Commonwealth of Massachusetts

Massachusetts Office of Information Technology

# Enterprise Information Security Policy

**Reference #:** **ITD-SEC-1.3 Revision Date: March 7, 2014
Issue #: 3**

## Table of Contents

[Table of Contents 1](#_Toc438204558)

[Executive Summary 1](#_Toc438204559)

[Whom this Policy Applies To 2](#_Toc438204560)

[Policy Statement 2](#_Toc438204561)

[Roles and Responsibilities 7](#_Toc438204562)

[Related Documents 9](#_Toc438204563)

[Contact 10](#_Toc438204564)

[Appendix A: Terms 11](#_Toc438204565)

[Appendix B: Document History 12](#_Toc438204566)

## Executive Summary

A strong security position is maintained through the application of security controls, data ownership responsibilities, and maintenance of the security infrastructure. This policy articulates requirements that assist management in defining a framework that establishes a secure environment. This framework provides the overarching structure for safeguarding Information Technology (IT) Resources, achieving confidentiality, integrity and availability of the data and IT Resources used to manage the services provided by Commonwealth agencies, authorities, and business partners.

It is the responsibility of Agency Heads to have controls in place and in effect that provide reasonable assurance that security objectives are addressed. The Agency Head has the responsibility to exercise due diligence in the adoption of this framework. Agencies must achieve compliance with the overall information security goals of the Commonwealth including compliance with laws, regulations, policies and standards to which their technology resources and data, including but not limited to personal information, are subject.

## Whom this Policy Applies To

These standards apply to:

* Executive Department Agencies, [[1]](#footnote-2) 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 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 Agencies are required to ensure compliance by third parties in any aspect of the process of providing goods and services to their agency. These include, but are not limited to, 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 the Enterprise Information Security Policy at a minimum or a more stringent agency specific policy in compliance with agency and business related directives, laws, and regulations.

## Policy Statement

Agencies are required to implement policies, associated procedures and controls that protect the agency’s information assets, including but not limited to personal information and IT Resources from all threats, whether internal or external, deliberate or accidental. In addition to the three guiding principles of information security (confidentiality, integrity and availability), agencies must review the overall implementation of security controls against all applicable laws, regulations, policies, standards and associated risks.

### Information Security Management Program:

Agencies are required to implement an Information Security Program (ISP). An ISP is a management system that represents the policies and controls implemented within an organization. An effective management system provides both management and users with a detailed understanding of the goals, approach and implemented controls for securing the organization’s information assets, including but not limited to sensitive information (for example, personal information), and must address the ISP lifecycle; including risk assessment, risk treatment, selection and implementation of security controls, ongoing evaluation and maintenance.

### Risk Assessment

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 managed to an acceptable level.

Risk assessments must include at a minimum:

* 1. **Identification of risk factors:**

Evaluation of risk by considering the potential threats to the information and the IT Resources, including:

* + 1. Loss of the information or systems due to accident or malicious intent.
		2. Loss of availability such as the system being unavailable for a period of time.
		3. Unknown changes to the information or system so the information is no longer reliable.
	1. **Identification of threat:**

Evaluation of impact and likelihood of potential threat, including:

* + 1. Cost if each threat were to actually occur. Costs should be interpreted broadly to include money, resources, time, and loss of reputation among others.
		2. Evaluation of the probability of each threat occurring.

### Risk Treatment:

Agencies are required to monitor and evaluate the specific controls that must be implemented to meet the stated security objectives. This process must identify which security controls will be or are implemented and identify and justify which security controls are not deemed necessary or applicable.

### Statement of Applicability:

The Statement of Applicability is a document that lists the entities’ information security control objectives, controls and adopted policies that are relevant and applicable to the organization's information security management program. Agencies are required to maintain a statement of applicability for all IT Resources and information assets, including but not limited to personal information. Specific agency information security objectives and controls, including document sources and details, are defined within the Statement of Applicability document.

### Security Policy, Policy Adoption and Documentation Review:

Agencies are required to adopt and document a comprehensive information security policy. Agencies may adopt the Enterprise Information Security Policy or a more granular policy (or set of policies) based on an evaluation of their own business drivers.

Agencies are required to review the adopted Information Security Policy annually at a minimum. The purpose of the review is to ensure the continued suitability, adequacy and effectiveness of the policies. Agencies are encouraged to review their Information Security Policy on a more frequent basis particularly if significant changes occur within their organization that may have an impact on the effectiveness of the policy. Agencies should inform MassIT of any policy related changes that are needed but conflict with current enterprise security policies.

### Organization of Information Security:

Agencies are required to maintain the security of the organization’s information and information processing facilities that are accessed, processed, communicated to, or managed by employees and contractors (staff), and third parties by:

* Documenting the specific responsibilities of staff and third parties and
* Ensuring that all applicable contractual agreements incorporate and support the security-based requirements.

### Asset Management:

Agencies are required to achieve and maintain appropriate protection of information assets, including but not limited to personal information and IT Resources by assigning the responsibility to implement controls for achieving:

* Inventory of IT-related assets,
* Data classification,
* Appropriate tagging and data handling per classification and
* Acceptable use via implementation and enforcement of an Acceptable Use Policy.

All entities 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)](http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/legal-guidance/acceptable-use-policy.html)[[2]](#footnote-3) that entities may use or augment with additional procedures and guidelines for the use of IT Resources within their organizations.

### Human Resources Security:

Agencies are required to ensure that employees, contractors and third party users understand their security responsibilities and have the requisite skills and knowledge to ensure the effective execution of the roles they are assigned to reduce the risk of unauthorized access, use or modification of IT Resources (theft, fraud or misuse of facilities), including:

* Risk assessment to determine applicable level of employee screening prior to and upon change in responsibility during employment.
* Security awareness and training during employment.
* Disablement of access rights to data systems after an extended period of inactivity.
* Return of agency issued equipment and/or devices upon termination or change of employment.
* Removal of access rights upon termination of employment.

### Physical and Environmental Security:

Agencies are required to secure against unauthorized physical access, damage and interference to the agency’s premises and information assets including but not limited to personal information and IT Resources by implementing:

* Workforce security,
* Facility access controls of IT Resources,
* Equipment security,
* Least privilege,
* Visitor control and
* Secure disposal or reuse of equipment.

### Communications and Operations Management:

Agencies are required to implement procedures for managing system activities associated with access to information and information systems, modes of communication, and information processing by implementing:

* Controls for securing removable media,
* Data backup procedures,
* Data collection and secure disposal of data,
* Monitoring system use,
* Audit logging,
* Protection of log information, including administrator and operator logs,
* Fault logging,
* Antivirus,
* Network controls,
* Clock synchronization and
* Network management controls.

### Access Control:

Commonwealth Secretariats and their respective Agencies, authorities and business partners are required to protect applications, information assets, IT Resources and infrastructure against improper or unauthorized access which could result in compromise of confidentiality, integrity and availability of data and IT Resources. Access control rules must take into account the existing Enterprise policies for information dissemination and authorization which map directly to the following ISO 27001/27002 Access Control Domain security objectives:

1. Business Requirements for Access Control
2. User Access Management
3. User Responsibilities
4. Network Access Control
5. Operating System Access Control
6. Application and Information Access Control
7. Mobile Computing and Teleworking

### Information Systems Acquisition Development and Maintenance:

Agencies must ensure that information security is an integral component to IT Resources from the onset of the project or acquisition through implementing:

* Application and system security,
* Configuration management,
* Change control procedures,
* Encryption and key management and
* Software maintenance including but not limited to upgrades, antivirus, patching and malware detection response systems.

### Information Security Incident Management:

Agencies are required to implement management controls that result in a consistent and effective approach for addressing incidents that is aligned with Enterprise Policies and Standards including:

* Collection of evidence related to the incident as appropriate,
* Reporting procedures including any and all statutory reporting requirements,
* Incident remediation and
* Minimum logging procedures.

### Business Continuity Management:

Agencies are required to document, implement and annually test plans including the testing of all appropriate security provisions to minimize impact to systems or processes from the effects of major failures of IT Resources or disasters via adoption of:

* Continuity of operations plan and
* A disaster recovery plan.

### Compliance:

Agencies are required to implement the security requirements of this policy in addition to any state or federal law, regulatory, and/or contractual obligations to which their information assets and IT Resources are subject, including but not limited to:

* Security and privacy of personal information.
* Patent, Copyright and trade secret protection.
* Documented plans for all audit requirements and activities for information systems and assets, as appropriate.
* Results of self-audits required by MassIT upon request and at a minimum annually.
* Compliance with security policies and standards.

### Maintenance:

Agencies must implement a regular or event driven schedule by which the ISP is reviewed for ongoing effectiveness. The agency’s ISP, including security policies, procedures, and other controls, should be subject to an appropriate level of monitoring and evaluation. Changes to the components of the agency’s ISP should be subject to appropriate review and approval and be adequately documented.

## Roles and Responsibilities

The roles and responsibilities associated with implementation and compliance with this policy follow:

### Assistant Secretary for Information Technology

* Issue detailed guidelines governing agency development, implementation, and maintenance of Electronic Security Plans (ESP).
* Require agencies to submit their ESP to the Massachusetts Office of Information Technology (MassIT) for review.
* Specify when agencies shall be required to update their ESPs, and submit updated ESPs to MassIT for approval.
* Issue policies requiring that incidents involving a breach of security or unauthorized acquisition of personal information be immediately reported to MassIT and to other required entities per M.G.L., Ch 93H.
* Develop mandatory standards and procedures for agencies to follow before such agencies enter into contracts with third parties that access personal information in electronic form.

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

* SCIOs and Agency heads are responsible for exercising due diligence in adoption of this framework to meet the obligations of the Commonwealth by ensuring that adequate security controls are in place and in effect to promote reasonable assurance of security control objectives that safeguard the information assets, including but not limited to personal information.
* Ensure that all IT systems and applications developed conform to this and all related Enterprise Information Technology Policies, Standards and Procedures promulgated by the Assistant Secretary for Information Technology. Non-conforming IT systems cannot be deployed unless the purchasing entity and their contractor have jointly applied for and received in writing from the Assistant Secretary for Information Technology or designee notice that a specified variance will be permitted.
* Provide communication, training and enforcement that support the security goals of the Secretariat, its agencies and the Commonwealth.
* Provide proper third party oversight as applicable for any IT systems and applications.
* Review and sign all agency security programs, plans, self-audits and reports submitted by the Agency.
* The Agency Heads are responsible for ensuring compliance with all applicable laws, regulations, and contractual obligations.
* The Agency Heads are responsible for signing off on the agency’s acceptable risk level for meeting IT security objectives.

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

* Ensure that the goals and requirements of the Enterprise Information Security Policy are implemented and met.
* Maintain all required documentation as specified in the Enterprise Information Technology Policies, Standards and Procedures promulgated by the Assistant Secretary for Information Technology.
* Conduct self-audits required by MassIT upon request and at a minimum annually documenting reasonable assurance that compliance with Enterprise Information Technology Policies, Standards and Procedures has been achieved.
* Coordinate their agency’s compliance with the requirements of applicable executive orders, federal and state laws and regulations, MassIT security standards and policies and security-related contractual requirements.
* Sign all required agency security programs, plans, self-audits, and reports to attest to the accuracy of completeness of the submissions.

### Enterprise Security Board (ESB)

* Recommend revisions and updates to this policy and related standards.
* Manage the variance process and provide recommendations to the Assistant Secretary for Information Technology for approval.
* Advise the Assistant Secretary for Information Technology in developing security policies, standards and guidelines.
* Act as a consultative body to the Assistant Secretary for Information Technology.

### Massachusetts Office of Information Technology (MassIT)

* Establish, adopt and implement the Enterprise-wide policies and standards as determined by the Assistant Secretary for Information Technology in support of the Commonwealth’s information security goals including:
	+ Continuous testing and monitoring of the enterprise environment.
	+ Requesting statements of compliance from Agency ISOs including additional information as required by the Assistant Secretary for Information Technology.
	+ Providing ongoing education and outreach.
* Consult with state entities on the planning and deployment of IT Resources.
* After review of any related recommendations of the Enterprise Security Board, issue revisions and updates to this policy and related standards.
* Approve or deny variance recommendations of the ESB.

### Third parties

* Ensure that all IT systems and applications developed by or for Executive Department agencies or operating within the Commonwealth’s Wide Area Network (MAGNet) conform to this and other applicable Enterprise Information Technology Policies, Standards and Procedures promulgated by the Assistant Secretary for Information Technology. Non-conforming IT systems cannot be deployed unless the purchasing entity and their contractor have jointly applied for and received in writing from the Assistant Secretary for Information Technology or designee, notice that a specified deviation will be permitted.

## Related Documents

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

* ISO 27001
* Executive Order 504

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

## 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)[[3]](#footnote-4) on the Massachusetts Office of Information Technology’s website.

***No terms specific to this policy have been included.***

## Appendix B: Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Action | Effective Date | Next Review Date |
| 04/01/2009 | ITD-SEC-1.2 Enterprise Information Security Policy Revised (replaces ITD-01-1) | 04/01/2009 | 04/01/2010 |
| 11/27/2001 | ITD-01-1 Original Enterprise Information Security Policy Published | 11/27/2001 | 05/27/2002 |
| 1/23/12 | Reviewed | 1/31/12 | 1/23/13 |
| 1/21/2014 | Updated | 3/6/14 | 1/1/15 |
| 1/15/15 | Reviewed | 1/16/15 | 2/1/15 |
| 12/18/2015 | Accessibility remediation – no content changes | 2/22/16 | 1/1/17 |

1. 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-2)
2. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/legal-guidance/acceptable-use-policy.html [↑](#footnote-ref-3)
3. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/glossary-of-commonwealth.html [↑](#footnote-ref-4)