LAMAR UNIVERSITY
INFORMATION TECHNOLOGY POLICIES

SECTION: Information Technlogy Number 10.01.00
AREA: Applicable Terms and Technologies
for Infornation Security Standards

SUBJECT: Definition Catalog

I. PURPOSE

This document is a definition catalog for applicable terms, technologies, and all LU information security policies, procedures, and standards.

II. DEFINITIONS

Access - The physical or logical capability to view, interact with, or otherwise make use of Information Resources.

Acceptable Risk - The level of Residual Risk that has been determined to be a reasonable level of potential loss/disruption for a specific information system.

Access Control - The process of granting or denying specific requests to:

- Obtain and use information and related information processing services.
- Enter specific physical facilities (e.g., data centers, physical plant, mechanical rooms, Network closets, secured buildings, and research laboratories).

Acquisition - Includes all stages of the process of acquiring products or services, beginning with the process for determining the need for the product or service and ending with contract completion and closeout.

Administrative Privileges - Rights granted to a Privileged User.

Adverse Events - Events with negative consequences. *(*E.g., System crashes. Packet floods. Unauthorized use of system privileges. Unauthorized access to sensitive data. An execution of malware that destroys data).

Affiliated User - See Organizational User.

Attribute - A claim of a named quality or characteristic inherent in or ascribed to someone or something.

Audit - Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational Procedures.

Audit Log / Audit Records - A chronological record of Information System activities, including records of system Accesses and operations performed in a given period.

Auditable Event - Events that are significant and relevant to the security of Information Systems and the environments in which those systems operate in order to meet specific and ongoing Audit needs. Audit events can include, for example, Password changes, failed log-on, or failed accesses related to Information Systems, Administrative Privilege usage, or third-party credential usage.

Authentication - Verifying the Identity of a User, process, or Device, often as a prerequisite to allowing Access to resources in an Information System.

Authenticator - The means used to confirm the Identity of a User, process, or Device. For Example, User Password or token).

Authorization - The right or permission that is granted to a system entity to access a system resource.

Authorization Boundary - All components of an Information System to be authorized for operation by an Authorizing Official and excludes separately authorized systems, to which the Information System is connected.

Authorizing Official (AO) - Official with the authority to formally assume responsibility for operating an Information System at a level of Acceptable Risk to institution operations (including mission, functions, image, or reputation), institution assets, or individuals.

Availability - The security objective of ensuring timely and reliable Access to and use of information.

Best Practice - See Guideline

Business Function – A Process or operation performed routinely to carry out a part of the mission of an institution.

Business Impact Analysis (BIA) - An analysis of an Information System's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Business Continuity Plan (BCP) - The documentation of a predetermined set of instructions or Procedures that describe how the institution's mission/business processes will be sustained during and after a significant disruption.

Certificate Authority - The entity in a Public Key Infrastructure (PKI) that is responsible for issuing public-key certificates and exacting compliance to a PKI policy. Also known as a Certification Authority.

Central Identifier - A unique Identifier issued by the Information Management and Decision Support (IMDS) division. This is commonly referred to by its public name, LEA (Lamar Electronic Access) or Lamar ID (L-Number).

Cloud Service / Cloud Computing Service - A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models. as defined in §2157.007(a), Texas Government Code.

Collaborative Computing Device - Tools that facilitate and enhance group work through distributed technology - where individuals collaborate from separate locations. Devices can include but are not limited to Networked whiteboards, cameras, and microphones.

Computer Security Incident Response Team (CSIRT) - A capability that is set up for the purpose of assisting in responding to computer security-related incidents.

Confidential Information - Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreements.

Confidentiality - The security objective of preserving authorized restrictions on information Access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control - Process for controlling modifications to hardware, Firmware, software, and documentation to protect the Information System against improper modifications before, during, and after system implementation.

Configuration Management - A collection of activities focused on establishing and maintaining the Integrity of information technology products and Information Systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Contingency Plan - Management policy and Procedures used to guide an institution's response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the institutional Risk managers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or disaster recovery plan (DRP) for major disruptions.

Continuity of Operations Plan (COOP) - See Business Continuity Plan.

Credentials – A combination of Identifiers and Authenticators used to authenticate.

Custodian - See Information Custodian.

Cryptographic - Relating to the discipline that embodies the principles, means, and methods for the transformation of Data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.

Cryptographic Module - Any combination of hardware, Firmware, or software that implements Cryptographic functions such as Encryption, Decryption, Digital Signatures, Authentication techniques, and random number generation.

Cryptographic Module Authentication - The set of hardware, software, Firmware, or some combination thereof that implements Cryptographic logic or processes, including Cryptographic algorithms, and is contained within the cryptographic boundary of the module.

Data - Information in a specific representation, usually as a sequence of symbols that have meaning.

Decryption - The process of changing ciphertext into plaintext using a Cryptographic algorithm and key.

Device - Any hardware component involved with the processing, storage, or forwarding of information making use of the institutional information technology infrastructure or attached to the Institutional Network. These Devices include but are not limited to, laptop computers, desktop computers, Servers, and Network Devices such as routers, switches, wireless access points, and printers.

Device Administrator - An individual with principal responsibility for the installation, configuration, registration, security, and ongoing maintenance of a Network-connected Device.

Device Owner - The department head charged with overall responsibility for the Networking component in the institution's inventory records. The Device Owner must designate an individual to serve as the primary Device Administrator and may designate a backup Device Administrator. All Network Infrastructure Devices, (e.g., Network cabling, routers, switches, wireless access points, and in general, any non-endpoint Device) shall be centrally owned and administered.

Digital Signature - The result of a Cryptographic transformation of Data which, when properly implemented, provides the services of:

- Origin Authentication
- Data Integrity
- Signer non-repudiation.

DIR CC – The security control catalog (CC) authored by the Texas Department of Information Resources (DIR) which provides state agencies and higher education institutions specific guidance for implementing security controls in a format that easily aligns with the National Institute of Standards and Technology Special Publication 800-53 Version 4 (NIST SP 800-53 Rev. 4).

Disaster Recovery Plan (DRP) - A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

Encryption - The conversion of plaintext information into a code or ciphertext using a variable called a "key" and processing those items through a fixed algorithm to create the Encrypted text that conceals the Data's original meaning.

Event - Any observable occurrence in a system or network. (E.g., A user connecting to a file share. A server receiving a request for a web page. A user sending email. A firewall blocking a connection attempt).

Execution Domain - Each Information System process has a distinct address space so that communication between processes is performed in a manner controlled through the security functions, and one process cannot modify the executing code of another process.

External Information System Service - An Information System service that is implemented outside of the Authorization Boundary of the institutional Information System (i.e., a service that is used by, but not a part of, the institutional Information System) and for which the institution typically has no direct control over the application of required security controls or the assessment of security control effectiveness. Examples include but are not limited to externally hosted or cloud-based Information Systems.

External Network - A Network not controlled by the institution.

External Service Providers – See Third-Party Providers.

Federal Information Processing Standards (FIPS) - A Standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topics in information technology in order to achieve a common level of quality or some level of interoperability.

Firewall - An inter-Network connection Device that restricts Data communication traffic between two connected Networks. A Firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance), which forwards or rejects/drops packets on a Network. Typically, Firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.

Firmware - Computer programs and Data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and Data cannot be dynamically written or modified during execution of the programs.

Guideline - Guidelines provide guidance for achieving additional positive outcomes. Guidelines are not compulsory unless explicitly stated, but they should still be followed when practicable. Guidelines can also be used as prescriptive or informational documents.

Guest Access (wireless) – Wireless services provided for visitors to Lamar University that do not have a university-supplied, centrally managed, unique electronic identifier. Such access is typically given only for short durations, such as 24 hours, and is limited in both bandwidth and allowed services upon the collection of minimal identifiable information, such as names, telephone numbers and email addresses, etc.

Identification - The process of discovering the true Identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

Identifier - Unique Data used to represent a person's Identity and associated Attributes. A name or a card number are examples of Identifiers. Note: This also encompasses non-person entities.

Identity - The set of Attributes by which an entity is recognizable and that, within the scope of an Identity manager's responsibility, is sufficient to distinguish that entity from any other entity.

Incident – See Security Incident.

Incident Response - The mitigation of violations of security policies and Best Practices.

Information Custodian - A department, agency, or Third-Party Provider responsible for implementing the Information Owner-defined controls and Access to an Information Resource.

Information Owner - A person(s) with statutory or operational authority for specified information or Information Resources.

Information Processing Facility - Facilities containing concentrations of information resources. Examples include data centers, networking closets. Sometimes referred to as "Location" for risk management purposes.

Information Resource Employee - Agency employees performing administrative, security, governance, or compliance activities on information technology systems. These types of employees generally have an occupational Category of "Information Technology" per the Texas State Auditor's Office or similar duties.

Information Resources - The Procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors. Information Resources include but are not limited to:

- All physical and logical components wired or wireless, of the Lamar University information network.
- Any Device that connects to or communicates electronically via Lamar University's network, including computers, printers, and communication Devices, both portable and fixed.
- Any fixed or portable storage Device or media, regardless of ownership, that contains Lamar University data.
- All Data created, collected, recorded, processed, stored, retrieved, displayed, or transmitted using Devices connected to Lamar University's network.
- All computer software and services licensed by Lamar University.
- Support staff and services employed or contracted by Lamar University to deploy, administer, or operate the above-described resources or to assist the community in effectively using these resources.
- Devices, software, or services that support the operations of Lamar University, regardless of physical location (e.g., SAAS, PAAS, IAAS, cloud services).
- Telephones, audio and video conferencing systems, phone lines, and communications systems provided by Lamar University.

Information Resources Management (IRM) - The planning, budgeting, organizing, directing, training, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by institutions.

Information Security - The protection of information and Information Systems from Unauthorized Access, use, disclosure, disruption, modification, or destruction in order to provide Confidentiality, Integrity, and Availability.

Information Security Officer (ISO) - The individual designated by the institution head who has the explicit authority and the duty to administer Information Security requirements institution-wide.

Information System - An interconnected set of Information Resources that share common functionality. An Information System normally includes, but is not limited to, hardware, software, Network Infrastructure, information, applications, communications, and people.

Information System Entry and Exit Points - These include but are not limited to Firewalls, electronic mail Servers, web Servers, proxy Servers, Remote Access Servers, workstations, notebook computers, and mobile Devices.

Information System Components - All components of an Information System to be authorized for operation by an Authorizing Official and excludes separately authorized systems, to which the Information System is connected.

Information System Owner - See Information Custodian.

IT Resource Project - An initiative that provides information resources technologies and creates products, services, or results within or among elements of a state agency; and is characterized by well-defined parameters, specific objectives, common benefits, planned activities, a scheduled completion date, and an established budget with a specified source of funding.

Information Management and Decision Support (IMDS) - Division with primary responsibility for the administration and operation of information resources for Lamar University.

Institutional Elements - Organizations, departments, facilities, or personnel responsible for a particular system's process.

Institutional Network - the Data transport and communications infrastructure at the institution. It includes the campus backbone, local area networks, and all equipment connected to those Networks (independent of ownership).

Integrity - The security objective of guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

Interconnection Security Agreement - A document that regulates security-relevant aspects of an intended connection between an agency and an external system. It regulates the security interface between any two systems operating under two different distinct authorities. It includes a variety of descriptive, technical, procedural, and planning information. It is usually preceded by a formal MOA/MOU that defines high-level roles and responsibilities in the management of a cross-domain connection.

Internet - The single, interconnected, worldwide system of commercial, governmental, educational, and other computer Networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB) and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

Intranet - A computer Network, especially one based on Internet technology, that the institution uses for its own internal (and usually private) purposes and that is closed to outsiders.

Least Privilege - The principle that a security architecture should be designed so that each entity is granted the minimum system resources and Authorization that the entity needs to perform its function.

LUnet - The Lamar University network on which all data traverses regardless of medium.

Maintenance Tools - Maintenance tools can include hardware, software, and Firmware items. Maintenance tools are potential vehicles for transporting malicious code into a facility either intentionally or unintentionally and subsequently into other information systems.

Malicious Code - Rogue computer programs designed to inflict a magnitude of harm by diminishing the Confidentiality, Integrity, and Availability of Information Systems and information.

Malware - Software or Firmware intended to perform an unauthorized process that will have an adverse impact on the Confidentiality, Integrity, or Availability of an Information System. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of Malware.

Management Controls - The security controls (i.e., safeguards or countermeasures) for an Information System that focus on Risk Management and the management of Information System security.

Managed Interfaces - An interface within an Information System that provides boundary protection capability using automated mechanisms or Devices.

Metrics - Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related Data.

Mission Critical - Information Resources defined by the owner or by the institution to be crucial to the continued performance of the mission. Unavailability of such Information Resources would result in more than an inconvenience. An event causing the unavailability of Mission Critical Information Resources would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations.

Mitigate – See Risk Mitigation.

Mobile Devices – A portable computing device that:

- has a small form factor such that it can easily be carried by a single individual.
- is designed to operate without a physical connection (e.g., wirelessly transmit or receive information).
- possesses local, non-removable data storage
- is powered-on for extended periods of time with a self-contained power source.

Mobile devices may also include voice communication capabilities, onboard sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smartphones, tablets, and E-readers. Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device.

Modern Enterprise Security Standards (wireless) - Wireless transport layer security methods and enterprise-level authentication methods that utilize an Identifier for each individual connecting to the network, such as a username and password or user security certificates, such as 802.1x PEAP and 802.1x EAP-TLS.

Network - Information System(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control Devices.

Network Address - A unique number associated with a Device's Network connection used for the routing of traffic across the Internet or another Network. Also known as Internet Protocol Address or IP Address.

Network Infrastructure - The hardware and software resources of an entire Network that enable Network connectivity, communication, operations, and management of an enterprise Network. It provides the communication path and services between Users, processes, applications, services, and External Networks/the Internet. These include but are not limited to cabling, routers, switches, hubs, Firewall appliances, wireless access points, virtual private network (VPN) Servers, network address translators (NAT), proxy Servers, and dial-up Servers.

NIST - National Institute of Standards and Technology.

Node - A Device or object connected to a Network.

Non-organizational User - A User who is not an institutional User (including public Users).

Non-local Maintenance – Maintenance activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network.

Non-portable System Media – An information system component that cannot be inserted into or removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data).

Organizational Identifier - An identifier formatted following special conventions to support uniqueness within an organization that is issued by the organization. For example, Lamar Electronic Account (LEA), Lamar Email, Lamar ID.

Organizational Users - An institutional User that the institution deems to have an affiliation including, for example, faculty, staff, student, contractor, guest researcher, or individual detailed from another organization.

Password - A type of Authenticator comprised of a string of characters (letters, numbers, and other symbols) used to authenticate an Identity or to verify Authorization.

Penetration Testing - A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system.

Personally Identifiable Information (PII) - A category of personal Identity information as defined by §521.002(a)(1), Business and Commerce Code.

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

Policy - A course or principle of action adopted by an enterprise to ensure its affairs are conducted prudently and appropriately. (It is a common error to confuse policies with definitions of Procedures. Procedures are important but should not be defined as, or within, policy documents).

Portable System Media – An information system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data).

Private Key - A Cryptographic key, used with a Cryptographic algorithm, that is uniquely associated with an entity and is not made public.

Privileged Account - An Information System account with approved Authorizations of a Privileged User.

Privileged Account (Very High) – An Information System account with approved Authorizations of the highest Privileged User. These accounts can operate on other privileged accounts. For Example, Root, Domain Admin, Schemer Admin, Oracle, Super Admin.

Privileged Activities – Activities performed by a Privileged User.

Privileged User - A User that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary Users are not authorized to perform.

Procedure - An operational-level document that details actions needed to implement a security control, configure a solution, or complete a task. Some Procedures may be compulsory, and other Procedures may just be one way of doing something. Procedures specify “how” things need to be done.

Protected Health Information (PHI) - Individually identifiable health information about an individual, including demographic information, which relates to the individual's past, present, or future physical or mental health condition, provision of health care, or payment for the provision of health care.

Public Key - A cryptographic key used with a cryptographic algorithm that is uniquely associated with an entity and that may be made public.

Public Key Certificate - A digital representation of information which at least:

- Identifies the Certification Authority issuing it.
- Names or identifies its subscriber.
- Contains the subscriber's Public Key
- Identifies its operational period
- Is digitally signed by the Certification Authority issuing it.

Reconstitution - Returning Information Systems to fully operational state.

Recovery Point Objective (RPO) - The point in time to which Data must be recovered after an outage.

Recovery Time Objective (RTO) - The overall length of time an Information System's components can be in the recovery phase before negatively impacting the institution's mission or mission/business processes.

Remediate – The act of mitigating a Vulnerability or a Threat.

Remote Access - Access to an institutional Information System by a User (or an Information System) communicating through an External Network (e.g., the Internet).

Research Project - Systematic investigation into and study of materials and sources to establish facts and reach new solutions which could result in the creation of an information resource project.

Residual Risk - Portion of Risk remaining after security measures have been applied.

Risk - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

- The adverse impacts that would arise if the circumstance or event occurs.
- The likelihood of occurrence.

Risk Assessment - The process of identifying Risks to institutional operations (including mission, functions, image, reputation), institutional assets, individuals, other institutions, resulting from the operation of a system. Part of Risk Management incorporates threat and Vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with Risk analysis.

Risk Management - The total process of identifying, controlling, and eliminating, or minimizing uncertain events that may adversely affect system resources. It includes Risk analysis, cost-benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

Risk Mitigation - Prioritizing, evaluating, and implementing the appropriate risk-reducing controls or countermeasures recommended from the risk management process.

Risk Tolerance - The degree of Risk or uncertainty that is acceptable to an institution.

Role-Based Access Control (RBAC) - Access Control based on User roles (i.e., a collection of Authorizations a User receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an institution. A given role may apply to a single individual or to several individuals.

Security Assessment - The testing and/or evaluation of the management, operational, and technical security controls in an Information System to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Security Control Assessments - See Security Assessment.

Security Categorization - The characterization of information or an Information System as high, moderate, or low based on an assessment of the potential impact that a loss of Confidentiality, Integrity, or Availability of such information or Information System would have on institutional operations, institutional assets, or individuals.

Security Classification - The categorization of information based on its need for Confidentiality, as determined by federal, state, local laws, policies or regulations.

Security Functions - The hardware, software, configuration, or Firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

Security Incident - A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Sensitive Personal Information (SPI) - A category of personal Identity information as defined by §521.002(a)(2), Texas Business and Commerce Code.

Separation of Duty - A security principle that divides critical functions among different staff members in an attempt to ensure that no one individual has enough information or Access privilege to perpetuate damaging fraud.

Server - A physical or virtual Device that performs a specific service or function on behalf of other Network Devices or Users.

Server Administrator - A type of Information Custodian designated by the Server Owner as responsible for performing Server Management functions.

Server Management - Functions associated with the oversight of Server operations. These include controlling User Access, establishing/maintaining security measures, monitoring Server configuration and performance, and Risk Assessment and mitigation.

Server Owner - An institution employee charged with overall responsibility for the Server asset in the university's inventory records.

Standard - A tactical-level, compulsory requirement to use the same technology, method, security control, baseline, or course of action to uniformly achieve the goals set by policies. Standards specify "what" needs to be done.

Security Awareness Steering Committee - An advisory committee comprised of faculty and staff, chaired by the security awareness officer responsible for providing guidance and ensuring the long-term success of the security awareness program.

Suspected Data Breach - Any incident in which sensitive, confidential, or otherwise protected Data in human or machine-readable form is put at Risk because of exposure to unauthorized individuals.

System Development Life Cycle (SDLC) - The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal.

System-Level Information - Information that includes but is not limited to, system-state information, operating system and application software, and licenses.

System Security Plan (SSP) - Formal document that provides an overview of the security requirements for an Information System and describes the security controls in place or planned for meeting those requirements.

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals by the unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Third-Party Providers - Service providers, staffing, integrators, vendors, telecommunications, and infrastructure support that are external to the institution.

Unauthorized Access - A person gains logical or physical Access without permission to institutional Information Resources.

University Affiliates – See Organizational User.

User - An individual, process, or automated application authorized to access an Information Resource in accordance with federal and state law, institution policy, and the Information Owner's Procedures and rules.

User Level Information - Any information other than System-Level Information.

Vulnerability - Weakness in an Information System, system security Procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment - Systematic examination of an Information System or product to determine the adequacy of security measures, identify security deficiencies, provide Data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

III. RELATED DOCUMENTS

A. Texas Administrative Code 202.1, Subchapter A
B. TSUS Information Technology Glossary
C. NIST Glossary Terms and Definitions

IV. REVISION AND RESPONSIBILITY

Oversight Responsibility: Information Technology

Review Schedule: Every three years

Last Review Date: 02/24/2022

Next Review Date: 02/24/2025

REVISION LOG

Revision Number	Approved Date	Description of Changes
6.0	2/24/2022	New and Updated Definitions