management
- AC-2(3) Account Management | Disable Accounts
- AC-2(13) - Account Management | Disable Accounts for High-Risk Individuals
- IR-6 - Incident Reporting
- PS-5 - Personnel Transfer
- SC-45(1) - System Time Synchronization | Synchronization with Authoritative Time Source

Days/Daily

- AC-2(2) - Account Management | Automated Temporary and Emergency Account Management
- AU-11 - Audit Record Retention
- CP-3 - Contingency Training
- CP-9 - System Backup
- IA-5 - Authenticator Management
- IA-5(1) - Authenticator Management | Password-Based Authentication
- IA-11 - Identification and Authentication | Re-Authentication
- IR-2 - Incident Response Training
- PS-4 - Personnel Termination
- PS-8 - Personnel Sanctions
- RA-5 - Vulnerability Monitoring and Scanning
- SI-2 - Flaw Remediation

Weekly

- AU-6 - Audit Review, Analysis, and Reporting
- SI-3 - Malicious Code Protection

Monthly

- CA-5 - Plan of Action and Milestones
- CM-8 - System Component Inventory
- PE-6 - Monitoring Physical Access
- PE-8 - Visitor Access Records
- SI-6 - Security Function Verification

Quarterly

- AC-22 - Publicly Accessible Content
- CM-5(5) - Access Restrictions for Change | Privilege Limitation for Production and Operation

Annually/yearly

- AC-6(7) - Least Privilege | Review of User Privileges
- AT-2 - Security Awareness and Training
- AT-3 - Role-Based Training
- AT-4 - Security Training Records
- AU-2 - Events Logging
- CA-2 - Security Assessments
- CA-3 - System Interconnections
- CA-6 - Authorization
- CA-7 - Continuous Monitoring
- CA-8 - Penetration Testing
- CA-9 - Internal System Connections

- CM-2 - Baseline Configuration
- CM-7(1) - Least Functionality | Periodic Review
- CM-7(5) - Least Functionality | Authorized Software – Allow by Exception
- CP-2 - Contingency Plan
- CP-4 - Contingency Plan Testing
- CP-9(1) - *System Backup | Testing for Reliability and Integrity*
- IA-4 - Identifier Management
- IR-3 - Incident Response Testing
- IR-8 - Incident Response Plan
- IR-9(2) - Information Spillage Response | Training
- MA-3 - Maintenance Tools
- PE-2 - Physical Access Authorizations
- PE-3 - Physical Access Control
- PL-2 - Security Plans
- PL-4 - Rules of Behavior
- PL-8 - Security Architecture
- PS-2 - Position Risk Designation
- PS-6 - Access Agreements
- RA-3 - Risk Assessment
- RA-3(1) - Risk Assessment | Supply Chain Risk Assessment
- SC-7(4) - Boundary Protection | External Telecommunications Services
- SR-2 - Supply Chain Risk Management Plan
- SR-6 - Supplier Assessments and Reviews

Statewide Plan Time Requirements

Annually/yearly

- 8 (AT) Awareness and Training
- 19 (PM) Program Management
 - 19.1.8 PM-9 RISK MANAGEMENT STRATEGY
 - 19.1.10 PM-11 MISSION AND BUSINESS PROCESS DEFINITION
 - 19.1.16 PM-17 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION ON EXTERNAL SYSTEMS
 - 19.1.17 PM-21 ACCOUNTING OF DISCLOSURES