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

Glossary of Terms

Document Name: Glossary of Terms	Effective Date: October 15, 2018
Document ID: IS.Glossary	Last Revised Date: December 4, 2023

Table of contents

1. PURPOSE

The purpose of this ***standard*** is to provide a centralized, common reference for definitions of terms used in information security ***policies*** and ***standards***.

2. AUTHORITY

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

3. SCOPE

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

4. RESPONSIBILITY

3.1 The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this document.

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

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

3.4 Additional information regarding this document may be found at https://www.mass.gov/cybersecurity/policies.

5. DEFINITIONS

The definitions in this glossary are for general informational purposes only and should not be considered as legal definitions in all instances. Different statutes, laws, and legal documents may have distinct legal definitions and interpretations. For specific legal applications, users must consult their agency's legal counsel or a qualified attorney. The information provided here does not constitute legal advice.

Access Control – Specific implementation or configuration intending to (fully or partially) mitigate a risk related to unauthorized parties accessing the Commonwealth's assets.

Administrative Account (Privileged Account) – An information system account where a user is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Agency - Any agency, executive office, department, board, commission, bureau, division, council, or authority of the Commonwealth, or any of its branches, or of any political subdivision thereof.

Application – a computer program designed to carry out a specific task other than the one relating to the operation of the computer itself, typically to be used by end users. (word processors, accounting software, etc.) applications can be installed locally on a specific device or hosted in cloud or on-premises servers.

Application Administrator – An information technology (IT) professional who manages specific applications or software. Application administrators are in charge of installing, updating, and maintaining their assigned applications. They also troubleshoot concerns and respond to inquiries from application users.

Asset – Any entity that the Commonwealth considers to have value. Assets can be tangible (e.g., computers, mobiles, network equipment and media) or intangible (information-related – e.g., information, software, and services). The Commonwealth considers information as an asset.

Breach of Security - The unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the Commonwealth.

Business Impact Analysis (BIA) - A review that predicts the consequences of disruption of a business function and process and gathers information needed to develop recovery strategies.

Business Recovery Event – Unplanned outage where the Recovery Time Objective is in jeopardy.

Capacity Management Process – Means of ensuring that IT services and the IT infrastructure may be delivered at the targeted service levels in a timely manner, within the costs allowed. The Capacity Management Process considers all resources required to deliver the IT service, and plans for short-, medium- and long-term requirements of the organization.

Change Advisory Board – A designated team of specialists who review requests for internal changes and manage service transitions smoothly, so they do not disrupt work and do not interfere with the organization's business.

Change Management Process - The process of guiding organizational change to fruition, from the earliest stages of conception and preparation, through implementation and, finally, to resolution.

Chief Data Officer (CDO) – The individual appointed by the Secretary of EOTSS pursuant to Mass. Gen. Laws. ch. 7D §4A. The Secretary of EOTSS may appoint a qualified individual to serve as the chief data officer for the Commonwealth, who shall develop administrative directives to govern the use, storage, collection, and dissemination of data assets for the executive department, and shall develop procedures for facilitating resolution of disputes between or among agencies, departments, and executive officers regarding the use and sharing of data. The CDO shall have the role of promoting and facilitating, subject to all relevant laws, rules, and regulation, the sharing and use of data assets of the Commonwealth in support of data-driven policymaking, research, analysis, study, or economic development.

Chief Digital Officer – The individual appointed by the Secretary of EOTSS pursuant to Mass. Gen. Laws. ch. 7D §4C. The Secretary of EOTSS may appoint a qualified individual to serve as chief digital officer to lead an effort to improve the public facing web presence and related services for executive department offices and agencies.

Chief Information Officer (CIO) – The person responsible for the management, implementation, security and usability of information, technologies, processes, and users within the organization's IT environment.

Chief Information Security Officer (CISO) – The person responsible for aligning security initiatives with enterprise programs and business objectives, ensuring that communication systems, confidential information and technologies are adequately protected. The CISO for the Commonwealth of Massachusetts, (and the Commonwealth CISO) is the CISO of the Executive Office of Technology Services and Security.

Chief Privacy Officer (CPO) – The person responsible for promoting privacy and security in the use and dissemination of sensitive data. The CPO is also responsible for resolving any concerns regarding privacy and security in the use of data.

Cloud Computing – Cloud computing is an approach to computing infrastructure typically defined by on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Deployments are subscription-based and delivered over the internet via an "as-a-service" model and can be scaled to meet the changing demands of the business. Cloud deployments could be Software as a Service, Platform as a Service, or Infrastructure as a Service. Cloud Computing may be developed internally, outsourced externally, or implemented through a hybrid model of internal and external methods.

Commonwealth CIO – The Secretary of Executive Office of Technology Services and Security is the Chief Information Officer of the Commonwealth, as provided for under M.G.L Ch. 7d, section 2. The Commonwealth CIO has supervisory authority over all activities concerning information technology of state agencies.

Commonwealth CISO - The CISO of the Executive Office of Technology Services and Security as provided for under M.G.L Ch. 7d, section 4.

Commonwealth CPO – The CPO of the Executive Office of Technology Services and Security as provided for under M.G.L Ch. 7d, section 4B.

Confidential Information – Data or information that must be kept private and is protected against unauthorized or unlawful access or processing by federal, local, or state laws or data exchange agreements or other contractual agreements to protect its proprietary worth. Organization or customer information that if inappropriately accessed, disclosed, or other wised compromised, could seriously damage the mission, safety, or integrity of an agency, and cause adverse financial, legal, regulatory, or reputational damage to the Commonwealth, its constituents, customers, and business partners. Confidential Information is important to the ongoing operations of the Commonwealth. Data or information is "confidential" if it is protected against unauthorized or unlawful access or processing. This Information is primarily used in day-to-day operations. This type of information is for select groups, and/or may be restricted to users with a specific need to know. Confidential information is not available to the general public. Confidential information, if necessary, will be assessed for release under the

Massachusetts Public Records Law, and in response to subpoenas and requests for production in litigation, and, subject to any applicable law, will be reviewed under all relevant procedures as to its releasability.

Contractor/Consultant – Personnel directly hired by an agency or the Commonwealth other than as full-time employees, who may be granted access to the Commonwealth's resources and assets, to support a business agreement or contract with the Commonwealth.

Control – Specific implementation or configuration intending to (fully or partially) mitigate a risk. Controls are embedded into standards and procedures as a means of ensuring accountability and audibility of a process.

Control Owner - An individual who is responsible for the effectiveness of controls within the Commonwealth's information technology (IT) environment.

Crypto Period – A crypto period is the time span during which a specific key is authorized for use by the Commonwealth or the keys for a given system will remain in effect.

Cryptographic Key – A string of data stored in a file, which, when processed through a cryptographic algorithm, can encode or decode cryptographic data.

Data – Factual information, numeric and descriptive, that is retained and/or used as a basis for analysis, reference, reasoning, discussion, calculation, publishing, or decision making. Any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Data Manager - The Data Manager develops general procedures and guidelines for the management, security, and access to data, as appropriate.

Data Owner - The individual who possesses 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.

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.

Disposal – Removal or destruction of sensitive data/Assets via secure methodology.

Document Owner – The individual responsible for the generation, collection, processing, dissemination and review of security policies, procedures, standards, and other information.

Electronic - relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

Encrypt – To conceal information or data by converting it into a cipher or code, to prevent unauthorized access.

Encrypted - Transformation of data through the use of a 128–bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation. Other laws or regulations may require different level of encryption.

Encryption - The process of protecting information or data by using mathematical models to scramble it in such a way that only the parties who have the key to unscramble it can access the data.

Endpoint – Includes desktops, laptops, tablets, smartphones, and other mobile devices used to store, process, or transmit the Commonwealth's Information.

Enterprise Privacy Office – EPO is an office within the EOTSS, directed by the Commonwealth Chief Privacy Officer, responsible for the development and ongoing maintenance and compliance of the Enterprise data privacy policy and initiatives.

ePolicy Orchestrator (ePO) – An extensible and scalable centralized security management software that unifies security management through an open platform and simplifies risk and compliance management for organizations.

Equipment – Refers to any tangible device that is used in operation of the Commonwealth business. All equipment are assets; however, not all assets are equipment.

Event – Any observable occurrence deemed noteworthy or unusual, as it does not conform to the standard or expected operating behavior.

Exception – A request for relief submitted by an Executive Office or Agency when they are unable to comply with a policy, procedure or standard issued by EOTSS.

Federal Tax Information – FTI are returns and return information as defined in 26 U.S.C. § 6103(b) that are received directly from the Internal Revenue Service or obtained through an IRS-authorized secondary source, that are in the Recipient's possession or control, and that are subject to the confidentiality protections and safeguarding requirements of the Internal Revenue Code and corresponding federal regulations and guidance.

Fusion Center – The CFC is the Commonwealth's principal state repository for the receipt, analysis, gathering and sharing of threat-related information, including criminal activity, threats to public safety, and terrorist activity, among state, local, federal, and private sector partners.

Governance Risk and Compliance Team - Entity responsible for the management and execution of the risk assessment process as well as approvals and tracking of identified risk mitigations.

Guideline - Statements that provide optional control recommendations based on industry leading best practices.

High-Value Asset – An asset (e.g. a server, information) that, if it were compromised, would negatively impact the Commonwealth's investment in the asset and threaten the Commonwealth's ability to serve the public.

Impact - The extent to which a risk (if realized) would impact the organization.

Incident – Any event or set of events that creates a potential threat for loss or disruption to business operations, reputation, or assets.

Incident Response Coordinator – The Commonwealth CISO, or his or her designee, who oversees, provides guidance, and directs the incident response team when a security incident occurs.

Incident Response Lead – The person designated by the Commonwealth CISO to oversee response efforts for a specific information security incident.

Information Asset - Any written business or customer information related to the Commonwealth, including but not limited to reports, emails, database content, code, and unorganized information sets.

Information Custodian – Person responsible for overseeing and implementing the necessary safeguards to protect the information system, at the level classified by the Information Owner (e.g., System Administrator, controlling access to a system component).

Information Owner – Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Security Team – Team responsible for the protection of Information and Information Systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability.

Information Security Incident – Any incident that compromises the confidentiality, integrity or availability of Information and creates a potential threat for loss or disruption to business operations, reputation or assets and is also a violation of information security Policies or general security practices.

Information System – A discrete set of technology resources organized for the creation, storage, processing, transmission, use or disposal of Information.

Information Technology Management – Individuals or groups with management responsibilities over the design, operations and maintenance of internal and customer-facing technology infrastructure, systems, and processes.

Information Technology Risk – Probability of occurrence of an event combined with its adverse consequences that would impact Information Systems, Information, or operations.

Inherent Risk - The exposure to a risk in the absence of controls.

Intellectual Property Rights – Intangible rights that protect the Commonwealth's or its vendors' copyrightable work, patented technology inventions, trademarks, and trade secrets.

Internal Use Information - Information that has NOT been expressly authorized for public release but that has not been classified as confidential. The disclosure of Internal Use information is unlikely to have a material financial, legal, regulatory, or reputational impact on the Commonwealth, its constituents, customers, and business partners.

Infrastructure as a Service (IaaS) – Type of Cloud Computing provided that allows the Commonwealth to use a cloud provider's infrastructure for fundamental computing requirements (e.g., storage, hardware, or servers).

Key – Data that is used to encrypt or decrypt information using a cryptographic algorithm.

Legal – the Office of General Counsel of Massachusetts Executive Office of Technology Services and Security (unless otherwise explicitly stated in text).

Log – A record of the Events occurring within an organization's systems and networks.

Malware – Consists of a variety of forms of hostile, intrusive or annoying software or program code designed to disrupt operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and cause other abusive behavior. Examples include, but are not limited to, computer viruses, worms, Trojan horses, spyware, adware, and other malicious and unwanted software or programs.

Mobile Device – A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, onboard sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets, and E-readers (generally running a mobile operating system).

Module – When developing a network architecture, industry leading practice is to break down the larger, more complex enterprise network into smaller manageable areas called modules. These modules are intended to logically categorize network platforms, systems and end-user devices into high-level areas that serve a distinct role and whose unique functions and features collectively constitute effective network architecture.

Multi-Factor Authentication (MFA) - A multi-step account login and user authentication method, in which a user is granted access to a website or application, only after successfully presenting two or more pieces of evidence to an authentication mechanism. MFA requires users to enter more information than just a password. For example, along with the password, users might be asked to enter a code sent to their email, or mobile device, answer a secret question, or scan a fingerprint. (See Two-Factor Authentication).

Originator Usage Period – The period of time during which cryptographic protection may be applied to data is called the originator usage period, and the period of time during which the protected information is processed is called the recipient usage period.

Passphrase – A passphrase is a sequence of words or other text used to control access to a computer system, program, or data. A passphrase is similar to a password in usage but is generally longer for added security. Passphrases should have the following characteristics:

- Long enough to be hard to guess
- Not a famous quotation from literature, holy books, et cetera
- Hard to guess by intuition—even by someone who knows the user well
- Easy to remember and type accurately

One method to create a strong passphrase is to use dice to select words at random from a long list. Another method is to choose two phrases, turn one into an acronym and include it in the second, making the final passphrase. Passphrases are preferred over passwords as they are more difficult to crack.

Patch Management Process - Procedures that involve identifying, acquiring, testing, and installing patches, or making code changes to solve security vulnerabilities, fix bugs, or add features to a network's software or operating systems.

Person – a natural person, corporation, association, partnership, or other legal entity.

Personally Identifiable Information (PII) - Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media. Other statutes or regulations may define PII differently.

Personal Information (MGL Ch. 93H) - 'Personal information'' as defined in M.G..L Ch. 93H includes a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that ''Personal Information'' shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Personnel – The Commonwealth’s state employees, contractors, consultants, vendors, and interns, including full-time, part-time, or voluntary.

Plan of Action and Milestones (POAM) – A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks and scheduled completion dates for the milestones.

Policy – Management statement on a topic defining the direction of the organization and describing the cultural norms and values to be upheld.

Privacy - The rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure, and disposal of personal information or PII.

Privacy Officer – Commonwealth Agencies and Offices must designate at least one individual to serve as their primary Privacy Officer to facilitate compliance with the Enterprise Privacy Office (EPO) privacy policies and standards, coordinate with the EOTSS EPO and the Commonwealth CPO on privacy initiatives.

Procedure – Technical documentation describing specific steps to configure systems or perform tasks in a manner which supports the related standard and Policies.

Process – A series of actions or steps taken in order to achieve a particular end. An organized group of related activities that work together to transform one or more kinds of input into outputs that are of value to an organization.

Process Owner - An individual who is responsible for the management and operations of identified IT processes.

Protected Health Information - Protected Health Information relates to electronic, paper, or oral accounts of a person’s health information and finances. ePHI are electronic records of health information related to individuals to include past, present, and future procedures, and finances.

Public Information - Information that has been expressly approved for public release or information available from public sources.

Release Management Process – The planning, designing, scheduling, testing, deploying, and controlling of software releases. RMP ensures that release teams efficiently deliver the applications and upgrades required by the organization, while maintaining the integrity of the existing production environment.

Remote Access – Any access to internal Commonwealth information assets from any external non-Commonwealth location, including Mobile-Access VPN and Site-to-Site Remote Access.

Residual Risk - Risk level that exists taking into consideration the treatment of risks utilizing controls.

Restricted Information – Any confidential or personal information that is intended for a limited number of persons who possess the highest level of access control and security clearance, and who need the restricted information to perform their duties. Restricted information is protected by law or policy. There are usually governing statutes, regulations or standards with very specific provisions that dictate how this type of data must be protected. It is intended for a very limited use and must not be disclosed except to those who have explicit authorization to view or use the data. Unauthorized disclosure of this information could have a serious adverse impact on the financial, legal, regulatory, or reputational impact on the Commonwealth, its constituents, customers, and business partners.

Risk - A risk is any event or circumstance that could adversely affect the achievement of organizational objectives. Risk is defined in terms of the likelihood of occurrence and impact if it occurs.

Risk Governance Committee - Committee responsible for the oversight of the risk assessment process.

Risk Tolerance - The willingness of an organization to accept a given level of risk. Clarifying risk tolerance levels supports informed decision-making by assisting in identifying the level of risk that is permissible.

Secretariat Chief Information Officer (SCIO) - The person responsible for technology services, security, and information technology in each executive office other than the executive office of technology services and security, who reports to both the secretary of technology services and security and the secretary of the executive office for whose technology services the SCIO is responsible.

Security Administrator - Personnel with security administration roles that are responsible for the creation of accounts and the assignment of privileges. The Security Administrator is often the point person for a cybersecurity team, who is responsible for installing, administering, and troubleshooting an organization's security solutions. The security administrator will ensure the network's security, protect against unauthorized access, modification, or destruction, and troubleshoot any access problems.

Security Incident - Any event which has the potential or has already resulted in the unauthorized acquisition, misappropriation, use or manipulation of information that compromises the confidentiality, integrity, or availability of the Commonwealth’s information assets.

Security Incident Response Team (SIRT) – a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity.

Sensitive Data – Restricted and/or Confidential information and data which is more significantly related to the notion of a person's reasonable expectation of privacy, such as medical or financial information, that must be kept safe and out of reach from all unauthorize individuals unless they have permission to access the data. Access to sensitive data should be limited through sufficient data security and information security practices designed to prevent data leaks and data breaches. (See *Confidential Information*).

Software - The programs and other operating information used by a computer and that when combined, form the instructions that tell a computer what to do. Software comprises the entire set of programs, procedures, and routines associated with the operation of a computer system. (The term 'Software' is used to differentiate these instructions from hardware—i.e., the physical components of a computer system).

Stakeholders – Internal and external parties who have an interest in and are directly affected by any decision or activity of an organization.

Standard – Management statement describing the behavioral expectations or technical implementations of the related sub-Policies and Policies.

Stateful Traffic Inspection – The inspection of traffic by platforms and systems where the state of connections is monitored for non-compliance with information in a state table.

Third Parties – Third Parties are individuals or firms that are not the Commonwealth's employees or the Commonwealth's entities, but that have access to the Commonwealth's resources.

Two-Factor Authentication: Authentication using two of the following:

- Something you know (i.e., a password)
- Something you have (i.e., a token device or smart card)
- Something you are (i.e., biometrics—fingerprint, retinal scan, etc.)

User – A person or entity (e.g., system, service) with authorized access.

Vulnerability – A vulnerability is any type of defect, flaw, or weakness present in a network, system, set of procedures or a computer that can be exploited by an attacker, or allows information security to be exposed to a threat. Vulnerabilities can occur through flaws, features, or user error. Threat actors will exploit one or more vulnerabilities to negatively impact a network, or to access confidential data within an organization.

6. DOCUMENT CHANGE CONTROL

Version No.	Revised by	Effective date	Description of changes
0.90	Jim Cusson	10/01/2017	Corrections and formatting.
0.95	Anthony O'Neill	5/31/2018	Corrections and comments.
1.0	Dennis McDermitt	06/01/2018	Pre-publication review
1.0	Andrew Rudder	10/4/2018	Approved for Publication by: John Merto
1.1	Megan Perkins	7/15/2020	Annual Review; Minor corrections and formatting
1.2	Sean M. Hughes	11/04/2021	Annual Review
1.3	Thomas E. McDermott	12/4/2023	Corrections, formatting, updating and Annual Review

1.4	Anthony O’Neill	12/4/2023	Final Review

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

5.1 Annual Review

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