Commonwealth of Massachusetts

Massachusetts Office of Information Technology

# Enterprise Data Classification Security Standards

**Reference #:** **Ent-Std-Sec-DataClass-2.2 Revision Date: March 6, 2014
Issue #: 2**

## Table of Contents

[Table of Contents 1](#_Toc438215463)

[Executive Summary 1](#_Toc438215464)

[Whom this Policy Applies To 3](#_Toc438215465)

[Policy Statement 3](#_Toc438215466)

[Additional Information 10](#_Toc438215467)

[Roles and Responsibilities 11](#_Toc438215468)

[Related Documents 13](#_Toc438215469)

[Contact 13](#_Toc438215470)

[Appendix A: Terms 14](#_Toc438215471)

[Appendix B: Document History 15](#_Toc438215472)

## Executive Summary

The purpose of this document is to identify the minimum standards that agencies must adopt for the appropriate classification of data and the ongoing management of that classification. Classification of data is a critical part of data management which includes planning and implementing comprehensive and responsible information security practices. This document describes a standard data classification scheme, the required considerations for classification, risk assessment, security control requirements and data management and lifecycle requirements.

Data classification is one of the required components of the [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) which addresses the security of information collected, used or maintained within electronic systems. The need to maintain and share all types of data, both internal and external, to the agency remains a key business requirement. Therefore, the need to properly protect that data is critical to the Commonwealth’s core mission. These standards ensure that agencies develop and maintain data classification levels and controls that are compliant with the Enterprise Information Security Policy.

In some circumstances, strict adherence to the rules for data dissemination as described under these standards will be inconsistent with the requirements of the Public Records Law, Mass. Gen. L. c. 66, section 10. Where an agency’s compliance with these standards and agency policies and classifications adopted hereunder conflict with the requirements of the Public Records Law, the Public Records Law takes precedence and agencies must meet its requirements.

Proper management of data requires agencies to perform periodic reviews of data and assess their classifications and controls. The controls for classified data must be commensurate with the level of identified risk, regulatory requirements and interagency agreements that may pertain to agency acquisition, use or maintenance of data.

For purposes of these standards, data is information maintained in an electronic, digital or optical format. Data includes numbers, text, images and sounds, which are created, generated, sent, communicated, received by and/or stored on Commonwealth owned or contracted Information Technology Resources (ITR’s). Data does not include hardware, platforms, software, applications or middleware.

The roles defined below are representative of the types of functions involved in the process of data classification and lifecycle management:

* **Data Owner:** The Data Owner has policy-level responsibility for establishing rules and use of data based on applied classification. The head of the agency is ultimately the Data Owner and is responsible for assigning the classification, ensuring the protection and establishing appropriate use of agency’s data. Individuals within the agency may be delegated some portion of this responsibility on behalf of the agency head. The Data Owner is also responsible for assigning individuals to the following roles.
* **Data Manager:** The Data Manager develops general procedures and guidelines for the management, security and access to data, as appropriate.
* **Data Steward:** The Data Steward has custodial responsibilities for managing the data for the day-to-day, operational-level functions on behalf of the Data Owner as established by the Data Manager.
* **Data User:** A Data User is any individual who is eligible and authorized to access and use the data.

The data classification standards are organized in four sections:

* Section 1: Classification Scheme
* Section 2: Required Considerations for Classification
* Section 3: Risk Assessment and Security Controls
* Section 4: Data Management Lifecycle

## Whom this Policy Applies To

Agencies governed by the [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)[[2]](#footnote-3) must adhere to the standards detailed in this document, except where such adherence would conflict with the Public Records Law or other laws, regulations or policies. Additional references that agencies may find useful as they classify their data are listed at the end of this document.

* Executive Department Agencies, [[3]](#footnote-4) 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 [name of this policy] at a minimum or a more stringent agency specific policy in compliance with agency and business related directives, laws, and regulations.

## Policy Statement

### Classification Scheme

Agencies must classify their data into at least one of the following three levels of classification: **Low Sensitivity** (General Use); **Medium Sensitivity** (Internal Use); and **High Sensitivity** (Confidential Use). For each of the three classification levels, the following information is provided:

* **Classification Title:** Classification Level/Type
* **Definition:** Description of Classification
* **Examples:** Types of data that may fall under defined classification. Agencies may choose to classify data that is cited in an example below at a different sensitivity level.
	1. **Low Sensitivity (General Use)**

Definition: Data classified as having low sensitivity should be thought of as being for general use and is approved by the agency as available for routine public disclosure and use. Security at this level is the minimum required by the agency to protect the integrity and availability of this data.

Examples: This may include, but is not limited to, data routinely distributed to the public regardless of whether the agency has received a public records request, such as: annual reports, publicly accessible web pages, marketing materials and press statements.

* 1. **Medium Sensitivity (Internal Use)**

Definition: Data classified as having medium sensitivity should be treated as internal, the release of which must be approved prior to dissemination outside the agency. Its compromise may inconvenience the agency, but is unlikely to result in a breach of confidentiality, loss of value or serious damage to integrity. The agency will define the level of protection required for this classification.

Examples: Data in this category is not routinely distributed outside the agency. It may include, but is not limited to non-confidential data contained within: internal communications, minutes of meetings and internal project reports.

* 1. **High Sensitivity (Confidential Use)**

Definition: Data classified as having high sensitivity is considered confidential. Such data should not be copied or removed from the agency’s operational control without authorized permission. High sensitivity data is subject to the most restricted distribution and must be protected at all times. Compromise of high sensitivity data could seriously damage the mission, safety or integrity of an agency, its staff or its constituents. It is mandatory to protect data at this level to the highest possible degree as is prudent or as required by law.

Examples: High Sensitivity data may include, but is not limited to, personally identifiable, legally mandated, or sensitive data associated with: investigations, bids prior to award, personnel files, trade secrets, appraisals of real property, test questions and answers, constituent records, health records, academic records, contracts during negotiation and risk or vulnerability assessments.

### Required Considerations for Classification

The considerations listed below must be evaluated by agencies when assigning classifications to their data.

* 1. **Evaluating Data**

**Laws, Regulations, Policies and Standards**

Agencies are required to ensure that all laws, regulations, policies and standards to which their data is subject are met. Examples of laws and regulations that give or restrict access to data and apply to certain Commonwealth agencies and departments include the [Fair Information Practices Act](http://www.mass.gov/legis/laws/mgl/gl-66a-toc.htm), the Tax Information Security Guidelines for Federal, State and Local Agencies and Entities [IRS Pub 1075](http://www.irs.gov/pub/irs-pdf/p1075.pdf), the [Health Insurance Portability Accountability Act](http://www.hhs.gov/ocr/hipaa/) (HIPAA), [Public Records Law](http://www.sec.state.ma.us/pre/preidx.htm) , [Massachusetts Identity Theft Law,](http://www.mass.gov/legis/laws/seslaw07/sl070082.htm) [Family Educational Rights and Privacy Act (FERPA),](http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html) the Federal Rules of Civil Procedures’ references to electronic discovery, the guidance issued by the Supreme Judicial Court regarding electronic discovery in state court, and agencies’ enabling legislation, regulations and policies and other laws that give or restrict access to data. Finally, agencies must take into consideration existing enterprise policies and standards while implementing and evaluating their data classification assignments. Questions regarding laws, regulations, policies and standards that apply to specific agencies and departments should be directed to agency or department counsel.

* 1. **Potential harm to the individuals to whom the data pertains**

It is imperative to take into consideration any potential harm or adverse impact that the compromise of data may have on the parties to whom the data pertains. This consideration pertains to, but is not limited to client data, personally identifiable information and medical information.

* 1. **Risk of loss of confidentiality**

Confidentiality has been defined by the [International Organization for Standardization](http://www.iso.org/) (ISO) as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security. Therefore, in appropriately assigning data with a classification level, agencies must evaluate what the risk is for unauthorized access to classified data and what likely impact that loss would have.

* 1. **Agency Mission and Business Objectives**

Agencies with unique missions and business objectives should take those needs into consideration when evaluating their data classifications. In some cases, agencies may be obligated to share as much of their data as possible with the public or other outside agencies while others may be under the strictest constraints in ensuring that their data is protected against any exposure whatsoever. In either case, while it is incumbent on the agency to ensure that those objectives are met, adequate controls need to be in place and in effect to address data integrity, security and availability.

* 1. **Combining or Aggregating Data**

At the point at which data is combined or aggregated its classification level should be reviewed. Some data may have little or no sensitivity in isolation, but may be highly sensitive when combined with other data. In some cases, aggregation of large quantities of a single data type can reveal sensitive patterns and/or plans and may facilitate access to sensitive or critical systems. In other cases, aggregation of information of several different and seemingly innocuous types can have similar effects. In general, the sensitivity of a given data element is likely to be greater in combination than in isolation (e.g., association of an account number with the identity of an individual and or institution).

* 1. **Data Sharing Agreements and Contractual Requirements**

Interagency Service Agreements (ISAs), Memoranda of Understanding (MOU’s), grants, contracts and other written agreements between agencies and external entities may include agreements regarding data sharing and the use, disclosure and maintenance of data, as determined by the data classification of the Data Owner. The recipient agency or department’s data classification must align with any such requirements.

Further, if an agreement states that the recipient agency or department may further share the data, the subsequent recipients must adhere to the requirements of the original classification, unless the data has been de-identified or otherwise modified such that a different classification is required.

* 1. **Industry Standards**

There are several industry standards that may be helpful to agencies in determining how to classify their data and in some instances agencies may be obligated to comply with certain industry standards. For example, agencies handling credit card transactions are subject to the [Payment Card Industry Data Security Standards (PCI DSS](https://www.pcisecuritystandards.org/tech/index.htm)). Other examples of industry standard references can be found at the end of this document.

* 1. **Up-stream and down-stream considerations**

It is important for agencies to consider how data will be used and what impact the intended use should have on the classification assigned to the data.

* 1. **Intellectual Property**

Agencies must take into consideration any intellectual property rights owned by an entity other than the agency while implementing and evaluating their data classification assignments.

* 1. **Evaluating Metadata**

Metadata can generally be defined as information that describes, or supplements, the central data, or as simply data about data. For example an email “wrapper” is not visible to the reader of the email message but can be retrieved and includes details about how the email traveled between sender and recipient. In some cases, the metadata adds information and is not critical to the functions of the main data. In other cases, metadata can be considered essential to the proper functioning of the main product. Since the difference between data and metadata is often subtle and context-specific, it is important to know what type of metadata is associated with an agency’s data. The classification of the data itself is considered metadata.

* + 1. Metadata may be maintained at the system level, table level, document level or more granularly based on the agency’s needs and capabilities.
		2. Metadata must be classified. The potential sensitivity of the metadata itself must be considered when determining whether or not to classify at the same level as the associated data.

### Risk Assessment and Security Controls

* 1. **Risk Assessment**

Once data is assigned the appropriate classification level, agencies must conduct a Risk Assessment to determine acceptable levels of risk and the appropriate level of security controls for information systems. Information Security Risk Assessments are part of sound security practices and are required by the Enterprise Information Security Policy. MassIT has published Information Security Risk Assessment Guidelines that agencies may use to inform their risk assessment processes.

**Risk Assessments must at a minimum include:**

* + 1. Appropriate documentation including what is being identified, system purpose and description and system security level based on data classification levels.
		2. System risk determination including identification of threats and vulnerabilities, description of risks, identification of existing controls, determination of likelihood of occurrence, determination of severity of impact and determination of risk levels.
		3. Safeguard determination including recommended controls and safeguards, determination of residual likelihood of occurrence, determination of residual severity of impact and determination of residual risk level.
		4. Data Owner acceptance and sign-off.
	1. **Security Controls**

The Risk Assessment will recommend safeguards or security controls and describe the expected level of risk that would remain if these controls were put in place. Following are minimum security controls that must be considered based on the three data classification levels. Agencies may assign more stringent requirements based on the results of their risk assessment. Agencies that receive data from other agencies must adhere to any security controls agreed to by the originating agency and the receiving agency.

* + 1. **Security Controls for High Sensitivity Data:** Confidential data must be protected using at least one physical control and at least one IT control. For examples of some acceptable options, please reference the list below. Also, any data that is classified as having high sensitivity that will be transported between agencies or externally to an environment outside of the Commonwealth’s wide area network (MAGNet) must be encrypted and a log maintained with details of the transfer, including the date, the data description, the receiving agency, entity or individual and if the recipient is an agency or entity, the person who received it. [[4]](#footnote-5) This is in addition to the physical and IT controls requirement above. When data is being transported it has less physical security than it does inside of an agency. Therefore additional physical security controls should follow accepted industry standards and industry best practices.
		2. **Security Controls for Medium Sensitivity Data:** Internal use data must be protected using at least one of the security controls from the list of examples below.
		3. **Security Controls for Low Sensitivity Data:** General use data may be protected using any of the security controls from the list of examples below. However, agencies may decide that data classified for general use does not need any security controls above and beyond the general security controls implemented at the agency level and that citizens may access agency data over the Internet without being subject to access controls such as IDs or passwords.

#### Examples of Security Controls – Partial List

* Physical Controls:
	+ Photo ID
	+ Lock & Key
	+ Location specific access
	+ Shredding
	+ Security Guards
	+ Intrusion Detection and Alarm Devices
* IT Controls:
	+ Security Software
	+ ID and Passwords
	+ Biometrics
	+ Encryption (of email, CDs, DVDs, jump drives, laptops)
	+ Digital Signatures
	+ Keys or Tokens
	+ Secure ID Card
	+ Role based authentication
	+ Logical Intrusion and Alert Solutions

### Data Management Lifecycle

Once a classification level has been assigned to data, it is important to understand how time, management and sharing of this data effects the overall security and management of this data from its inception to the end of its life. Data Owners are not released from their responsibility for this data upon an authorized disclosure to another agency or 3rd party. An MOU or ISA associated with any data disclosure must set the requirements for how this data can be used by the agency or 3rd party to whom it has been disclosed. [[5]](#footnote-6) An MOU or ISA must contain language that defines the security level, monitoring, use and destruction of the data. Compliance with these requirements is the responsibility of the receiving agency. An annual self-audit should be mandated by the receiving agency to ensure that compliance with the requirements is in place and is monitored by the receiving agency.

**Agencies must include the following in their ongoing monitoring, evaluation and data management:**

* 1. Assigned data classification levels should be reviewed and evaluated on a periodic basis to insure that the classification remains valid. Best practices indicate that classifications should be reviewed annually. However, it is ultimately the responsibility of the Data Owner to identify the appropriate review cycles.
	2. Documentation of ongoing efforts must be maintained indicating the scope, date and results to show compliance with this standard.
	3. Agencies are obligated to observe classification and security controls assigned to data obtained under written agreement from other agencies or external sources throughout the data’s lifecycle. [[6]](#footnote-7)
	4. Except as required under the Public Records Law, data must only be accessed on a need to know, need to perform or need to protect basis.
	5. Data must only be accessed by systems or persons with the appropriate security level. Access must be revisited whenever persons change roles within the agency.
	6. Access to High Sensitivity data must be audited and logged.
	7. Data must keep its classification level across different media.
	8. Data must keep its classification level across changes in business process (i.e. if it’s sensitive on paper, it’s still sensitive when the business process goes online).
	9. Agencies must consider chain of custody issues with classified data and the personnel responsible for the handling, accessing, maintaining or creating data.
	10. The appropriate individuals working for the agencies that own the data must be consulted prior to any release of data including:
* Individuals responsible for responding to public records requests (Custodians as defined by 950 C.M.R. 32.03).
* Individuals responsible for making determinations about the disclosure of certain personally identifiable data that is subject to the Fair Information Practices Act (Responsible Persons as defined by 950 C.M.R. 33.06).
* Individuals who respond to subpoenas and requests for production.

## Additional Information

The following references were used in development of these standards:

[ISO[[7]](#footnote-8):](http://www.iso.org/) International Standards Organization

[FIPS PUB 199](http://www.nist.gov/manuscript-publication-search.cfm?pub_id=150439)[[8]](#footnote-9): Standards for Security Categorization of Federal Information and Information Systems

[NIST 800-60 (PDF)](http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf)[[9]](#footnote-10): Guide for Mapping Types of Information & Information Systems to Security Categories

[IRS Pub 1075 (PDF)](http://www.irs.gov/pub/irs-pdf/p1075.pdf)[[10]](#footnote-11): Tax Information Security Guidelines for Federal, State and Local Agencies and Entities

[Fair Information Practices Act](http://www.mass.gov/legis/laws/mgl/gl-66a-toc.htm)[[11]](#footnote-12): Mass. Gen. L. ch. 66A

[Executive Order 504](http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/legal-guidance/privacy-and-security/exec-order-504/)[[12]](#footnote-13): Executive Order regarding protection and privacy of personal information

[Public Records Division](http://www.sec.state.ma.us/pre/preidx.htm)[[13]](#footnote-14): Public records resources as provided by the Secretary of the Commonwealth

[Massachusetts Identity Theft Law[[14]](#footnote-15):](http://www.mass.gov/legis/laws/seslaw07/sl070082.htm) Law relative to Security Freezes and Notification of Data Breaches

[Family Educational Rights and Privacy Act (FERPA)[[15]](#footnote-16):](http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html)  The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.

[Information Security Risk Assessment Guidelines](http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/risk-assessment/risk-assessment-guideline.html)[[16]](#footnote-17): Risk assessment methodology based on the Centers for Medicare and Medicaid Services (CMS) Information Security RA Methodology.

[Mass. Gen. L. 93H](https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h)[[17]](#footnote-18): Commonwealth of Massachusetts Law that protects residents’ personal information

[FIPA](http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleX/Chapter66A)[[18]](#footnote-19): The Fair Information Practices Act

[201 CMR 17.00 (PDF)](http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf)[[19]](#footnote-20): Standards for the protection of personal information of residents of the Commonwealth.

[HIPAA](http://www.hhs.gov/hipaa/)[[20]](#footnote-21): Health Insurance Portability and Accountability Act for protection and confidentiality handling of health information

## 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

[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)[[21]](#footnote-22)

## 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)[[22]](#footnote-23) on the Massachusetts Office of Information Technology’s website.

## Appendix B: Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Action | Effective Date | Next Review Date |
| 10/26/07 | Published | 10/26/07 |  |
| 01/23/12 | Reviewed | 1/31/12 | 1/23/13 |
| 01/17/14 | Updated | 3/6/14 | 1/1/15 |
| 1/10/15 | Reviewed | 1/10/15 | 1/11/16 |
| 12/18/2015 | 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. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html [↑](#footnote-ref-3)
3. 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-4)
4. Note that regardless of whether an agency classifies public record data as High, Medium or Low Sensitivity Data, it must, if it receives a public records request for such data, follow the Public Records Law and the Supervisor of Public Records’ requirements, including the requirement that “if a custodian is able to provide information in a compatible format or medium, then he or she is obligated to do so.” Supervisor of Public Records Bulletin No. 3-96. Production of encrypted data may not always meet this requirement. Moreover, an agency that receives a public records request for High Sensitivity Data may not always know who the ultimate recipient of the data is; many public records requests are made by agents on behalf of the true recipient and the requestor is not required to disclose such individuals. According to the Supervisor of Public Records, “[a] records custodian may not ask a requestor the reason for the request or the intended use of the requested records.” A Guide to the Public Records Law, December 2006. [↑](#footnote-ref-5)
5. However, if such data becomes the subject of a public records request, agencies cannot require that requestors enter such agreements. [↑](#footnote-ref-6)
6. However, agencies cannot enter agreements with other agencies or external sources that restrict data dissemination in a manner inconsistent with the Public Records Law. [↑](#footnote-ref-7)
7. http://www.iso.org/ [↑](#footnote-ref-8)
8. http://www.nist.gov/manuscript-publication-search.cfm?pub\_id=150439 [↑](#footnote-ref-9)
9. http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60\_Vol1-Rev1.pdf [↑](#footnote-ref-10)
10. http://www.irs.gov/pub/irs-pdf/p1075.pdf [↑](#footnote-ref-11)
11. http://www.mass.gov/legis/laws/mgl/gl-66a-toc.htm [↑](#footnote-ref-12)
12. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/legal-guidance/privacy-and-security/exec-order-504/ [↑](#footnote-ref-13)
13. http://www.sec.state.ma.us/pre/preidx.htm [↑](#footnote-ref-14)
14. http://www.mass.gov/legis/laws/seslaw07/sl070082.htm [↑](#footnote-ref-15)
15. http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html [↑](#footnote-ref-16)
16. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/risk-assessment/risk-assessment-guideline.html [↑](#footnote-ref-17)
17. https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93h [↑](#footnote-ref-18)
18. http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleX/Chapter66A [↑](#footnote-ref-19)
19. http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf [↑](#footnote-ref-20)
20. http://www.hhs.gov/hipaa/ [↑](#footnote-ref-21)
21. http://www.mass.gov/anf/research-and-tech/cyber-security/security-for-state-employees/security-policies-and-standards/information-security-policy.html [↑](#footnote-ref-22)
22. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/glossary-of-commonwealth.html [↑](#footnote-ref-23)