APPENDIX B
GLOSSARY

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: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., data centers, physical plant, mechanical rooms, Network closets, secured buildings, and research laboratories).

Accessible - Describes an electronic and information resource that can be used in a variety of ways and (the use of which) does not depend on a single sense or ability.

Account - A mechanism relating to identity that provides access to an information system or network.

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 Access - Privileged access that bypasses user-level controls in order to manage the information system.

Administrative Privileges - Rights granted to a Privileged User.

Alternate Formats - Alternate formats usable by people with disabilities may include, but are not limited to, Braille, ASCII text, large print, recorded audio, and electronic formats that comply with this chapter.

Alternate Methods - Different means of providing information, including product documentation, to people with disabilities. Alternate methods may include, but are not limited to, voice, fax, relay service, TTY, Internet posting, captioning, text to-speech synthesis, and audio description.

Archived Web Content - Web content that (1) was created before the date the public entity is required to comply with Title II of the Americans with Disabilities Act as published on 4/24/2024, reproduces paper documents created before the date the public entity is required to comply with Title II of the Americans with Disabilities Act as published on 4/24/2024, or reproduces the contents of other physical media created before the date the public entity is required to comply with Title II of the Americans with Disabilities Act as published on 4/24/2024; (2) is retained exclusively for reference, research, or recordkeeping; (3) is not altered or updated after the date

of archiving; and (4) is organized and stored in a dedicated area or areas clearly identified as being archived.

Assistive Technology - Any item, piece of equipment, or system, whether acquired commercially, modified, or customized, that is commonly used to increase, maintain, or improve functional capabilities of individuals with disabilities.

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 which 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 logons, 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 (e.g., User Password or token).

Authorization - The right or a 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) – See “Information Owner”.

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

Backup - A copy of files and programs made to facilitate recovery, if necessary.

Baseline Configuration - A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures

Best Practice - See Guideline.

Boundary Protection Device - A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.

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.

Business Function - 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.

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.

Cloud Computing - 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. For the purpose of this Policy, Cloud Computing encompasses any computing, software services, hosting environment, or storage environment that is not directly owned and controlled by LIT.

Cloud Service Provider - A vendor that offers Cloud Services.

Cloud Services - Services utilizing Cloud Computing technologies that are available via the Internet and are managed by third parties. Examples of Cloud Services include, but are not limited to, Internet-based web applications, software, commercial email and other messaging, document storage, and cloud platforms and infrastructure.

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.

Common Control - A security control that is inherited by one or more information systems.

Compensating Security Controls - The security controls employed in lieu of the recommended controls that provide equivalent or comparable protection.

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

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.

Configuration Settings - The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.

Content - The information and services delivered through a Web page or website.

Content Owner - A person who owns the responsibility for a website or web page, including the accuracy, timeliness, and appropriateness of all material and services resident at that website or web page.

Contingency Plan - Management policy and Procedures used to guide an institution 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.

Control - A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. A control may be technical or administrative in nature.

Control Assessment - See Security Assessment.

Conventional Electronic Documents - Web content or content in mobile apps that is in the following electronic file formats: portable document formats (PDF), word processor file formats, presentation file formats, and spreadsheet file formats.

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.

Custodian - See Information Custodian.

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.

Destruction - The result of actions taken to ensure that media cannot be reused as originally intended and that information is technologically infeasible to recover or prohibitively expensive.

Developer - A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; and (iv) product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.

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 Media - A form of electronic media where data are stored in digital (as opposed to analog) form.

Digital Signature - The result of a Cryptographic transformation of Data which, when properly implemented, provides the services of: 1. origin Authentication, 2. Data Integrity, and 3. 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 in response to a major hardware or software failure or destruction of facilities.

Domain - An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

Electronic and Information Resources (EIR) - Includes information technology and any equipment or interconnected system or subsystem of equipment used to create, convert, duplicate, or deliver data or information. EIR includes telecommunications products (such as telephones), information kiosks and transaction machines, web sites, multimedia, and office equipment such as copiers and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, thermostats or temperature control devices, and medical equipment that contain information technology that is integral to its operation, are not information technology. If the embedded information technology has an externally available web or computer interface, that interface is considered EIR. Other terms such as, but not limited to, Information and Communications Technology (ICT), Electronic Information Technology (EIT), etc. can be considered interchangeable terms with EIR for purposes of applicability or compliance.

Electronic and Information Resources (EIR) Owner - The individual responsible for a business function who determines controls for and oversees the development, acquisition, and/or use of EIR supporting that business function.

Encryption - The conversion of plaintext information into a code or cipher text 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.

Enterprise Architecture - A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.

Event - Any observable occurrence in an information system.

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 Information System Service - An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service

that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External Network - A Network not controlled by the institution.

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 topic 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.

Hardware - The physical components of an information system.

Home Page - The initial page that serves as the front door or entry point to a state website.

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.

Impact - The effect on organizational operations, organizational assets, individuals, or other organizations of a loss of confidentiality, integrity, or availability of information or an information system.

Incident - See Security Incident.

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

Information - Data as processed, stored, or transmitted by a computer.

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 and with responsibilities assigned in TSUS and component institution policy.

- Information owners are responsible for ensuring the implementation of security controls required by component institution policies and standards.
- In consultation with the component institution's ISO and IRM, information owners may also prescribe and implement additional controls or overlays specific to the information or Information Resource(s) for which they have statutory or operational authority.

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 Institutional Network;
- any Device that connects to or communicates electronically via the Institutional Network, including computers, printers, and communication Devices, both portable and fixed;
- any fixed or portable storage Device or media, regardless of ownership, that contains institution Data;
- all Data created, collected, recorded, processed, stored, retrieved, displayed, or transmitted using Devices connected to the Institutional Network;
- all computer software and services licensed by the institution;
- support staff and services employed or contracted by the institution 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 the institution, regardless of physical location (e.g.; SAAS, PAAS, IAAS, cloud services); and
- telephones, audio and video conferencing systems, phone lines, and communications systems provided by the institution.

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

Information Resources Manager (IRM) - A designated employee authorized to manage the Institute's information resources and charged with assuming the responsibilities identified in Texas Government Code §2054 Subchapter D.

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 Security Program - The policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish an information resources security function within an institution of higher education or state agency.

Information Security Risk - The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.

Information Spill(age) - Security event that results in the transfer of information onto an information system not authorized to store or process that information or information of the spilled information’s Security Classification.

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

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 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 Owner - See Information Owner.

Information System Service - A capability provided by an information system that facilitates information processing, storage, or transmission.

Information Technology - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information. The term includes computers (including desktop and laptop computers), ancillary equipment, desktop software, client-server software, mainframe software, web application software and other types of software, firmware and similar procedures, services (including support services) and related resources.

Institute Home Page - The web page that displays when www.lamarpa.edu is the URL.

Institute Websites - Websites and web pages owned or controlled by Lamar Institute of Technology that represent the college.

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.

Intellectual Property - Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract properties has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered.

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 management of a cross-domain connection.

Internal Network - A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.

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.

ISO - See “Information Security Officer”.

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

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 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.

Media - Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Metadata - Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).

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.

Mobile App - See **Mobile Application**.

Mobile Application - A software application that is downloaded and designed to run on mobile devices such as smartphones and tablets.

Mobile Device - 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); and is powered on for extended periods of time with a self-contained power source. Mobile Devices may also include voice communication capabilities, on-board 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 laptops, smart phones, tablets, smart watches, and e-readers.

Multifactor Authentication - Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See Authenticator.

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.

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

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

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 Milestones - 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.

Portable Storage Device - An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

Potential Impact - The loss of confidentiality, integrity, or availability that could be expected to have: (i) a limited adverse effect (low); (ii) a serious adverse effect (moderate); or (iii) a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals.

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 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 Information - A category of information as defined by Texas Government Code §552.002.

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 (1) identifies the Certification Authority issuing it, (2) names or identifies its subscriber, (3) contains the

subscriber's Public Key, (4) identifies its operational period, and (5) is digitally signed by the Certification Authority issuing it.

Reconstitution - Returning Information Systems to fully operational states.

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.

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

Removable Media - Portable data storage medium that can be added to or removed from a computing device or network. Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external / removable hard drives; external / removable Solid State Disk (SSD) drives; magnetic / optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external / removable disks (floppy, Zip, Jaz, Bernoulli, UMD).

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: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) 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, it 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/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.

Sanitization - Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.

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 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 Category - See “Security Categorization”.

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

Security Control - A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Security Control Assessments - See Security Assessment.

Security Incident - An event which results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources.

Security Plan - Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See System Security Plan or Information Security Program Plan.

Self-Contained, Closed Products - Products that generally have embedded software and are commonly designed in such a fashion that a user cannot easily attach or install assistive technology. These products include, but are not limited to, information kiosks and information transaction machines, copiers, printers, calculators, fax machines, and other similar products.

Sensitive Information - Information that may be subject to release under the Texas Public Information Act but should be controlled to protect third parties. This includes data that meets the definition of Personally Identifiable information under the Texas Business and Commerce Code §521.002(a)(1) and §521.002(a)(2), such as employee records and gross salary information. Other examples include but are not limited to emails, voicemails, instant messages, internal

communications, and departmental procedures that might reveal otherwise protected information.

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 perpetrate 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 college's inventory records.

Site Policies Page - A web page containing website policies or a link to each policy.

Software - Computer programs and associated data that may be dynamically written or modified during execution.

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.

Suspected Data Breach - Is 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 Administrator - Individual responsible for the installation and maintenance of an information system, providing effective information system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.

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.

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

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals.

TRAIL - Texas Records and Information Locator, or its successor, providing a method to do a statewide search.

Transaction Risk Assessment - An evaluation of the security and privacy required for an interactive web session providing public access to government information and services.

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

Unauthorized Disclosure - An event involving the exposure of information to entities not authorized access to the information.

Uninterruptable Power Supply (UPS) - A device with an internal battery that allows connected devices to run for at least a short time when the primary power source is lost.

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 Agent - Any software that retrieves and presents web content for users.

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

Voluntary Product Accessibility Template (VPAT) - A vendor-supplied form for a commercial Electronic and Information Resource used to document its compliance with technical accessibility standards and specifications.

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.

Web Content - The information and sensory experience to be communicated to the user by means of a user agent, including code or markup that defines the content’s structure, presentation, and interaction. Examples of web content include text, images, sounds, videos, controls, animations, and conventional electronic documents.

Web Page - Presentation of state website content, including documents and files containing text, graphics, sounds, video, or other content, that is accessed through a web browser.

Web Presence - A representation of Lamar Institute of Technology in text, graphics, audio, video, and any other forms of communication on the Web.

Website - A set of related web pages that are prepared and maintained as a collection in support of a single purpose.