Commonwealth of Massachusetts

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

Glossary of Terms

Document Name: Glossary of	Effective Date: October 15, 2018
Terms Document ID: IS.Glossary	Last Revised Date: March 20, 2025

Table of Contents

1. Purpose

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

2. Authority

2.1. Pursuant to M.G.L. Ch. 7d, the Executive Office of Technology Services and Security, (EOTSS), possesses the authority to establish ***policies***, ***procedures***, and objectives with respect to activities concerning ***information*** technology. M.G.L. Ch. 7d provides in pertinent part: "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

3.1. This document applies to the use of ***information, information systems***, ***assets***, ***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 use or participate in services provided by the Executive Office of Technology Services and Security, (EOTSS), by any form of contractual arrangement, are required to comply with this document, as a condition of use. Commonwealth Agencies and Offices are required to implement ***procedures*** that ensure their ***personnel*** comply with the requirements herein to safeguard ***information***.

4. Responsibilities

4.1. The Enterprise Risk Management Office is responsible for the development and ongoing maintenance of this ***standard***. The Enterprise Risk Management Office is responsible for this ***standard*** and may enlist other departments to assist in maintaining and monitoring compliance with this ***standard***. The owner of this document is the ***Commonwealth CISO***, or his or her designee. The ***document owner*** will review and update this ***standard*** on an annual basis, or when significant ***policy*** or procedural changes necessitate an amendment. Questions regarding this document must be submitted to the ***document owner*** by sending an email to ERM@mass.gov.

4.2. The Enterprise Risk Management Office is responsible for this ***standard*** and may enlist other departments to assist in the monitoring and maintenance of compliance with this ***standard***.

4.3. Additional *information* regarding this *standard* and its related *policies* and *standards* may be found at https://www.mass.gov/cybersecurity/*policies.*

4.4. In the event of any conflict between the provisions contained in this *standard* and the provisions set forth in any of the Enterprise Information Security Policies, the provisions in the Enterprise Information Security Policies will govern.

4.5. Definitions of terms in bold may be found in the *IS.Glossary of Terms* at https://www.mass.gov/cybersecurity/policies.

5. Compliance

5.1. Compliance with this document is mandatory for the Executive Branch and all Commonwealth Agencies and Offices. Violations are subject to disciplinary action in accordance with applicable employment and collective bargaining agreements, up to and including the termination of their employment and/or assignment with the Commonwealth.

5.2. In the event any Commonwealth Agency or Office is unable to comply with any of the requirements of this document, the agency or office must submit an Information Security Policy Non-Compliance Report to the Enterprise Risk Management Office online through ServiceNow, https://www.mass.gov.service-now.com).

5.3. The Non-Compliance Report will:

5.3.1. Specifically state the reason/cause of the non-compliance

5.3.2. Identify and explain in detail the ***risks*** created due to the non-compliance

5.3.3. Provide a detailed explanation of the ***controls*** the agency, or office will implement to mitigate the ***risks*** to an acceptable level

5.3.4. Specify the time-frame required to implement the ***controls*** and mitigate the identified ***risks***. All Risk Mitigation Plans (RMP) will be for a limited time.

5.3.5. The names and contact information for both the ***risk owner*** and the ***control owner*** designated by the agency to accept and manage the ***risks*** associated with the non-compliance and implement the ***controls*** that will effectively mitigate the identified ***risks***.

6. 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.

Active Directory – A Microsoft directory service for the management of identities in Windows domain networks.

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 may 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.

Artificial Intelligence (AI) - A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments.

Artificial Intelligence System - Any data system, software, hardware, application, tool, or utility that operates in whole or in part using AI.

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

Authentication - A security measure designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Backup - The process of copying information or processing status to a redundant system, service, device or medium. A copy of files, programs or other information made to facilitate recovery when needed.

Breach of Security - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where persons other than authorized users, accesses or potentially accesses information or systems, or where authorized users take actions for an other than authorized purposes, have access or potential access to information, whether physical or electronic. The unauthorized acquisition or unauthorized use of data or, 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 (CAB) – 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 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 - The individual within an agency or office who is accountable for implementing and maintaining specific risk mitigation controls. The control owner works with the risk owner to ensure the effectiveness of specific 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. The Commonwealth considers data and information as assets.

Data Loss Prevention (DLP) - Systems ability to identify, monitor, and protect data in use (e.g. endpoint actions), data in motion (e.g. network actions), and data at rest (e.g. data storage) through deep packet content inspection, contextual security analysis of transaction (attributes of originator, data object, medium, timing, recipient/destination, etc.), within a centralized management framework. Data loss prevention capabilities are designed to detect and prevent the unauthorized use and transmission of NSS information.

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

Data Owner - The individual responsible 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 - Refers 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) – Any return or return information (and information derived from it) that is in the recipient's possession or control that is covered by the confidentiality protections of the Internal Revenue Code (IRC) and corresponding federal regulations and guidance. FTI is subject to the IRC safeguarding requirements including IRS oversight. FTI may contain personally identifiable information (PII). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source. FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

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.

Generative Artificial Intelligence (Generative AI) - a type of artificial intelligence technology that can generate many forms of content including but not limited to texts, images, and multimedia.

General — information that has NOT been published and has NOT been expressly authorized for public release but has not been classified as confidential or restricted. General information is intended for use within the agency or office. General information is available to internal personnel and authorized external parties, (e.g., external audit firms, third-party vendors, etc.). General information may be subject to disclosure under Public Records laws. Examples may include but are not limited to organization charts and personnel directories, internal policies and documentation, and personnel awareness and training collateral.

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 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 - Any communication or representation of knowledge such as facts, ideas, data, instructions, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual, that can be communicated between system entities, or which can be represented (encoded) as various forms of data. The Commonwealth considers data and information as assets.

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 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 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 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.

Infrastructure as a Service (IaaS) – Type of cloud computing that allows the Commonwealth to use a cloud provider's infrastructure for fundamental computing requirements such as servers, storage, networking and virtualization.

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.

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.

Metadata – Information that describes the characteristics of data including, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels). Metadata is structured information that describes, explains, locates, or otherwise make it easier for the user to retrieve, use, or manage an information resource. Metadata is data about data. Metadata is data that provides information about one or more aspects of the data, such as the author of a document, date created, date modified and file size. Metadata is used to summarize basic information about data to make tracking and working with specific data easier.

Mitigate – To reduce the severity, or impact of an event or incident. A decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities. The temporary reduction or lessening of the impact of a vulnerability or the likelihood of its exploitation. In cybersecurity, mitigation is centered around strategies to limit the impact of a threat to an information technology environment.

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).

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.

Password - A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. A protected/private string of letters, numbers, and/or special characters used to authenticate an identity or to authorize access to data and/or systems.

Patch - A small piece of software deployed to fix problems that were detected in a program to ensure that endpoints are protected from cyberattacks and security threats. Patches are software and operating system (OS) updates that address security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance issues, as well as to provide enhanced security features.

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 (M.G.L. 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.

Phishing - A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the threat actors disguise themselves as a legitimate business or reputable person.

Plan of Action and Milestones (POAM) – A document that identifies tasks needing to be accomplished. A POAM 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 – The person responsible for promoting privacy and security in the use and dissemination of sensitive data. A privacy officer is also responsible for resolving any concerns regarding privacy and security in the use of data. Commonwealth Agencies and Offices must designate at least one individual to serve as their primary Privacy Officer to facilitate compliance with the Commonwealth CPO on privacy initiatives.

Privilege Creep – the gradual accumulation of network access levels beyond what a user needs to do his or her job. Users need specific privileges to perform the tasks associated with their positions. Privilege creep involves the gradual accrual of access rights beyond those necessary for an individual to perform the duties of the user's current role. Privilege creep poses a substantial security risk, potentially opening the door to inadvertent and intentional internal data breaches within an organization.

Privileged Access – Account holders with elevated capabilities beyond regular users. Individual with privileged access may possess the ability to add, delete, or change the permissions of other users. Privileged access users may also have the credentials to install and uninstall software and access restricted parts of operating systems that are off-limits to a standard user.

Privileged Access Management (PAM) - An identity security solution that helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources. PAM provides visibility into what personnel are using privileged accounts and what they are doing while they are logged in. Limiting the number of users who have access to administrative functions increases system security while additional layers of protection mitigate data breaches by threat actors.

Principle of Least Privilege (PoLP) – An information security doctrine in which a user is given the minimum levels of access, or permissions, needed to perform his or her job functions, and nothing more. PoLP is a cybersecurity industry best practice and is a fundamental step which must be implemented to protect the Commonwealth's information, data, assets and IT systems.

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 (PHI) – Information that 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.

Published Information - Information that has been expressly approved for public release or information available from public sources. Information can only be designated as Published by the authorized personnel; each Secretariat is responsible for maintaining the list of authorized personnel. Examples may include but are not limited to press releases, information on public facing websites (e.g., Mass.gov), promotional materials for Commonwealth constituent services (e.g., Medicaid enrollment), advertising of open positions and roles.

Ransomware - A type of malicious attack where attackers encrypt an organization's data and demand payment to restore access.

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

Remediate – The process of improving or correcting a situation. Remediation is a process that focuses on effectively identifying and addressing the root cause of vulnerabilities and resolving security incidents when they occur. Incident remediation is the final stage of an incident response process where the impacts of a cyberattack are reduced, reversed, or neutralized.

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 Owner – The individual within an agency or office who is responsible to oversee each individual risk identified in an ERM report. The risk owner is a management-level official, (SCISO, agency SCISO, or similar manager level), who serves as an accountable point of contact and is responsible to manage, track and respond to individual risks. The risk owner works with the control owner to develop a risk mitigation plan and ensures that specific controls are implemented that will effectively mitigate identified risks.

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). Types of 'Software' include, but are not limited to:

- Operating Systems - system software on enterprise assets that manages computer hardware and software resources and provides common services for programs. Operating systems are considered a software asset and can be single- and multi- tasking, single- and multi-user, distributed, templated, embedded, real-time, and library.
- Applications - a program, or group of programs, hosted on enterprise assets and designed for end users. Applications are considered a software asset in this document. Examples include web, database, cloud-based, and mobile applications. There are multiple components that make up applications and operating systems, including services and libraries.
- Services - refers to a software functionality or a set of software functionalities, such as the retrieval of specified information or the execution of a set of operations. Services provide a mechanism to enable access to one or more capabilities, where the access is provided using a prescribed interface and based on the identity of the requestor per the enterprise's usage policies.
- Libraries - pre-written code, classes, procedures, scripts, configuration data, and more, used to develop software programs and applications. It is designed to assist both the programmer and the programming language compiler in building and executing software.

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, vendors, or firms that are not the Commonwealth's employees or Commonwealth organizations but have authorized 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.

Virtual Private Network (VPN) – A VPN is a technology used to create a safe and encrypted point-to-point connection between a device and a server over a less secure network. The encrypted connection helps ensure that sensitive data is safely transmitted. A VPN creates an encrypted tunnel to transmit data and has the ability to hide a user's IP address and protect the user's online identity. Using a VPN prevents unauthorized persons from eavesdropping and allows the user to perform work remotely.

Virus - A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.

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.

Zero-Day Attack – A cybersecurity attack that exploits a previously unknown flaw in software, hardware or firmware. "Zero day" refers to the fact that the software or device vendor has zero days to fix the flaw because malicious actors can already use it to access vulnerable systems.

Zero-Day Vulnerability – A flaw in software for which no official patch or security update is available. A software vendor may or may not be aware of the vulnerability, and no information about the vulnerability is publicly available.

Zero-Trust Architecture – A cybersecurity framework that requires all users, whether inside or outside of the organization's network, to be authenticated, authorized, and continuously validated in order to obtain access and retain access to the Commonwealth's IT environment. Zero Trust Architecture is a system management strategy which acknowledges that threats exist both inside and outside the Commonwealth's network. The Zero Trust security model eliminates implicit trust in any one element, component, node, service, system or user and instead requires continuous verification through real-time information from multiple sources to determine access and other system responses.

7. 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 McDermott	12/4/2023	Corrections, formatting, updating and Annual Review
1.4	Anthony O'Neill	12/4/2023	Final Review
1.5	Miklos Lavicska	8/8/2024	Corrections, formatting, updating
1.5	Thomas McDermott	12/27/2024	Corrections, formatting, updating and Annual Review
1.5	Anthony J. O'Neill	1/1/2025	Final Review
1.6	Thomas McDermott	3/6/2025	Updates, Corrections and Formatting
1.6	Miklos Lavicska	3/11/2025	Corrections and Formatting
1.6	Anthony J. O'Neill	3/20/2025	Final Review