Commonwealth of Massachusetts

Massachusetts Office of Information Technology

# Enterprise Information Security Organization Policy

**Reference #: ITD-SEC-14.1 Issue Date: 3/6/2014  
Issue #: 1.0**

## Table of Contents

[Table of Contents 1](#_Toc438210064)

[Executive Summary 1](#_Toc438210065)

[Whom this Policy Applies To 2](#_Toc438210066)

[Policy Statement 2](#_Toc438210067)

[Roles and Responsibilities 6](#_Toc438210068)

[Related Documents 7](#_Toc438210069)

[Contact 7](#_Toc438210070)

[Appendix A: Terms 8](#_Toc438210071)

[Appendix B: Document History 9](#_Toc438210072)

## Executive Summary

This policy articulates the requirements that assist management in defining an organizational framework to initiate and control the implementation of information security practices including development and implementation of security policies, standards, and procedures within their respective agencies.

The overall objective is to safeguard the organization’s information and information processing facilities and to mitigate security risks when interfacing with third parties. This security policy is in compliance with and support of all Commonwealth enterprise security policies and standards.

Adoption of this framework asserts Commonwealth management’s commitment to information security, through collaboration with Secretariat Chief Information Officers (SCIO) to ensure appointments of information security officers (ISOs) to coordinate information security guidelines at the agency level. Further, it is the ISO’s responsibility to ensure that independent security reviews and self-audits are conducted on a periodic basis as required by Executive Order 504.

It is the responsibility of Agency Heads to have controls in place which provide reasonable assurance that security objectives are addressed. The security objectives are primarily defined within the agency’s existing Internal Control Plan and EO 504 Information Security Plan. Other security objectives should be delineated within the context of the sensitivity of the data owned and managed by the agency.

The Agency Head (and/or their designee(s)) has/have the responsibility to exercise due diligence in the adoption and communication of this framework. Agencies must achieve compliance with the overall information security goals of the Commonwealth including compliance with laws, regulations, policies, standards and contractual obligations pertaining to information security to which their technology resources and data, (including but not limited to personal information) are subject.

## Whom this Policy Applies To

All 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 requirements of this supporting policy.

* Executive Department 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 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, at a minimum, security requirements in accordance with this Enterprise Information Security Organization Policy or a more stringent agency policy that addresses agency specific and business related directives, laws, and regulations.

## Policy Statement

Agency management at all levels are required to actively support security within their organization by providing clear directives, demonstrated commitment, and explicit acknowledgement of information security responsibilities, specifically such responsibilities delineated within MassIT’s Enterprise Security Policies and Executive Order 504.

Internal and External Parties represent risks to security that must be properly identified, measured, remediated, or managed. Security risks associated with Third Parties can be addressed by implementing effective security controls and compensating controls, and enforcing Third Party agreements (including without limitation the contractual language that is currently standard within all Commonwealth contracts (e.g. Executive Order 504) or specific to a particular contract.

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, contractors (staff), and third parties by:

### Documenting the specific responsibilities of Internal Parties:

Agencies are required to allocate information security responsibilities and related security activities to agency representatives based on: relevant roles and job functions, including documenting specific responsibilities of staff by:

* 1. Identifying all staff serving as members of the information security team, putting emphasis on the Information Security Officer (ISO) and or the Chief Information Security Officer (CISO) when/if appropriate
  2. Identifying the roles and responsibilities of information security team members, utilizing Form 30s and/or EPRS/ACES as a toolset

At a minimum, agencies are required to assign the following roles and define associated responsibilities for each to one or more individual(s). In some cases; agencies may opt to outsource the following responsibilities. However, regardless of where the responsibility is assigned; the Agency must assign responsibility for:

* Information Security Officer and/or Chief Information Security Officer [[3]](#footnote-4)
* Security Assessment
* Intrusion Detection
* Incident Management & Resolution
* Policy Development and Implementation
* Policy Enforcement
* Monitoring
* Physical Access Management
* System Access Management
* Audit and Reporting
  1. Identifying the personnel reporting hierarchy within the information security team, via organizational charts

### Documenting the specific responsibilities of External Parties:

The documentation should include the identification of third party risks to the agency’s information from business processes involving external parties with appropriate controls implemented prior to granting access, by:

* 1. Performing a risk assessment of the identified security risks associated with conducting business with the third party prior to granting access and determine whether:
     1. The security risks can be remediated either by third parties or agency action.
     2. Compensating controls may be applied to satisfactorily diminish the security risks.
     3. The security risks can be effectively managed without undue risk to the agency.
  2. Appropriate screening process must be conducted for employees of contracting companies doing business with the Commonwealth as well as for subcontractors doing business with the Commonwealth.

### Management’s commitment to Information Security:

Management demonstrates support and commitment to information security by appointing an Information Security Officer (required per Executive Order 504, but subject to footnote 2 below). The Agency’s Information Security Officer must be able to meet the responsibilities associated with the Agency’s development and enforcement of an Information Security Program as required by the Enterprise Information Security Policy. It should be noted that while EO504 requires agencies to adopt ISPs to protect personal information; the Enterprise Information Security Policy is broader in nature and requires agency management to address:

* 1. Assessment and identification of security risks to the agency (reference the most recent security risk assessment).
  2. Compliance with security related laws and regulations; contractual provisions imposing security obligations on the agency; and Commonwealth enterprise security policies and standards.
  3. Review and verification that controls are in place to address and mitigate security risks.
  4. Management and execution of the Executive Order 504 mandate, including the agency’s obligation with respect to its EO504 Information Security Plan and Self-Assessment Questionnaire.
  5. Review of audit and assessment findings (where such audits are required by state or federal law or contractual requirements) and remediation of such findings.
  6. Review and updating of risk treatment plans (remediation plans and procedures drafted or in place) to address residual security risks to an acceptable level by management.
  7. Determination of ways to effect the improvement of the Information Security Program.
  8. Periodic review of the effectiveness of the information security program, including external review as appropriate, and updating of related policies and procedures as needed. Require agencies to provide written assurance of the adequacy and efficiency of their information security program.
  9. Coordination of information security efforts across the organization, including designation of ISOs and security working committee(s).
  10. Communicate clear direction and support for information security initiatives including providing appropriate resources for information security controls across the agency.
  11. Authorize the continued operation of the Information Security Program via certification of the program annually.

### Contractual agreements including confidentiality and Third Party:

Ensuring that all applicable contractual agreements incorporate and support the security-based requirements.

* 1. Requirements for confidentiality or non-disclosure agreements should reflect the organization’s needs for the protection of information and be reviewed periodically as needed. All agency contract staff members) must sign a confidentiality agreement as their role dictates. As changes are made to the language and/or scope of such agreements, contract staff members are required to be covered under updated agreements. Agreements must be kept within a secure location to prevent unauthorized alteration, destruction, or theft.
  2. Confidentiality Agreements must be developed and executed with third parties who will be involved in accessing, processing, communicating or managing the organization’s information or information processing facilities or adding products or services to them as appropriate based on the sensitivity classification of the information in question. Such agreements must be executed prior to the date on which such third party is granted access to agency information or information processing facilities or the agency commences conducting business with them.

## Roles and Responsibilities

All 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)[[4]](#footnote-5) are subject to the referenced roles and responsibilities in addition to those specifically stated within this supporting policy. The roles and responsibilities associated with implementation and compliance with this policy follow:

### Assistant Secretary for Information Technology

* Require all agency heads, managers, supervisors, and employees (including contract employees) to attend mandatory information security training and incorporate such training as part of the standardized orientation provided to new employees at the time they commence work.
* Develop mandatory standards and procedures for agencies to follow before entering into contracts that will provide third parties with access to electronic medium sensitivity and 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 Information Security Organization Policy and its revisions.

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

* SCIOs and Agency heads are responsible for exercising due diligence in adhering to the requirements contained in this policy.
* Provide communication, training and enforcement of this policy that support the security goals of the Secretariat, its agencies and the Commonwealth.
* Provide proper third party oversight as applicable for access to and communication with agency IT Resources including applications and information assets.

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

* Ensure that the goals and requirements of the Enterprise Information Security Organization Policy are implemented and met.

### Enterprise Security Board (ESB)

* Recommend revisions and updates to this policy and related standards.

### Massachusetts Office of Information Technology (MassIT)

* After review of any related recommendations of the Enterprise Security Board, issue revisions and updates to this policy and related standards.

### Third parties

* Comply with agency implementation of this policy at a minimum or a more stringent agency specific policy including:
  + Attestation and certification that third parties have read Executive Order 504.
  + 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.
  + Communicating such provisions to and enforce them against their subcontractors, and requiring them to implement and maintain any other reasonable and appropriate security procedures and practices necessary to protect medium sensitivity and high sensitivity information including but not limited to personal information to which they are given access as part of 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
* Executive Order 504
* Chief Information Security Officer Advisory, April 26, 2013

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](mailto: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)[[5]](#footnote-6) on the Massachusetts Office of Information Technology’s website.

**Staff —** Staff include contract employees, independent contractors, volunteers, interns, temporary employees, and trainees.

## Appendix B: Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Action | Effective Date | Next Review Date |
| 3/7/2014 | Published Enterprise Information Security Organization Policy | 3/6/2014 | 1/1/2015 |
| 1/30/15 | Reviewed | 1/30/15 | 2/1/16 |
| 12/18/2015 | Accessibility remediation, corrected section 1 numbering – 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. Due to information technology consolidation, the ISO role may be played by an individual not employed by the agency. Specifically, secretariats, groups of agencies, and agencies may choose any one of a number of ways to appoint an information security officer, as long as their method is consistent with one of the following; Appoint a secretariat ISO reporting to the secretary and responsible for playing the ISO role for both the executive office and all agencies thereunder;

   Appoint a multi-agency ISO reporting to the secretary and responsible for playing the ISO role for multiple agencies under the secretariat or

   Appoint an ISO who reports to the agency head who is responsible for playing the ISO role only for that agency. [↑](#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/policies-legal-and-technical-guidance/glossary-of-commonwealth.html [↑](#footnote-ref-6)