Commonwealth of Massachusetts

Massachusetts Office of Information Technology

# Enterprise IT Asset and Risk Management Policy

**Reference #: ITD-SEC-8.2 Revision Date: March 6, 2014
Issue #: 2**

## Table of Contents

[Table of Contents 1](#_Toc438479635)

[Executive Summary 1](#_Toc438479636)

[Whom this Policy Applies To 2](#_Toc438479637)

[Policy Statement 2](#_Toc438479638)

[Roles and Responsibilities 6](#_Toc438479639)

[Related Documents 7](#_Toc438479640)

[Contact 8](#_Toc438479641)

[Appendix A: Terms 9](#_Toc438479642)

[Appendix B: Document History 10](#_Toc438479643)

## Executive Summary

This policy articulates requirements for performing annual reviews of Secretariats’ and their respective Agencies’ IT (Information Technology) assets, determining appropriate data classifications and controls, and assessing and reacting to risks in order to safeguard those assets. Secretariats and their respective Agencies must institute periodic reviews and risk assessments based on changes in the IT environment including new threats, vulnerabilities and consequences to ensure the continued effectiveness of the implemented controls. The purpose of employing such a process is to institute remediation where warranted to reasonably ensure that planned and deployed controls meet the security goals of the agency and the Commonwealth enterprise.

It is the responsibility of the Secretariat Chief Information Officers and Agency Heads to have controls in place and in effect that provide reasonable assurance that the overall information security goals of the Commonwealth are met. This includes compliance with laws, regulations, policies and standards to which their technology resources and data, including but not limited to personal information (PI), are subject.

## Whom this Policy Applies To

Secretariats and their respective Agencies and entities governed by the overarching [Enterprise Information Security Policy](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html)[[1]](#footnote-2) must adhere to the requirements of this supporting policy.

* Executive Department Secretariats and their respective Agencies, [[2]](#footnote-3) in addition to any agency or third party that connects to the Commonwealth’s wide area network (MAGNet), must comply with this policy.
* Executive Department Secretariats and their respective Agencies are required to ensure compliance by any business partner that accesses Executive Department IT Resources or shared environments, e.g. MAGNet; and
* Executive Department Secretariats and their respective Agencies are required to ensure compliance with this policy by third parties in any aspect of the process of providing goods and services to their agency. These include, but are not limited to, access control (including VPN), electronic data collection, storage, processing, disposal, dissemination and maintenance. Third parties that interact in any way with Executive Department Commonwealth IT Resources, e.g. MAGNet, are required to comply with this policy.

Other Commonwealth entities are encouraged to adopt security requirements in accordance with this policy or a more stringent agency policy that addresses agency-specific directives, laws, and regulations.

## Policy Statement

Secretariats and their respective Agencies are required to implement policies, associated procedures and controls that identify and protect their IT assets from all threats, whether internal or external, deliberate or accidental. The controls for classified data must be commensurate with the level of identified risk, based on business value and importance of the asset, regulatory requirements and interagency agreements that may pertain to agency acquisition, use or maintenance of the data.

Secretariats and their respective Agencies must implement ongoing Asset Management procedures including inventory of identified IT assets, ownership and business value of those assets, and information classification of the assets. In addition, they must adopt Risk Management (Risk Assessment and Risk Treatment) procedures that implement necessary security controls to minimize the identified risks to an acceptable level. Once data is assigned the appropriate data classification level, agencies must conduct a Risk Assessment to determine acceptable levels of risk and the appropriate level and combination of security controls (administrative, technical and physical) for IT systems.

In accordance with this IT asset and risk management policy, the practitioner must apply the Plan-Do-Check-Act methodology as it pertains to the Risk Management process:

* Plan: Establish the context of the Risk Assessment; conduct the Risk Assessment; develop the Risk Treatment Plan; and perform Risk Acceptance if applicable
* Do: Implementation of the Risk Treatment Plan
* Check: Continual monitoring and reviewing of risks
* Act: Maintain and improve the Information Security Risk Management Process

### IT Asset Management:

Secretariats and their respective Agencies are required to manage and maintain their IT assets, including but not limited to personal information, by assigning the responsibility of asset management in the following areas:

* 1. Inventory of IT Assets: Secretariats and their respective Agencies must maintain an inventory of IT assets which consist of physical IT assets (hardware, network devices, etc.) and logical IT assets (data, software, licensing, and applications). Inventories of assets assist in ensuring that effective asset protection takes place and are key to the Risk Assessment process. Secretariats and their respective Agencies must also identify ownership of IT assets, and must collect the following information for each asset which they own and/or are responsible for:
		1. Identify the asset, e.g. ID number, type or description of asset, make or manufacturer, model, serial number, etc.
		2. Identify the location—physical or logical--of the asset and the information classification of each asset.
		3. Identify the relationships and dependencies between physical and logical assets.
		4. Identify the security processes or controls (including access controls, backups, etc.) associated with each asset.
		5. Identify the data owner for each asset with responsibility for ensuring that: the asset is correctly classified, identified controls are maintained on a daily basis, access controls are defined and periodically reviewed, and vulnerabilities are identified.
		6. Determine if the asset contains confidential information including but not limited to personal information as well as the type of personal information (e.g. health information, payment card data, etc.).
		7. Annually conduct a physical audit of IT assets and reconcile the audit with the IT asset inventory. Agencies must investigate and resolve discrepancies between the physical audit of IT assets and the IT asset inventory.
		8. Update and maintain the asset inventory as assets are acquired and/or disposed of throughout the asset lifecycle.
	2. **Information Data Classification:** Secretariats and their respective Agencies governed by this policy must adhere to the standards detailed in the Enterprise Information Security Standards: Data Classification document.
	3. **Tagging/Labeling and Data Handling:** Secretariats and their respective Agencies must consider the IT asset data classification when handling and tagging or labeling assets. Agencies must develop and implement procedures for information tagging and labeling and handling in accordance with the classification scheme referenced in the Enterprise Information Security Standards: Data Classification standard as adopted by the Commonwealth.
	4. **Acceptable Use:** Secretariats and their respective Agencies are required to ensure acceptable use of IT assets (also known as IT resources) through the implementation and enforcement of an Acceptable Use Policy at the Secretariat or Agency level. All entities, e.g. agencies, departments, secretariats, must formally adopt, and comply with, an acceptable use policy. The Executive Office of Administration and Finance (EOAF) has issued an Acceptable Use Policy (AUP) that entities may use or augment with additional procedures and guidelines for the use of IT assets within their respective organizations.

### Risk Management:

Risk Management is fundamental to protecting the Confidentiality, Integrity and the Availability (CIA) of agency IT assets.

Risk management is the continuous process that allows business owners to balance the operational and economic costs of protective measures while achieving gains in mission capability and protecting the IT systems and data that support their organizational goals and objectives.

Risk management encompasses:

* Risk Assessment
* Risk Treatment
* Risk Monitoring and Review
	1. **Risk Assessment:** Risk Assessments are fundamental to the security of the agency and are essential in ensuring that controls and expenditures are fully commensurate with the risks to which the agency is exposed.

Agencies are required to identify, quantify and prioritize risks against operational and control objectives and to design, implement and exercise controls that provide reasonable assurance that objectives will be met and that risk will be mitigated and managed to an acceptable level.

Agencies are required to conduct the Risk Assessment process:

* prior to production implementation of new applications or IT systems;
* when substantive changes have occurred in the IT Resource and IT Organizational environments; and
* at least every 3 years.

The risk assessment methodology ensures that risk assessments produce comparable and reproducible results.

Risk assessments must include at a minimum:

* + 1. Identification of the assets that are within scope
		2. Identification of the threats, the type of threats represented and their sources (e.g. hardware, software, network, media/peripherals, business process, etc.)
		3. Identification of the vulnerabilities for known threats that may be exploited and which assets could be affected
		4. Identification of the controls and their status, as either existing or planned
		5. Identification of the consequences that losses of confidentiality, integrity and availability may produce
		6. Identification of relevant incident scenarios, including the identification of threats, vulnerabilities, affected assets, consequences to assets and business processes
		7. Assessment of the likelihood of incident scenarios, whether Qualitative or Quantitative
		8. Application of a risk estimation methodology (either Qualitative or Quantitative) to measure risk levels
		9. Estimation of the level of risk with appropriate values assigned
		10. Evaluation and prioritization of the risks in relation to incident scenarios and risk levels
	1. **Risk Treatment:** The goal of risk treatment is to reduce risk(s) to the lowest acceptable residual risk level. Risk treatment also includes prioritizing risks and implementing the treatment measures identified during the assessment. Secretariats and their respective Agencies must apply one or more of the following risk treatment measures:
		1. Avoidance: Avoid the risk by eliminating it via alteration of business practice, applying technology, etc.
		2. Mitigation: Reduce the level of risk and/or its impact to the organization.
		3. Transfer: Transfer the risk to another organization (e.g., vendor or business partner) via contractual agreement, or insurance policy.
		4. Manage: Choose to accept and manage the risk.
	2. **Risk Monitoring and Review:** Risks and their factors (asset value, impacts, threats, vulnerabilities, and likelihood) must be monitored and reviewed regularly to identify any changes. Secretariats and their respective Agencies are required to monitor and evaluate the specific controls that must be implemented to meet the stated security objectives.

## Roles and Responsibilities

All agencies and entities governed by the overarching Enterprise Information Security Policy are subject to the referenced roles and responsibilities in addition to those specifically stated within this supporting policy. The roles and responsibilities for compliance with this policy follow:

### Assistant Secretary for Information Technology

* The Assistant Secretary for Information Technology has developed mandatory standards and procedures for Secretariats and their respective Agencies to follow before entering into contracts that provide third parties with access to electronic high sensitivity information, including but not limited to personal information or IT systems containing such information.
* The Assistant Secretary for Information Technology is responsible for the approval and adoption of the Enterprise IT Asset and Risk Management Policy and its revisions.

### Secretariat Chief Information Officer (SCIO) and Agency Head, and Agency Chief Information Officer (CIO)

* SCIOs, Agency Heads, and CIOs are collectively responsible for exercising due diligence in adhering to the requirements contained in this policy, and must either adopt this policy for their agency and/or Secretariat or publish their own in a manner consistent with this policy.
* SCIOs, Agency Heads, and CIOs will collectively provide communication, training and enforcement of this policy that support the security goals of the Secretariat, its agencies and the Commonwealth.
* Agency Heads, SCIOs and CIOs are collectively responsible for ensuring risk assessments are conducted on all new IT systems, applications and major upgrades, and will sign off on the agency’s risk treatment decisions for satisfying IT security objectives.

### Secretariat or Agency Information Security Officer (ISO)

* Ensure that the goals and requirements of the Enterprise IT Asset and Risk Management Policy are implemented and met.
* Ensure that the data owners have authorized the accuracy of the applied classification levels.
* Ensure that appropriate labeling mechanisms are utilized and applied.
* Ensure that this policy is communicated to the appropriate parties.

### Enterprise Security Board (ESB)

* The Enterprise Security Board will recommend revisions and updates to this policy and related standards.

### Massachusetts Office of Information Technology (MassIT)

* The Information Technology Division will issue revisions and updates to this policy and related standards.

### Third parties

* Third parties are required to comply with agency implementation of this policy at a minimum or a more stringent agency-specific policy including:
	+ Review and compliance with all information security programs, plans, guidelines, standards and policies that apply to the work they will be performing for their contracting agency and that are provided to them by the agency.
	+ Communication of such provisions to and enforcement against their subcontractors; implementation and maintenance of any other reasonable and appropriate security procedures and practices necessary to protect high sensitivity information, including but not limited to personal information to which they are given access under the contract, from unauthorized access, destruction, use, modification, disclosure or loss.

## Related Documents

Primary references that were used in development of this policy include:

* ISO 27001
* ISO 27005
* [Acceptable Use Policy](http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/it-policies-standards-and-procedures/other-policies/acceptable-use-policy.html)[[3]](#footnote-4)
* [Enterprise Information Security Policy](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html)[[4]](#footnote-5)
* [Enterprise Information Security Standards: Data Classification](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/enterprise-information-security-standards.html)[[5]](#footnote-6)
* [Executive Order 504](http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/legal-guidance/privacy-and-security/exec-order-504/vendor-certification-requirements.html)[[6]](#footnote-7)
* [NIST Risk Management Guide for IT Systems](http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)[[7]](#footnote-8)

Additional information referenced includes:

* M.G.L., Ch 93H
* M.G.L., Ch 93I
* M.G.L., Ch 66A
* ISO 27002
* CobiT
* ITIL
* HIPAA Security Rule
* HIPAA Privacy Rule

## Contact

Standards@state.ma.us

## Appendix A: Terms

Key terms used in this policy have been provided below for your convenience. For a full list of terms please refer to the glossary of [Commonwealth Specific Terms](http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/glossary-of-commonwealth.html)[[8]](#footnote-9) on the Massachusetts Office of Information Technology’s website.

**Entity –** An agency, department, secretariat, authority, college or other unit of government of the Commonwealth of Massachusetts.

**IT Asset –** An IT asset can be a physical IT asset (hardware, network devices, etc.) or a logical IT asset (data, software, licensing, and applications).

**Risk Assessment –** Risk Assessment is the process of identifying, qualifying and prioritizing risks against operational and control objectives, and designing and implementing controls that provide reasonable assurance that objectives will be met and that risks will be managed to an acceptable level.

**Risk Values –** Risk values can be Qualitative (High, Medium, and Low) or Quantitative (dollar value or other metric).

**Third Party –** Private sector companies or individuals that conduct business with MAGNet members.

## Appendix B: Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Action | Effective Date | Next Review Date |
| 05/26/2010 | ITD-SEC-8.1 Enterprise IT Asset and Risk Management Policy | 05/26/2010 | 05/26/2011 |
| 01/23/12 | Reviewed | 1/31/12 | 1/23/13 |
| 01/17/14 | Updated | 3/6/14 | 1/17/15 |
| 1/21/15 | Reviewed | 1/21/15 | 1/22/16 |
| 12/21/2015 | Accessibility remediation – no content changes | 2/22/16 | 1/1/17 |

1. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html [↑](#footnote-ref-2)
2. The Executive Department is comprised of the Executive Branch minus the Constitutional Offices, i.e., the State Auditor, State Treasurer, the Attorney General, and the Secretary of the Commonwealth. [↑](#footnote-ref-3)
3. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/it-policies-standards-and-procedures/other-policies/acceptable-use-policy.html [↑](#footnote-ref-4)
4. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html [↑](#footnote-ref-5)
5. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/enterprise-information-security-standards.html [↑](#footnote-ref-6)
6. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/legal-guidance/privacy-and-security/exec-order-504/ [↑](#footnote-ref-7)
7. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf [↑](#footnote-ref-8)
8. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/glossary-of-commonwealth.html [↑](#footnote-ref-9)