pennsylvania
OFFICE OF ADMINISTRATION

EBR, Office of Information Technology Policy Definitions

Name:	Policy and Procedure Definitions
Effective Date:	January 2019
Category:	Administrative
Version:	1.3

1. Scope:

This applies to all policies for the agencies supported by the Employment Banking & Revenue (EBR) delivery center.

2. Definitions:

Term	**Definition**
Access Control	A security control class that is the selective restriction of access to a physical location or other resource, based on identification, authentication and authorization. The act of accessing may mean consuming, entering, or using. Identification includes a credential or password to distinguish one user from another. Authentication is a layer of scrutiny applied to the identification. Permission to access a resource is called authorization.
Access Management	The ITSM process responsible for allowing users to make use of IT services, data or other assets. Access management helps to protect the confidentiality, integrity, and availability of assets by ensuring that only authorized users are able to access or modify them. Access management implements the policies of information security management and is sometimes referred to as rights management or identity management.
After Action Review (AAR)	AAR is a simple process used by a team to capture the lessons learned from past successes and failures with the goal of improving future performance.
Agency Website	For the purposes of EBR policy, all Internet, Intranet, and subsites under the management, control, or oversight of the agencies in EBR.
Agile Model	A highly iterative software application development model used in an SDLC, that involves an interactive, cross-functional, and focused team approach to build software solutions in a time boxed (sprints) development methodology. The Agile model uses feedback and checklists, tightly integrated cross functional teams, and multi-faceted iterations or sprints to quickly build custom software applications. Feedback is driven by regular tests and releases of the software.

EBR, Office of Information Technology Policy Definitions

Application Management	The ITSM function responsible for managing applications throughout their lifecycle.
Application-Level backup	Application-Level information includes information other than system-level information specifically; installation, configuration, and data collections used by a specific application.
Asset and Configuration Management	The ITSM process responsible for ensuring that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets.
Audit Log	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Audit Record	Individual record of security event information such as successful and failed authentication attempts, file accesses, security policy changes, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges.
Availability	Ensuring that authorized users have access to information and associated assets when required.
Availability Management	The ITSM process responsible for ensuring that IT services meet the current and future availability needs of the business in a cost-effective and timely manner. Availability management defines, analyzes, plans, measures, and improves all aspects of the availability of IT services. Availability management ensures that all IT infrastructures, processes, tools, roles, etc. are appropriate for the agreed service level targets for availability.
Baseline Configuration	In configuration management, a "baseline" is an agreed description of the attributes of a product, at a point in time, which serves as a basis for defining change. A "change" is a movement from this baseline state to a next state.
Bug Fix	See Major & Minor Release
Business Entity User	Any user within organizations that provide services to, or receive services from the commonwealth. These organizations may have multiple users that work and access

	the L&I domain. These organizations include employers, service/training providers, and business partners.
Business Impact Analysis (BIA)	BIA is a systematic process to quantify the business impact of a loss of a service as a result of a disaster, accident, or emergency.
Business Partners	Businesses that enter into contractual relationships to provide services on behalf of or in conjunction with the commonwealth.
Business Relationship Management	The ITSM process responsible for maintaining a positive relationship with customers. Business relationship management identifies customer needs and ensures that the service provider is able to meet these needs with an appropriate catalogue of services. This process has strong links with service level management.
Capacity management	The ITSM process responsible for ensuring that the capacity of IT services and the IT infrastructure is able to meet agreed capacity- and performance-related requirements in a cost-effective and timely manner. Capacity management considers all resources required to deliver an IT service, and is concerned with meeting both the current and future capacity and performance needs of the business. Capacity management includes three sub-processes: business capacity management, service capacity management, and component capacity management.
Change Control	A systematic approach to managing all changes made to an application, system or the underlying hardware. The purpose is to ensure that no unnecessary changes are made, that all changes are documented or approved, that services are not unnecessarily disrupted and that resources are used efficiently.
Change Evaluation	The ITSM process responsible for formal assessment of a new or changed IT service to ensure that risks have been managed and to help determine whether to authorize the change.
Change Management	The ITSM process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

EBR, Office of Information Technology Policy Definitions

Cleansing, Wiping, or Sanitizing	The use of approved “WipeDrive” software in accordance with Federal Department of Defense standards to remove all data from a hard drive or other storage device. (See also Sanitization)
Commonwealth (EBR) IT assets	Includes laptops, desktops, tablet PC's, Blackberrys, PDAs, printers (see also Computing Device and IT Equipment)
Commonwealth Network (EBR Infrastructure)	Direct access through network ports in EBR facilities and connections directly through the commonwealth-provided remote access solutions.
Computing Device	Any computerized machine or related device with electronic memory or storage that is either owned or leased by EBR, or that is owned by contractors and used on behalf of the commonwealth (whether or not it is connected to the network). Examples of these devices include PCs, laptops, network copiers, multi-function printers, Personal Digital Assistant (PDA) devices, data-style cell phones, floppy disks, CDs, optical platters, zip disks, storage/back-up tapes, and memory storage cards.
Confidentiality	Ensuring that information is accessible only to authorized users.
Configuration Item (CI)	Configuration Items, in ITIL terminology, are components of an infrastructure that currently is, or soon will be under configuration management. CIs may be a single module such as a monitor or tape drive, or more complex items, such as a complete system. CIs are fundamental structural unit of a configuration management system.
Configuration Management (CM)	Configuration Management (CM) is an ITIL systems engineering process for establishing and maintaining consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.
Configuration Management Database (CMDB)	configuration management database is an ITIL term, that is a repository that acts as a data warehouse for information technology (IT) installations. It holds data relating to a collection of IT assets (commonly referred to as

	configuration items (CI)), as well as to descriptive relationships between such assets
Contingency Plan	A plan or procedure that will take effect if an event or emergency situation occurs. See also BIA.
Continuity of Operations Planning (COOP)	Efforts within program areas to ensure that their critical functions continue during a wide range of emergencies and disruptions, including, for example, localized acts of nature, accidents, and technological or attack-related emergencies. COOP activities include plans and procedures to ensure that critical functions are performed; testing, training, and exercising ensuring a viable COOP capability; managing agency response during a disruption; and continuing and/or resuming agency critical functions throughout a disruption.
Coordinated Universal Time (UTC)	Abbreviated as UTC, is the primary time standard by which the world regulates clocks and time.
Custom application	Includes any non-COTS software that was developed and/or is maintained by EBR employees or EBR contractors.
CWOPA User	Any user who has a login through the CWOPA domain and can access protected commonwealth resources (e.g., department Intranets, e-mails). These users include, but are not limited to commonwealth employees, contractors, and help desk staff.
Cyber Security Incident	Event that violates an explicit or implied OA/Department computer security policy including all defined computer user agreements; or the possibility of a data breach through compromised equipment and/or theft/loss. (see also Information Security Incident)
Cyberattack	A deliberate exploitation of computer systems, technology-dependent enterprises, or networks. Cyberattacks use malicious code to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft.
Data Owner	Person or persons from the program area(s) or external to the agency, who have possession of and responsibility for a single piece or set of data elements. Data Owners provide rules concerning the use and distribution of their data.

EBR, Office of Information Technology Policy Definitions

Demand Management	The ITSM process responsible for understanding, anticipating, and influencing customer demand for services. Demand management works with capacity management to ensure that the service provider has sufficient capacity to meet the required demand. At a strategic level, demand management can involve analysis of patterns of business activity and user profiles, while at a tactical level, it can involve the use of differential charging to encourage customers to use IT services at less busy times, or require short-term activities to respond to unexpected demand or the failure of a configuration item.
Design Coordination	The ITSM process responsible for coordinating all service design activities, processes, and resources. Design coordination ensures the consistent and effective design of new or changed IT.
Desktop application	Includes any software accessed from a desktop computer and does not include software that is accessed from a mobile device.
Desktop operating system	Refers to the desktop software program that provides a graphical user interface and enables a computer to perform basic functions.
Digital Signature	This is a type of method for authenticating digital information analogous to ordinary physical signatures on paper, but implemented using techniques from the field of public key cryptography. A digital signature method generally defines two complementary algorithms, one for signing and the other for verification, and the output of the signing process is called a digital signature.
Disaster	A sudden event, such as an accident or a natural catastrophe, that causes great damage or loss of life.
Disaster Recovery Plan (DRP)	The documented process of recovering IT systems in the event of a disruption or disaster. The plan accounts for business continuity in an event that destroys part or all of a business's resources, including IT equipment, data records and the physical space of an organization.

EBR, Office of Information Technology Policy Definitions

Disruption	A circumstance or event that interrupts or prevents the correct operation of system services and functions.
Domain	A group of computers that are part of a network and share a directory database. This database is housed on a server called the domain controller. In order to log on to a domain, both the computer and user must have an account in the domain database. Networking resources are centrally allocated and administered by the domain administrator.
Domain Name System (DNS)	A system for naming computers and network services that is organized into a hierarchy of domains. DNS naming is used in TCP/IP networks, such as the Internet, to locate computers and services through user-friendly names.
Downtime	The period of time when something, such as a piece of machinery, or IT system, is not in operation, or is in degraded in operation.
e-Discovery	e-discovery refers to any process in which ESI is identified, collected, secured, searched, and analyzed for the purpose of using it as evidence in a civil or criminal legal case. See Electronically Stored Information (ESI)
Electronic Signature	Is "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." Although all electronic signatures are represented digitally, they can take many forms and can be created by many different technologies. (See also "Signature")
Electronically stored information (ESI)	Electronically Stored Information, for the purpose of the Federal Rules of Civil Procedure (FRCP) is information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software. This includes any data found in e-mail, voicemail, instant and text messages, databases, metadata, digital images and any other type of file.
Elevated Privilege	A level of system or application permission, based on role that allows the user to perform a greater variety of operations including advanced functions. (See Role-Based Access.)

EBR, Office of Information Technology Policy Definitions

Emergency Release	Required to solve immediately, critical system or business issue for which there is no work around and the fix is required before the next scheduled release.
Enhancement	See Major & Minor Release
Enterprise VPN Service	A "user-managed" service whereby remote access is provided to the Commonwealth Enterprise Network via a pre-existing Internet connection. This pre-existing connection may be, but is not limited to, Digital Subscriber Line (DSL), Cable modem, and direct Internet connections (either wired or wireless). Using an available public telecommunications infrastructure, information is encrypted before sending it through the public network and decrypted at the other end. This service provides a secure and private computing session through which authorized users can remotely connect via the Internet to Commonwealth Enterprise and agency resources.
Event	A change of state or occurrence that has significance for the management of an IT service or other configuration item (CI). Events are typically recognized through alerts or notifications detected by a monitoring tool.
Event Management	The ITSM process responsible for managing events throughout their lifecycle. Event management is one of the main activities of IT operations.
e-waste	Broken or unusable IT Equipment.
External Website	For the purposes of EBR policy, any website that is not under the management or control of the commonwealth.
Federal Tax Information (FTI)	FTI is a term of art and consists of federal tax returns and return information (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections and safeguarding requirements including IRS oversight. FTI is categorized as Sensitive and may contain personally identifiable information (PII).
Financial Management	This ITSM function and processes responsible for managing an IT service provider's budgeting, accounting, and charging

	requirements. Financial management for IT services secures an appropriate level of funding to design, develop and deliver services that meet the strategy of the organization in a cost-effective manner.
Formatting	The use of the operating system format command to remove all data from a hard drive. (See also Cleansing, Wiping, or Sanitizing)
Governance	Rules, policies, processes, and in some cases laws by which businesses are operated, regulated and controlled. Strategic perspective of IT focusing on the "what." IT Governance captures the IT process and service performance requirements that are important to achieve strategically and directly map to Corporate Governance objectives and desired outcomes.
Identity and access management (IAM)	The security discipline that enables the right individuals to access the right resources at the right times for the right reasons. IAM addresses the mission-critical need to ensure appropriate access to resources across heterogeneous technology environments, and to meet rigorous compliance requirements. IAM is business-aligned, and it requires business skills, not just technical expertise.
Incident Management	The ITSM process responsible for managing the lifecycle of all incidents. Incident management ensures that normal service operation is restored as quickly as possible and the business impact is minimized.
Information Security	Preservation of confidentiality, integrity, and availability of information.
Information Security Breach	An event believed to compromise the security or confidentiality of information used in the conduct of EBR business.
Information Security Incident	An event or warning of an event that in any way compromises critical information to the department; including, but not limited to, client/employee personal data and internal organizational data that is not explicitly deemed available for public access. (See also Cyber Security Incident)

EBR, Office of Information Technology Policy Definitions

Information Security Infrastructure	The complete set of information-security-related systems, procedures, policies, and physical implementations of information technology security administration within EBR.
Information Security Management	The ITSM process responsible for ensuring that the confidentiality, integrity and availability of an organization’s assets, information, data, and IT services match the agreed needs of the business. Information security management supports business security and has a wider scope than that of the IT service provider, and includes handling of paper, building access, phone calls, etc. for the entire organization.
Information System	The network or combinations of all computing equipment, telecommunication or other communication or information processing devices and channels used within an organization.
Integrated Voice Response (IVR)	In telecommunications, an IVR allows callers/customers to interact with an organization’s computer systems via a telephone keypad or by speech recognition, after which they can service their own inquiries by following the IVR dialogue. IVR systems can respond with prerecorded or dynamically generated audio to further direct users on how to proceed. IVR applications can be used to control almost any function where the interface can be broken down into a series of simple interactions.
Integrity	Safeguarding the accuracy and completeness of information and processing methods.
Intrusion Detection System (IDS)	An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information systems through malicious activities or through security policy violations.
Intrusion Prevention System (IPS)	An IPS is a system that monitors a network for malicious activities such as security threats or policy violations. The main function of an IPS is to identify suspicious activity, and then log information, attempt to block the activity, and finally to report it.
IPAM	Identity Protection and Access Management
IT Equipment	PC desktops, laptops, docking stations, keyboards, mice, monitors, monitor stands, PC speakers, servers, routers,

	switches, firewalls, load balancers, printers/copiers/multi-function devices, scanners, APC/UPS, cellular/smart phones, iPhones, iPads, tablets, personal digital assistants (PDAs), external devices that connect to a PC, audio/video equipment, computer cables (only patch cables), electronic media such as, USB drives, thumb/flash drives, SD cards, hard drives, CD, DVD, tapes, and any items that would be defined in the Asset and Configuration Management System.
IT Operations Management	The ITSM function within an IT service provider that performs the daily activities needed to manage IT services and the supporting IT infrastructure. IT operations management includes IT operations control and facilities management.
IT Service Continuity Management	The ITSM process responsible for managing risks that could seriously affect IT services. IT service continuity management ensures that the IT service provider can always provide minimum agreed service levels by reducing the risk to an acceptable level and planning for the recovery of IT services. IT service continuity management supports business continuity management.
IT Surplus	Usable equipment such as toner cartridges, fax machines, overhead projectors, computer cables (non-patch cables), televisions, and digital equipment used in office settings.
ITIL	IT Infrastructure Library (ITIL) - an acronym for Information Technology Infrastructure Library, is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. It is a five-stage lifecycle of IT services, including strategy, design, transition, operation, and continual service improvement.
ITSM	IT Service Management (ITSM) - The entirety of activities – directed by policies, organized and structured in processes, and supporting procedures – that are performed by an organization to plan, design, deliver, operate, and control information technology (IT) services offered to customers.
Knowledge Management	The ITSM process responsible for sharing perspectives, ideas, experience and information, and for ensuring that these are available in the right place and at the right time. The knowledge management process enables informed

	decisions and improves efficiency by reducing the need to rediscover knowledge.
Least privilege	A principle and practice of securing information technology systems. As a system principle; it refers to the security objective of granting users only those accesses they need to perform their official duties. As a practice; it is the application of limiting access to the minimal level that will allow normal functioning. It is the lowest level of user rights for the user to still do their job.
Litigation Hold	Files that are preserved in relation to an actual or reasonably anticipated litigation. See Records Legal Hold.
Major Release	Significant functional enhancements which impact multiple parts of the system, or multiple systems. Includes: New application Go-live, Existing application: major functional changes, COTS product version upgrades. Changes to an existing application/system initiated by a change in platform (java/.Net, Oracle/SQL, WAS/IIS), OS (AIX vs. Win) or architecture (COTS/Custom, single server/redundant/load balanced). A new service that provides more than a new data stream or functionality added to an existing system. Database changes altering table structure, importing or exporting data
Maximum Tolerable Downtime (MTD)	The total amount of time that a business process can be disrupted or inoperative without causing any unacceptable consequences. See also Downtime, RPO, and RTO.
Minor Release	Simple changes that are contained within one element of the system and which do not require a full regression test. Includes: incident (defect) fixes/bug fixes, a change to an existing application/system that corrects something which doesn't work as expected or documented. Changes to an existing application/system that provides additional functionality. Database changes adding/removing/changing stored procedures
Miscellaneous Media/Devices	Any computerized machine or related device with electronic memory or storage that is either owned or leased by EBR, or that is owned by contractors and used on behalf of the commonwealth (whether or not it is connected to the network) with exception to mainframes, PCs, and laptops. Examples of these devices include Personal Digital Assistant (PDA) devices, data-style cell phones, floppy disks, CDs,

	optical platters, zip disks, storage/back-up tapes, and memory storage cards. *See Removable storage media
Mission Critical Applications (MCA)	A system that is essential to the survival of the agency. When an MCA fails or is interrupted, business operations are significantly impacted.
Mission Essential Function (MEF)	MEF are the limited set of department and agency level government functions that must be continued throughout, or resumed rapidly after, a disruption of normal operations. MEFs are functions that cannot be deferred during an emergency or disaster.
Mobile Device	Any tablet, cell phone, smart phone, hand held scanner or similar device.
Multi-Function Device (MFD)	An office machine that incorporates the functionality of multiple devices in one, so as to have a smaller footprint in a business setting, and provide centralized document management /distribution /production in a large-office setting. A typical MFP may act as a combination of some or all of the following devices – printer, scanner, copier, fax and email.
Network Time Protocol (NTP)	A protocol that is used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.
New Development	Replaced by Major & Minor Release
NIST	National Institute of Standards and Technology (NIST), a non-regulatory agency of the of the U.S. Department of Commerce was established to advance science, standards, and technology with uniform metrics.
Non-IT Surplus	Non-electronic items such as printer paper or labels, shredders, typewriters, adding machines, calculators, tables, desks, chairs, cabinets or bookshelves, and power strips.
OIT Policies	Statements of management direction on specific subjects intended to influence and determine decisions and actions. These statements establish boundaries for action by OIT management and may necessitate the creation of supporting procedures to specify such direction.

OIT Procedures	Statements and/or interpretations of EBR OIT Policy in sufficient detail to establish methods for execution. Procedures assign responsibility and organize workflow in a manner that indicates precisely what is to be done and how it is to be done.
Operational release	Collection of planned, non-emergency changes that have the potential to affect multiple system underpinning applications like: webMethods, Identity Manager, or SiteMinder. Each release will have limited scope.
Personal Identification Number (PIN)	A secret number that a claimant memorizes and uses to authenticate his or her identity. PINs are generally only decimal digits.
Personally Identifiable Information (PII)	PII as used in US privacy law and information security, is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context, such as: Name (Full name, Maiden name, Mother's maiden name, Alias), Date of Birth, Personal identification numbers (Social Security number (SSN), Passport number, Driver's license number, State identification card number, Taxpayer identification number, Federal Employer Identification Number (FEIN) or Employer Identification Number (EIN) – In cases where SSN could be used as FEIN or EIN Financial account or credit card numbers, Address information (Street address, Mailing address, Physical address), Personal characteristics (Fingerprints, Other biometric data (e.g., retina scan, palm scan, voice signature, facial geometry))
Problem Management	The ITSM process responsible for managing the lifecycle of all problems. Problem management proactively prevents incidents from happening and minimizes the impact of incidents that cannot be prevented.
Protected data	Information that is subject to some degree of protection under any Pennsylvania or federal statute, order, or regulation. This information includes but is not limited to: Data elements as defined in the Breach of Personal Information Notification Act P.L. 474, No. 94 or Information received from a federal or Commonwealth entity bound by specific regulations including but not limited to the following

	sources: Social Security Administration (SSA), Internal Revenue Service (IRS), Criminal Justice Agencies in accordance with CHRIA, Educational Institutions subject to the Family Education Rights and Privacy Act (FERPA), Entities subject to the Payment Card Industry (PCI) data security standards, Health care entities subject to HIPAA or other data privacy or security law in the health care industry (including internal entities). Third Party Data: Information associated with and specific to the Commonwealth's regulated entities, vendors, suppliers, business partners, contractors, and other third party entities, including the trade secrets of third parties. Contract Data: Information associated with contract, award, and bidding activities related to procurement of supplies or services, at appropriate stages of procurement.
Public Key Cryptography	Public-key cryptosystems have two primary uses, encryption and digital signatures. In their system, each person gets a pair of keys, one called the public key and the other called the private key. The public key is published, while the private key is kept secret. The need for the sender and receiver to share secret information is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. In this system, it is no longer necessary to trust the security of some means of communications. The only requirement is that public keys be associated with their users in a trusted (authenticated) manner (for instance, in a trusted directory). Anyone can send a confidential message by just using public information, but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient. Furthermore, public-key cryptography can be used not only for privacy (encryption), but also for authentication (digital signatures) and other various techniques.
Public Key Infrastructure (PKI)	A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. A PKI also is called a trust hierarchy.

EBR, Office of Information Technology Policy Definitions

Public User	Any user who self-registers for access to applications online and is not accessing applications as a Business Entity User or CWOPA User. These users have more lenient account policies (password expiration, etc.) than Business Entity or CWOPA Users. Public users include, but are not limited to UC claimants, job seekers, and CWDS participants.
Records Legal Hold	Per MD 210.5 The suspension of ordinary practices and procedures for disposing of records, as necessary, to comply with existing preservation obligations related to actual and reasonably anticipated litigation, government investigation, or audit. See Litigation Hold.
Recovery Point Objective (RPO)	The age of files that must be recovered from backup (last known good copy) storage for normal operations to resume if a computer, system, or network goes down. See also MTD and RTO.
Release and Deployment Management	The ITSM process responsible for planning, scheduling, and controlling the build, test, and deployment of releases and for delivering new functionality required by the business while protecting the integrity of existing services.
Remote Access	Access to the commonwealth network from a workstation that is not directly connected to the commonwealth network
Removable storage media	Any type of storage device that can be removed from a computer while the system is running. Examples of removable media include CD/DVDs, and USB drives. Removable media makes it easy for a user to move data from one computer to another. They are designed to be read to or written to by removable readers, writers and drives. Examples include: Optical discs (Blu-ray discs, CD/DVDs) Memory cards (CompactFlash card, Secure Digital card, Memory Stick) *See Miscellaneous Media/Devices
Request Fulfillment	The ITSM process responsible for managing the lifecycle of all service requests.
Resource Access Control Facility (RACF)	Is a security system that provides access control and auditing functionality for the z/OS and z/VM operating systems. RACF provides basic security tools to manage user access to critical resources and auditing functionality.

EBR, Office of Information Technology Policy Definitions

Return to Operation (RTO)	The maximum tolerable amount of time needed to bring all critical systems back online as a result of a disaster. See also MTD and RPO.
Role Based Access	A method of regulating access to IT Equipment or systems based on the roles of individual users within an enterprise. (See IT Equipment and Elevated Privileges)
Sanitization	The process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or released for disposal. (See also Cleansing, Wiping, or Sanitizing)
Secure Sockets Layer (SSL)	Is a protocol designed by Netscape Communications Corporation to provide encrypted communications on the Internet. SSL is layered beneath application protocols such as HTTP, SMTP, Telnet, FTP, Gopher, and NNTP and is layered above the connection protocol TCP/IP.
Secured areas	EBR owned or leased spaces that currently are or are designated to house EBR systems, including wiring closets, computer rooms, EBR data centers, OIT storage areas, and OIT workspaces.
Security Control	Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. There are three class designations (i.e., management, operational, and technical)
Security Information and Event Management (SIEM)	SIEM software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by network hardware and applications.
Security Log	(Audit Log) A chronological record of security-relevant, destination, and source information providing documentary evidence of activities that have affected a specific operation, procedure, or event.

EBR, Office of Information Technology Policy Definitions

Security Operations Center (SOC)	A SOC is a centralized unit that deals with security issues on an organizational and technical level. A SOC within a building or facility is a central location from where staff supervises the site, using data processing technology.
Security Related data	Security-related information includes, inventories of hardware, software, and firmware components. Alternate storage sites typically serve as separate storage facilities. Additionally, may include mechanisms employed by organizations to protect the integrity of information system backups include, for example, digital signatures and cryptographic hashes.
Service Catalog Management	The ITSM process responsible for providing and maintaining the service catalogue and for ensuring that it is available to those who are authorized to access it.
Service Desk	The single point of contact between the service provider and the users. A typical service desk manages incidents and service requests, and also handles communication with the users.
Service Level Management	The ITSM process responsible for negotiating achievable service level agreements and ensuring that these are met. It is responsible for ensuring that all IT service management processes, operational level agreements, and underpinning contracts are appropriate for the agreed service level targets. Service level management monitors and reports on service levels, holds regular service reviews with customers, and identifies required improvements.
Service Portfolio Management	The ITSM process responsible for managing the service portfolio. Service portfolio management ensures that the service provider has the right mix of services to meet required business outcomes at an appropriate level of investment. Service portfolio management considers services in terms of the business value that they provide.
Service Validation and Testing	The ITSM process responsible for validation and testing of a new or changed IT service. Service validation and testing ensures that the IT service matches its design specification and will meet the needs of the business.

EBR, Office of Information Technology Policy Definitions

Signature	An electronic or physical signature is a symbol that signifies intent. The definition of "signed" in the Uniform Commercial Code includes "any symbol" so long as it is "executed or adopted by a party with present intention to authenticate the writing." A signature may signify intent to be bound to the terms of a contract, the approval of a subordinate's request for funding of a project, confirmation that a signer has read and reviewed the contents of a document, and/or indication that the signer was the author of a document.
Smart Card	A plastic card containing a computer chip and enabling the holder to purchase goods and services, enter restricted areas, access medical, financial, or other records, or perform other operations requiring data stored on the chip.
Spiral Model	An incremental software development process model used in an SDLC, that incorporates requirements, design, build/construct, test/simulations, and deploy prototype phases separated by planning and risk assessment. A prototype is created with each iteration and evaluated until a final production ready (i.e., fully functional and validated) prototype model has been created. This method can be used to create temporary prototype solutions that are later discarded or for large, expensive, and complicated projects using each iterative prototype build as a phase gate and/or milestone. Documentation in this process is dynamic and incrementally refined. Documentation is finalized with the implementation of the final production ready prototype.
Standards	Specific directives, specifications, or procedures that must be followed in order to ensure a consistent implementation of information technology security practices.
Strategy Management for IT Services	The ITSM process responsible for strategic assessment, strategy generation, and strategy execution through the service lifecycle.
Supplier Management	The ITSM process responsible for obtaining value for money from suppliers, ensuring that all contracts and agreements with suppliers support the needs of the business, and that all suppliers meet their contractual commitments.
System	A computer or set of components for collecting, creating, storing, processing, and distributing information, typically

	including hardware and software, system users, and the data itself in order to solve business problems.
System Development Life Cycle (SDLC)	The SDLC is a conceptual model used in software engineering as well as project management that describes the phases involved in an information system solution development and delivery. A SDLC framework consists of multiple phases to assure high quality systems are delivered, provide strong management controls over IT projects, and ensure that the information system can, and will, work as required and is effectively maintained to support agency's missions. A subset of this process includes efforts related to software development life cycle.
System Owner	(Service Owner) Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. A key contributor in developing system design specifications to ensure the security and user operational needs are documented, tested, and implemented. Accountable for a provided service(s).
System-Level backup	System-level information includes, for example, system-state information, operating system and application software, and licenses.
Technical Management	The ITSM function responsible for providing technical skills in support of IT services and management of the IT infrastructure. Technical management defines the roles of support groups, as well as the tools, processes, and procedures required.
Transaction Security Levels	Low Risk / Low Impact Transactions (Level A) - Transactions in this category have little value to potential hackers and would have minimal consequences if compromised. Low to Medium Risk / Medium to High Impact Transactions (Level B) - Transactions in this category have moderate to high value to potential hackers and/or have moderate to high consequences if compromised. High Risk / High Impact Transactions (Level C) - Transactions are high risk, high consequence transactions that require high security measures.

EBR, Office of Information Technology Policy Definitions

Transition Planning and Support	The ITSM process responsible for planning all service transition processes and coordinating the resources that they require.
Transport Layer Security (TLS)	TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions. TLS has replaced SSL.
User-Level backup	User-level information includes any information other than system-level information.
Users	Employees, business partners, contractors, vendors, or any other parties who are granted access to an EBR production system or application.
Videoconferencing	Use of technology to connect with video and voice, to conduct agency meetings between physically distant locations, as well as non-commonwealth entities. Instead of trips that may be expensive in terms of lodging, transportation, and non-retrievable time away from the office, participants may utilize the many benefits of videoconferencing technology in disseminating information and performing job duties.
Virtual Private Network (VPN) Remote Access	Network access utilizing broadband wired/wireless technology that enables a PC to establish a network connection from the employee's commonwealth PC.
Waterfall Model	A software development process model used in an SDLC, that involves distinct sequential phases (i.e., conception, requirements, design, build/construct, test, and implementation). Solution progress is seen as flowing steadily downwards (like a waterfall) through each of the phases. A phase in the development process may begin only if the previous phase is complete. There can be some slight variations in the waterfall approach (i.e., modified water fall) that define the circumstances and processes to go back to the previous phase. Documentation in this process is also sequential, and is typically created, delivered, and approved with each phase as a prerequisite for the next phase to begin. Each phase in this model is a phase gate or key milestone.

EBR, Office of Information Technology Policy Definitions

Web browser	Refers to the desktop software program that provides a display medium for Web sites and Web pages throughout the World Wide Web.
Workstation	Any desktop, laptop, notebook, netbook, tablet or other personal computing device.

3. Version Control:

Version	**Date**	**Purpose**
1.0	08/2018	Base Document
1.1	10/2018	Updates for SEC-000
1.2	12/2018	Updates for APP-000
1.3	01/2019	Updates for SEC-002