Commonwealth of Massachusetts
Executive Office of Technology Services and Security (EOTSS)
Enterprise Risk Management Office

Asset Management Standard

Document Name: Asset Management	Effective Date: October 15th, 2018
Document ID: IS.004	Last Revised Date: November 16, 2023

Table of contents

1. Purpose 2
2. Authority 2
3. Scope 2
4. Responsibility 2
5. Compliance 2
6. Standard Statements 3
   6.1. Information Asset Management 3
   6.2. Information Classification 4
   6.3. Information Labeling and Handling 5
   6.4. Information Disposal 6
   6.5. Information Protection Requirements 8
   2. 8
   6.6. Information System Classification 8
   6.7. Endpoint Security 9
   6.8. Mobile Device Management 10
7. Control Mapping 13
8. Related Documents 13
9. Document Change Control 14

1. PURPOSE

1.1. The purpose of this ***standard*** is to document the requirements and key security considerations to enable the ongoing ownership and effective management of Commonwealth's ***information assets***.

2. AUTHORITY

2.1. M.G.L. Ch. 7d provides that "Notwithstanding any general or special law, rule, regulation, executive order, policy or procedure to the contrary, all executive department agencies shall, and other state agencies may, adhere to the policies, procedures and objectives established by the executive office of technology services and security with respect to activities concerning information technology."

3. SCOPE

3.1. This document applies to the use of ***information***, ***information systems***, electronic and computing devices, ***applications***, and network resources used to conduct business on behalf of the Commonwealth. The document applies to the Executive Branch including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus, hereinafter referred to as Commonwealth Agencies and Offices. Other Commonwealth entities that voluntarily use or participate in services provided by the Executive Office of Technology Services and Security, such as mass.gov, must agree to comply with this document, as a condition of use. Commonwealth Agencies and Offices are required to implement ***procedures*** that ensure their ***personnel*** comply with the requirements herein to safeguard ***information***

4. RESPONSIBILITY

4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this ***standard***.

4.2. The Enterprise Risk Management Office is responsible for this ***standard*** and may enlist other departments to assist in maintaining and monitoring compliance with this ***standard***.

4.3. Any inquiries or comments regarding this ***standard*** must be submitted to the Enterprise Risk Management Office by sending an email to ERM@mass.gov.

4.4. Additional information regarding this ***standard*** and its related ***standards*** may be found at https://www.mass.gov/cybersecurity/policies.

5. COMPLIANCE

5.1. Compliance with this document is mandatory for the Executive Branch including all executive offices, boards, commissions, agencies, departments, divisions, councils, and bureaus, hereinafter referred to as Commonwealth Agencies and Offices. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

Exceptions to any part of this document must be requested online through ServiceNow, https://www.mass.gov.service-now.com). A ***policy exception*** may be granted only if the benefits of the ***exception*** outweigh the increased ***risks***, as determined by the ***Commonwealth CISO*** or his or her designee. Any and all ***exceptions*** will be for a limited time and will be narrow in scope***.***

6. STANDARD STATEMENTS

6.1. Information Asset Management

All ***information assets*** will be accounted for and have an assigned owner.

6.1.1. Inventory of ***information assets***

Commonwealth Agencies and Offices will identify all ***information assets*** (i.e., physical, and logical) and document the importance of these ***assets***. The ***asset*** inventory must include all ***information*** necessary in order to effectively manage the ***information asset*** throughout its life cycle from creation/receipt through disposal. At a minimum, the following attributes will be recorded (where applicable):

6.1.1.1. ***Information system*** type (e.g., server, router, computer, smartphone)

6.1.1.2. Manufacturer (e.g., Cisco, Dell, Apple)

6.1.1.3. Model and/or version number

6.1.1.4. ***Asset*** tag, serial number, or some other unique identifier

6.1.1.5. IP address (if applicable)

6.1.1.6. ***Information Owner*** (business and technical)

6.1.1.7. Classification level

6.1.1.8. Business criticality

6.1.1.9. Physical location (office building, room, city, and state) and details of the virtual environment (if applicable)

6.1.1.10. License ***information*** and details regarding ownership, expiration and maintenance (if applicable)

6.1.1.11. End-of-support/end-of-life date and considerations (if applicable)

6.1.2. Ownership of ***information assets***

Information Owners will be identified for all ***information assets***. The implementation of specific ***controls*** may be delegated by the ***Information Owner***, as appropriate, but the owner remains responsible for the management and security of the ***information asset***. Specifically, the ***Information Owner*** will:

6.1.2.1. Ensure that the ***information asset*** is accurately inventoried and classified.

6.1.2.2. Ensure that the ***information asset*** has appropriate access restrictions.

6.1.2.3. Perform periodic reviews of the ***information asset*** inventory, not less than annually, to ensure all ***assets*** are properly documented.

6.1.2.4. Perform periodic reviews to verify appropriate access; review frequency will be dictated by the ***application*** classification level.

6.1.2.5. Manage ***risk*** to the ***information asset***, including mitigating the ***risks*** associated with operating at end-of-support/end-of-life (if applicable).

6.1.3. Acceptable use of ***assets***

6.1.3.1. All Commonwealth Agencies and Offices with ***personnel*** that access to ***information assets*** owned or managed by the Commonwealth must comply with the associated permissions and restrictions as documented in *IS.002 Acceptable Use of Information Technology Policy*.

6.2. Information Classification

The classification or sensitivity level of all ***information*** must be established to ensure that appropriate measures are taken to protect the ***information*** commensurate with its value to the organization and the legal restrictions on its dissemination. The ***Information Custodian*** is responsible for assigning the appropriate classification level. The examples below are not exhaustive lists of all types of ***information***. Determining appropriate classification may be based on a combination of source and content (i.e., PII may be ***Restricted*** or ***Confidential*** depending on source). When ***information*** meets criteria for multiple classifications, it should be classified at the highest level.

6.2.1. ***Restricted*** – Any ***confidential*** or ***personal information*** that is intended for a limited number of persons who possess the highest level of access control and security clearance, and who need the ***restricted information*** to perform their duties. ***Restricted information*** is intended for a very limited use and must not be disclosed except to those who have explicit authorization to view or use the ***data***. Unauthorized disclosure of this ***information*** could have a serious adverse impact on the financial, legal, regulatory, or reputational impact on the Commonwealth, its constituents, customers, and business partners. *(see IS.Glossary of Terms).*

6.2.2. ***Confidential*** — organization or customer ***information*** that if inappropriately accessed or disclosed could cause adverse financial, legal, regulatory, or reputational damage to the Commonwealth, its constituents, customers, and business partners. *(see IS.Glossary of Terms).*

Except as required by law, ***confidential information*** must be access-restricted to a narrow subset of ***personnel*** who have a business need to access the ***information***. Examples may include but are not limited to:

6.2.2.1. ***Personally identifiable information (PII)***

6.2.2.2. Regulated ***information*** (Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI), Federal Tax Information (FTI) and other types of ***information***)

6.2.2.3. Employee performance and appraisal documentation

6.2.2.4. Internal, external, and regulatory audit reports.

6.2.2.5. ***Information*** on the Commonwealth's security posture (e.g., firewall setting ***information***, security configurations, ***vulnerability*** test reports, breach reports)

6.2.2.6. Passwords or any form of security ***key***

6.2.3. ***Internal Use*** — ***information*** that has NOT been expressly authorized for public release but that has not been classified as ***confidential*** or ***restricted***. The disclosure of ***Internal Use information*** is unlikely to have a material financial, legal, regulatory, or reputational impact on the Commonwealth, its constituents, customers, and business partners. Examples may include but are not limited to:

6.2.3.1. Organization charts and ***personnel*** directories

6.2.3.2. Internal policies and documentation

6.2.3.3. ***Personnel*** awareness and training collateral

6.2.4. ***Public*** — ***information*** that has been expressly approved for public release. ***Information*** can only be designated as Public by the authorized ***personnel***; each Secretariat is responsible for maintaining the list of authorized ***personnel***. Examples may include but are not limited to:

6.2.4.1. Press releases

6.2.4.2. ***Information*** on public facing websites (e.g., Mass.gov)

6.2.4.3. Promotional materials for Commonwealth constituent services (e.g., Medicaid enrollment)

6.2.4.4. Advertising of open positions and roles

6.3. Information Labeling and Handling

6.3.1. Procedures for the handling and labeling of ***information***, both in electronic and physical formats, will be defined and maintained by each Secretariat and will also comply with legal and regulatory obligations.

6.3.2. ***Data*** loss prevention (DLP) technologies approved or managed by the Enterprise Security Office will be implemented to monitor ***data***-at-rest, ***data***-in-transit, and ***data***-in-use.

6.3.3. ***Information*** must be protected in line with its assigned level of classification. Classification levels must be reviewed and updated at least annually.

6.3.4.1. Limit direct access to ***confidential*** customer ***information*** (e.g., SSN) whenever possible. Access to ***information*** must be limited to those with a need to know.

6.3.4.2. Use disclaimer statements when transferring ***information*** to internal and external parties.

6.3.4.3. The sending of Commonwealth ***restricted*** or ***confidential information*** to personal email addresses (e.g., Gmail or Yahoo Mail) is prohibited.

6.3.4.4. Use ***encryption*** to protect ***data*** at rest and in transit, commensurate to its classification level (See *Approved Cryptographic Techniques in IS.008 Cryptographic Management Standard*).

6.3.4. ***Information*** available in a physical format (e.g., paper) will be labeled accordingly.

6.3.5. Protect media containing Commonwealth ***information*** against unauthorized access, misuse, or corruption during transportation.

6.3.5.1 Verify the identity of couriers.

6.3.5.2 Use only authorized couriers to send ***confidential information***.

6.3.5.3 Refrain from marking exterior packaging of ***confidential information*** with the classification level. Package sufficiently to protect the contents from physical damage.

6.3.5.4 Maintain an audit ***log*** of the content of the media, including the ***information*** protection applied and transportation logistics.

6.3.6. Commonwealth Agencies and Offices will by default, restrict removable media use by ***personnel*** (see *Endpoint Protection* in IS.004 *Asset Management Standard*). Removable media use will only be granted on an ***exception*** basis when there is a compelling organizational need.

6.4. Information Disposal

Establish procedures for the secure disposal and sanitization of media to minimize the ***risk*** of ***restricted*** or ***confidential information*** leakage. ***Information*** will be retained in accordance with applicable laws, executive orders, directives, regulations, ***policies***, ***standards***, guidelines, and operational requirements, including the Massachusetts Statewide Records Retention Schedule.

6.4.1 Log the disposal of ***restricted*** and/or ***confidential information*** to maintain an audit trail

6.4.2 Verify that the ***information assets*** containing any ***restricted*** and/or ***confidential information*** have been removed or securely overwritten prior to ***disposal*** or reuse.

6.4.2.1 Render media unusable (e.g., degaussing), unreadable or indecipherable prior to disposal.

6.4.2.2 Use acceptable industry best practices and standards (e.g., 7-pass overwrite) for ***information*** erasure to ensure ***information*** is unrecoverable.

6.4.2.3 Use a ***third-party*** service that specializes in ***information*** or media disposal.

6.4.2.4 Identify and securely delete stored ***information*** that exceeds defined retention periods on a quarterly basis.

6.4.2.5 Hard copies of ***information*** will only be generated when necessary. Excess copies must be disposed of securely (e.g., shredding).

6.4.2.6 Regulatory compliance requirements may supersede this ***standard***.

6.4.2.7 Obtain a disposal certificate or other written attestation from the ***third-party*** confirming proper disposal

6.5. Information Protection Requirements

The following table summarizes the ***information*** protection requirements for Commonwealth ***information***.

Security Considerations	Public	Internal Use	Confidential
Impact of unauthorized disclosure	No harm.	Limited harm.	Significant harm.
Access restrictions	None.	Access normally restricted to employees and approved non-employees for business purposes only.	Access granted only to authorized individuals.
Encryption	None required.	None required.	Commonwealth-approved ***encryption*** required (see Approved Cryptographic Techniques in the Cryptographic Management Standard).
Physical labeling (paper, magnetic media, CD/DVD/USB, or tape label)	None required.	***Information*** classification label must be visible. All magnetic media assets must be sent in lockable containers with a label affixed across the opening of the container.	***Information*** classification label must be visible. All magnetic media assets must be sent in lockable containers. The label should not be affixed on outside of shipping container.
Electronic labeling (digital file, email, or webpage)	None required.	E-mail: non-disclosure disclaimer must be visible.	E-mail: ***information*** must be labeled and ***encrypted***.
Physical disposal (paper, tape, or hard drives)	None required.	After applicable electronic disposal, secure onsite or off-site physical disposal using Commonwealth-approved methods.	After applicable electronic disposal, secure onsite disposal using Commonwealth-approved methods. Paper – Shred or use secure disposal bins. Electronic media — render unreadable or unrecoverable, depending on the use case. Disposal audit trail required.
Electronic disposal (Digital file)	None required.	Removal of the directory entry for the file.	Removal of the directory entry for the file. File space should be over-written using best industry standards where possible.

6.6. Information System Classification

To promote a consistent approach to ***risk*** management, business continuity and disaster recovery, etc. process, all ***information systems*** must be classified. ***Information Owners*** are responsible for determining the ***information system*** classification of their ***information system***.

6.6.1 The classification of an ***information system*** must be based on its most critical component (e.g., where ***information*** is transmitted, processed, or stored).

6.6.2 Commonwealth Agencies and Offices must conduct a ***business impact analysis*** or a ***risk*** assessment to determine ***information system*** classifications for their ***information assets***.

6.6.3 ***Information system*** classification must be reviewed at least annually and whenever a significant system change occurs.

6.6.4 Classify all ***information systems*** as follows:

Classification level(s)		Description
🟧🟧🟧🟧⬜	Critical	● ***Information assets*** subject to legal and/or regulatory requirements if breached (e.g., HIPAA, FTI, PII, PCI) ● Critical core network infrastructure, including perimeter firewalls, routers, switches, domain name server (DNS) and cloud services ● Systems that generate or manage in excess of $1m or more per annum for the Commonwealth (e.g., HIX, MMIS) ● Systems involved in the transmission or processing of financial ***information*** ● ***Restricted information***
🟥🟥🟥⬜⬜	High	● High-value ***assets*** that store, process, or transmit ***restricted*** and/or ***confidential information*** ● Core business support systems (e.g., email) ● Externally facing systems that process or handle ***restricted*** and/or ***confidential information*** ● Systems that impact payroll or similar internal processes ● End-of-life ***information systems*** no longer supported by a vendor and without a ***risk exception*** on file ● ***Confidential information***
🟨🟨⬜⬜⬜	Medium	● Non-core business support systems, including externally facing systems that do not process ***restricted*** and/or ***confidential information*** ● ***Internal Use information***
🟦⬜⬜⬜⬜	Low	● Development, test and quality assurance environments or ***user*** workstations ● ***Public information***

6.7. Endpoint Security

6.7.1 ***Endpoint*** security ***controls*** to protect against malicious ***software***, including viruses and ***malware***, will be implemented.

6.7.1.1 Implement antivirus solutions on all ***endpoints***.

6.7.1.2 Implement ***endpoint*** detection and response (EDR) solutions on high-***risk information systems*** (including ***endpoints***) that store ***restricted*** and/or ***confidential information*** and ***data*** persistently.

6.7.1.3 Configure antivirus and/or EDR solutions to detect, remove and protect against known types of malicious ***software***.

6.7.1.4 Configure antivirus and/or EDR solutions so that they cannot be circumvented, disabled, or removed from an ***endpoint*** by an end ***user***.

6.7.1.5 Update antivirus definitions in accordance with their severity rating (*see IS.016 Vulnerability Management Standard*). Signature definitions must be centrally managed and pushed to ***endpoints***. End ***users*** must not be able to prevent updates to their Commonwealth-issued ***endpoint***.

6.7.1.6 Retain audit ***logs*** for antivirus and EDR solutions for at least one year with a minimum of three (3) months readily available for analysis (*see IS.011 Logging and Event Monitoring Standard*).

6.7.1.7 Integrate antivirus and EDR solutions with the enterprise SIEM, where technically feasible.

6.7.1.8 Full-disk ***encryption*** must be configured for all laptops. Desktops that store ***restricted*** and/or ***confidential information*** on a persistent basis must implement full-disk ***encryption***.

6.7.1.8.1 ***Encryption keys*** must be centrally managed. Mechanisms to recover ***encryption keys*** in the case of loss will be available and tested.

6.7.2 Implement host-based firewall solutions for ***information systems*** with direct connectivity to the Internet (e.g., laptops used by ***personnel*** at home or on public Wi-Fi), which are used to access the organization's network.

6.7.3 Implement host-based firewalls for end of life (EOL) ***information systems***.

6.7.4 Implement host-based intrusion prevention systems (IPS) on high-***risk*** systems.

6.7.5 Implement ***controls*** to protect ***endpoints*** from virus and ***malware*** that can be introduced via removable media (e.g., USB storage media).

6.7.5.1 Auto scan removable media for virus and ***malware*** prior to use.

6.7.5.2 Disable functionality that allows auto-run upon insertion of removable media.

6.7.5.3 Force ***encryption*** on removable media prior to allowing ***information*** transfer to and from the media.

6.7.6 Implement technical ***controls*** to restrict the installation of unauthorized ***software*** on Commonwealth-owned or managed ***endpoints***.

6.7.7 Restrict the use of local administrator privileges on ***endpoints***.

6.7.7.1 Individuals with a verified business need (e.g., help desk or designated ***security administrators***) may, via their direct managers, submit an ***exception*** request as detailed above, to obtain local administrator privileges.

6.7.7.2 An up-to-date inventory of ***users*** with persistent access to administrative privileges must be maintained and reported to the ***Commonwealth CISO*** or his or her designee, on a quarterly basis.

6.7.8 Perform a full antivirus and anti-***malware*** scan on ***endpoints***, at a minimum, monthly.

6.7.9 ***Third parties*** that require a connection to the Commonwealth family of networks must have up-to-date antivirus and anti-***malware*** solutions installed.

6.7.10 Ensure that Commonwealth-owned or managed devices do not leave the United States.

6.8. Mobile Device Management

The Commonwealth will implement a mobile device management (MDM) solution, approved, and maintained by the Enterprise Security Office, to manage mobile devices in its environment.

6.8.1 The MDM solution will support, at a minimum, the following functionalities:

6.8.1.1 Provide the highest coverage of mobile devices and operating systems

6.8.1.2 Have the ability to remotely update firmware and ***applications*** on mobile devices.

6.8.1.3 Inventory management (i.e., self-enrollment, directory integration, enforcement of *IS.002 Acceptable Use Policy* , remote wipe, backup and restore)

6.8.1.4 Device policy management (i.e., centralized enforcement of policy, group/location policies, compliance checks)

6.8.1.5 Security management (i.e., ***information*** and device ***encryption***, ***information*** segmentation, logging and monitoring, password/PIN management, jailbreak detection)

6.8.1.6 Monitoring and reporting (i.e., configurable dashboard, device tracking, canned/custom reporting)

Controls will be implemented to prevent unauthorized disclosure of ***information*** on mobile devices (e.g., mobile phones and tablets). At a minimum, Commonwealth Agencies and Offices will adhere to the following:

6.8.2 ***Users*** must obtain authorization to use a personal mobile device to directly access Commonwealth ***information***.

6.8.2.1 ***Users*** that voluntarily choose to use their personal mobile device for Commonwealth business must sign off that they understand the ***risk*** of using a mobile device and adhere to Commonwealth ***policies*** and ***standards***.

6.8.2.2 Sign off that he/she understands and accepts ***risks*** associated with using a mobile device that is owned or managed by the Commonwealth, including inclusion in the mobile inventory, installation of an MDM solution, enforcement of password policy, authorization to review and retrieve phone ***information*** and remote wipe.

6.8.3 Create an inventory of all mobile devices (Commonwealth-owned and personal) that connect to the Commonwealth family of networks. The inventory must be reviewed at least annually and include ownership ***information*** and device specifications (e.g., manufacturer, model, OS).

6.8.4 Personal mobile devices that directly connect to the Commonwealth family of networks or that have direct access to Commonwealth's ***confidential information*** must connect via VPN and an inventory of devices authorized to connect must be actively maintained (see *Remote Access in IS.006 Communication and Network Security Standard, and Information Asset Management in IS.004 Asset Management Standard*).

6.8.5 Commonwealth-owned ***information***-at-rest on mobile devices must be ***encrypted*** with an approved ***software encryption*** solution (see *Approved Cryptographic Techniques in IS.008 Cryptographic Management Standard*).

6.8.6 Enforce password requirements for mobile devices through technical means as outlined in *Password Management in IS.004 Access Management Standard*.

6.8.7 Restrict mobile device ***users*** from making modifications of any kind to Commonwealth-owned or installed hardware and ***software*** on the mobile device.

6.8.8 Mobile devices, regardless of ownership, housing Commonwealth ***information*** will be securely decommissioned, when no longer needed for business or legal reasons.

6.8.9 Commonwealth Agencies and Offices must ensure mobile device ***users*** are aware of the ***risks*** involved with mobile computing and the types of ***information*** that can and cannot be stored on such devices, through regular security awareness training.

7. CONTROL MAPPING

Section	NIST SP800-53 R4 (1)	CIS 18 V8	NIST CSF
6.1 Information Asset Management	CM-8	CSC 1	ID.AM-1
	CM-9	CSC 4	PR.IP-1
	PM-5	CSC 1	-
	PL-4	-	-
	CM-10	CSC 2	ID.AM-2
	CM-11	CSC 2	
6.2 Information Classification	RA-2	CSC 3	ID.AM-5
	AC-22	CSC 14	
6.3 Information Labeling and Handling	AC-16	-	PR.AC-4
	MP-1		
	MP-2	CSC 3	PR.PT-2
	MP-3	-	-
	SC-16	-	-
6.4 Information Disposal	SI-12	CSC 3	-
			PR.IP-6
	MP-6	CSC 3	PR.DS-3
6.5 Information Protection Requirements			
	AC-3	CSC 3	PR.AC-4
		-	-
	SC-28	CSC 3	PR.DS-1
	SI-12	CSC 3	-
6.6 Information System Classification	RA-2	CSC 3	ID.AM-5
6.7 Endpoint Security		-	PR.DS-3
	SI-12	CSC 3	-
		-	-
	MP-2	CSC 3	
	MP-7	CSC 3	
		-	PR.AC-2
		-	PR.AC-2
		-	PR.AC-2
		-	-
		-	-
		-	PR.IP-5
		-	ID.GV-1
	AU-2	CSC 3	PR.PT-1
			PR.PT-1
			PR.DS-4
			PR.PT-1
			PR.PT-1
			PR.PT-1
			PR.PT-1
			PR.PT-1
			PR.PT-1
			PR.PT-1
	SI-4	CSC 1	ID.RA-1
		-	DE.DP Family
6.8 Mobile Device Management	CM-8	CSC 1	ID.AM-1
		-	ID.GV-1
	AC-17	CSC 3	PR.AC-3
			PR.PT-4
	AC-19	CSC 4	PR.AC-3
	PL-4	-	-
	PS-6	CSC 13	PR.DS-5
		-	-

8. RELATED DOCUMENTS

Document	Effective date

9. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.9	Jim Cusson	10/01/2017	Corrections and formatting
0.95	John Merto	12/22/2017	Wording
0.96	Sean Vinck	5/7/2018	Corrections and formatting
0.97	Andrew Rudder	5/31/2018	Corrections and Formatting
0.98	Anthony O'Neill	05/31/2018	Corrections and Formatting
1.0	Dennis McDermitt	6/1/2018	Final Pre-publication Review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Sean M. Hughes	08/29/2022	Minor Updates to meet NIST 800-53R5; annual review
1.4	Thomas E. McDermott	11/16/2023	Corrections, formatting, updating and Annual Review
1.5	Anthony O'Neill	11/16/2022	Final Review

The owner of this document is the ***Commonwealth CISO*** (or his or her designee). It is the responsibility of the ***document owner*** to maintain, update and communicate the content of this document. Questions regarding this document must be submitted to the ***document owner*** by sending an email to ERM@mass.gov.

9.1 Annual Review

This *Asset Management Standard* should be reviewed and updated by the ***document owner*** on an annual basis or when significant ***policy*** or ***procedure*** changes necessitate an amendment.