CONE HEALTH	**Guideline:** ITS Information Security Terms and Definitions	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 06/07/2024
	Effective Date: 06/07/2024	**Next Review Date:** 06/07/2025

INTENDED AUDIENCE:
Entire workforce

PROCEDURE:
In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), Cone Health is committed to ensuring the confidentiality, integrity, and availability of protected health information (PHI/ePHI), sensitive, and confidential data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.
The purpose of this procedure is to define the different terms and their definitions used in information security policies and procedures.

Scope and Goals:
The scope of this procedure is to define terms used within the organization's information security policies and procedures. Goals of this procedure are, but are not limited to, the following:

- Clarify the use and understanding of terminology used in information security policies/procedures.
- Create a common lexicon for the organization's information security program.
- Eliminate confusion associated with similar terms used in other areas of the organization.

Responsibility:
Chief Information Security Officer (CISO)
The CISO is responsible for maintaining this glossary as a resource for the workforce when reading information security policies and procedures.

Terms and Definitions:
The following terms are used within Cone Health's information security policies and procedures. These terms are provided with their definitions to assist readers of the organization's policies/procedures for a clear understanding intent for each policy/procedure.

Access: The ability of an entity (typically a user or process) to connect to a resource (e.g. Website, database, shared folder, application, or some other network resource). Access can be in the form of reading, writing or deleting information.

Access control: The method and/or technology used to manage workforce access to covered information, to only those who have been properly authorized in accordance with the applicable policy. Authorization will be based on need-to-know and minimum necessary to perform assigned job responsibilities.

Access control lists (ACLs): A register of:

- Users (including groups, machines, processes) who have been given permission to use a particular system resource, and
- The types of access they have been permitted.

Accountability: The security goal that generates the requirement for actions of an entity to be uniquely traced. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery, and legal action.

Accountable asset: Any asset containing covered information or requiring accountability in accordance with other organizational policy.

Accreditation (Authorization to Operate): The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations, based on the implementation of an agreed-upon set of security controls.

Accreditation (authorization) boundary: All components of an information system to be approved for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Administrative controls: Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information.

Advanced encryption standard (AES): The advanced encryption standard specifies a U.S. government-approved cryptographic algorithm that can be used to protect electronic data.

Annual training: Mandatory training for all organization workforce members. Receipt of this training must be documented and accepted by signature from the person receiving the training. Annual training typically focuses on organizational policies and procedures along with lessons learned from the previous year.

Application: A software program hosted by an information system that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

Approval to Operate (ATO): A formal declaration by a designated approving authority (DAA) that authorizes operation of an information system in a production environment that explicitly accepts the risk to organization operations (including business mission, functions, image, or reputation, patient safety, etc.), assets, or individuals, based on the implementation of an agreed-upon set of information security controls.

Guideline: ITS Information Security Terms and Definitions

Asset: A general term used to define a system, application, physical facility, or attribute, personnel, computer, network equipment, media, or portable device.

Asset management: The process of actively accounting for and managing assets throughout their lifecycle in the organization. This includes but is not limited to tracking by type, cost, ownership, business criticality, security criticality (i.e., stores electronic covered information), etc.

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, and to recommend necessary changes in controls, policies, or procedures.

Audit controls: Technical mechanisms that track and record computer/system activities.

Audit logs: Records of activity maintained by the system which provide 1) date and time of significant activity; 2) origin of significant activity; 3) identification of user performing significant activity; and 4) description of attempted or completed significant activity. Audit logs also provide a means to monitor information operations to determine if a security violation has or is occurring by providing a chronological series of logged computer events that relate to an operating system, an application, database, network directory, or user activities. Audit logs provide:

- Individual accountability for activities such as an unauthorized access of covered data;
- Reconstruction of an unusual occurrence of events such as an intrusion into the system to alter information; and
- Problem analysis such as an investigation into a slowdown of a system's performance.
- An audit log identifies who (login) did what (create, read, modify, delete, add, etc.) to what (data) and when (date, time).

Audit trail: A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result

Authenticate: To confirm the identity of an entity when presented.

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Availability: Ensuring timely and reliable access to and use of information.

Background check: The act of reviewing both confidential and public information to investigate a person or entity's history. Background checks are commonly performed by employers to ensure that (1) an employee is who he or she says they are, (2) to determine that the individual does not have a damaging history (such as criminal activity) that may reflect poorly on the company, (3) to confirm information that an applicant included on their application for employment.

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

Banner: Display on an information system that sets parameters for system or data use.

Baseline configuration: A set of specifications for a system, or configuration item (CI) 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. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Breach: The unauthorized acquisition, use, or disclosure of covered information which includes the security or privacy of covered information.

Business associate (BA): A person (or entity) who is not a member of the organization's workforce and who performs any function or activity involving the use or disclosure of individually identifiable health information or who provides services to the organization that involves the disclosure of individually identifiable health information, such as legal, accounting, consulting, data aggregation, management, accreditation, etc. This would also include third party services that could come into contact with covered data under reasonable circumstances during the performance of their responsibilities. Examples of these services include but are not limited to outsourced information technology services, paper and device disposal services, leasing companies who take responsibility for sanitizing business machines that were used copying, faxing, and storing covered data, etc.

Business associate agreement (BAA): A legally binding agreement entered into by a covered entity and business associate that establishes permitted requirements defined in policy, in addition to required uses and disclosures of protected health information (PHI), provides obligations for the business associate to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is a material violation. This agreement can take the form of a service level agreement or contract for services, provided the provisions of the organization's policies and procedures are met.

Business continuity: Encompasses a loosely defined set of planning, preparatory, and related activities which are intended to ensure that an organization's critical business functions will either continue to operate despite serious incidents or disasters that might otherwise have interrupted them, or will be recovered to an operational state within a reasonably short period.

Business continuity plan (BCP): The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business functions will be sustained during and after a significant disruption.

Business impact analysis (BIA): An analysis of an enterprise's requirements, processes, and interdependencies used to characterize information system contingency requirements and priorities in the event of a significant disruption.

Certification: A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, 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.

Change Advisory Board (CAB): A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system.

Change management: An ITS service management discipline. The objective of change management in this context is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to control ITS infrastructure, in order to minimize the number and impact of any related incidents upon service. Changes in the ITS infrastructure may arise reactively in response to problems or externally imposed requirements (e.g., legislative changes) or proactively from seeking improved efficiency and effectiveness or to enable or reflect business initiatives, or from programs, projects or service improvement initiatives. Change management can ensure standardized methods, processes, and procedures which are used for all changes, facilitate efficient and prompt handling of all changes, and maintain the proper balance between the need for change and the potential detrimental impact of changes. The goals of a change control procedure usually include minimal disruption to services, reduction in back-out activities, and cost-effective utilization of resources involved in implementing change.

Compensating controls: Safeguards or countermeasures used to mitigate the severity or impact of a vulnerability (i.e., risk) to covered information. Compensating controls can be technical or non-technical in nature.

Compliance assessment/evaluation: Evaluating information security compliance with laws, regulations, and ethical standards, and assessing the effectiveness of the information security program in achieving its objectives.

Configuration control: Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation.

Configuration items (CI): An aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process.

Continuous monitoring: The process and technology used to detect compliance and risk issues associated with an organization's environment. The environment consists of people, processes, and systems working together to support efficient and effective operations. Through continuous monitoring of the operations and controls, weak or poorly designed or implemented controls can be corrected or replaced, thus enhancing the organization’s operational risk profile.

Covered information: General term used to define all data requiring specific administrative, physical, technical, and operational controls to ensure the confidentiality, integrity, and availability of information in accordance with regulatory requirements and corporate governance. At a minimum, this would include all confidential and sensitive data. Protected health information/electronic protected health information is also considered covered information but could have additional unique requirements/controls, depending on the situation.

Degauss: Using a magnetic field to erase (neutralize) the data bits stored on magnetic media.

Designated approving authority (DAA): Authorizing official (i.e., CEO) within the organization, or his/her designated representative who has been formally given the authority to assume responsibility for accepting risk on behalf of the organization. The DAA grants or denies authority to accept risk based on his or her knowledge of the needs of the business, and the recommendations of the information security officer.

Destruction: The act of completely destroying media or equipment beyond any possibility of data recovery.

Disaster: In general, defined as any damaging or destructive event that overwhelms available resources, causes serious loss, destruction, hardship, unhappiness, or death. For ITS environments, a disaster is thought of as any event that creates an inability on an organizations part to provide critical business functions for some extended period of time. It may entail the loss of data and processing capability.

Disaster recovery: An extension of business continuity, which addresses recovery after a disaster that destroys or otherwise disables a system(s) or disrupts ITS operations. Disaster recovery techniques typically involve restoring data to a second (recovery) system, then using the recovery system in place of the destroyed or disabled application system. Disaster recovery could also mean relocating to an alternate operating location. Disaster recovery planning is the responsibility of the ITS department.

Disaster recovery plan: A written plan for recovering one or more information system (or relocation to an alternate facility) or other supporting function (i.e., commercial data lines, environmental controls, etc.) in response to a network, system, application, hardware or software failure, destruction of facility, or other disaster that disrupts or disables ITS operations.

Disclosure: Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Electronic computing device: A device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit ePHI. Electronic computing devices may include, but are not limited to, laptop or desktop computers, personal digital assistants (PDAs), tablet PCs, iPads, smartphones, etc. For the purposes of this procedure, “electronic computing device” also includes the combination of hardware, operating system, application software, and network connection.

Electronic media: Media which has the ability to store any amount of electronic data on it for future recovery and use. Examples include but are not limited to, flash/thumb drives, CD-ROMs, DVDs, magnetic tapes, DAT drives, hard drives (portable or fixed), memory sticks, etc.

Electronic protected health information (ePHI): Any individually identifiable health information protected by HIPAA that is created and transmitted by or stored in electronic form.

Encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of interpreting the meaning of the data without use of a confidential process or key.

Endpoint: Term used to collectively identify processes, users, devices, etc., that access information stored within a system. Endpoints involve an identifiable user or process utilizing a device such as a computer, laptop, smart phone, tablet, medical device, or specialized equipment such as bar code readers or point of sale (POS) terminals, etc., to access internal resources and information.

Escorted access: The accompaniment while in a restricted area by an approved individual who maintains continuous direct visual surveillance at all times over an individual who is not approved for unescorted access.

Event: An event is defined as an occurrence that does not constitute a serious adverse effect on the organization or its operations, though it may be less than optimal. Examples of events include, but are not limited to:

- A hard drive malfunction that requires replacement
- Systems become unavailable due to power outage that is non-hostile in nature
- Accidental lockout of an account due to incorrectly entering a password multiple times
- Network or system instability

External access (connectivity): The ability to access data and internal resources (i.e., applications, network folders, etc.) from outside the corporate network perimeter. This usually means from across the internet and on the public side of the corporate firewall. See also the Information Access Management policy/procedure.

Firewall: A firewall is a set of related programs and/or hardware providing protection from TCP/IP attacks, probes, scans, and unauthorized access by buffering the internal network from the internet.

Guest account: An account assigned to a guest/visitor of the organization hosting a wireless network.

Incidental access: Access to covered information in connection with or resulting from something more important, casual, or fortuitous that occurs as a by-product of another form of permissible or required access.

Indication: A sign that an incident may have occurred or may be occurring at the present time. Examples of indications include:

- The network intrusion detection sensor alerts when a known exploit occurs against an FTP server. Intrusion detection is generally reactive, looking only for footprints of known attacks. It is important to note that many IDS “hits” are also false positives and are neither an event nor an incident.
- The antivirus software alerts when it detects that a host is infected with malware.
- The web server crashes.
- Users complain of slow access on the internet.
- The system administrator sees a filename with unusual characteristics.

- The user calls the help desk to report a threatening email message (and it is determined by Information Technology and Services that it is a legitimate risk issue).

Individually identifiable health information: Information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Initial awareness training: Mandatory training for all newly hired workforce members. Receipt of this training must be documented and accepted by signature from the person receiving the training. Initial training typically focuses on organizational policies and procedures. Initial training typically takes place within the first 5 days of being hired.

Insider threat: An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.

Interim Approval to Operate (IATO): Temporary authorization (i.e., no more than 90 days) to operate an information system under the conditions or constraints identified in the plan of action and milestones.

Law enforcement official: Any officer or employee of an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Least privilege: The security objective of granting users access to only what they need to perform their official duties.

Malicious code: 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 malicious code.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim.

Minimum necessary information: Protected health information that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The "minimum necessary" standard applies to all covered data in any form.

Mobile device: A portable computing device such as a smartphone, tablet, or laptop that has a display screen with touch input and/or a keyboard.

Mobile device management (MDM): Type of security software used by an ITS department to monitor, manage and secure employees' mobile devices deployed across multiple mobile service providers and across multiple mobile operating systems being used in the organization.

Multifactor authentication: Authentication using two or more factors to achieve authentication. Factors include (1) something you know (e.g., password/PIN); (2) something you have (e.g., cryptographic identification device, token); or (3) something you are (e.g., biometric).

Non-technical controls: Management and operational controls such as security policies, procedures, and standards that address personnel, physical, and environmental security risks.

Non-technical security incident: The attempted or successful unauthorized access, use, disclosure/loss/theft, modification, or destruction of information meant to interfere or compromise business operations. Examples include but are not limited to the following:

- Unauthorized disclosure, loss, or theft of covered information in paper or electronic form (e.g., thumb drive, computer, smartphone, tablet, backup tape, etc.).
- Unauthorized change or destruction of covered information (i.e., delete dictation, data alterations not in compliance with organizational policies/procedures).
- Denial of service not attributable to identifiable physical, environmental, human, or technology causes.
- Physical breach of security controls.

Patch: An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Patch management: The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Penetration test (Pentest): Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Personally identifiable information (PII): Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

Personally owned device: Any device or media owned by a workforce member that he/she uses for work-related purposes.

Plan of action and milestones (POAM): Also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished to meet the requirements of a risk acceptance decision (i.e., approval to operate). It details resources required to accomplish the elements of the plan, including any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POAM is to assist the organization with identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Portable media: Portable electronic device capable of storing and playing digital media such as audio, images, video files, and documents. The data is typically stored on a CD, DVD, flash memory, micro-drive, or hard drive.

Precursor: A sign that an incident may occur in the future. Examples of precursors include:

- Suspicious network and host-based IDS events/attacks.
- Alerts as a result of detecting malicious code at the network and host levels.
- Alerts from file integrity checking software.
- Alerts from third party monitoring services.
- Audit log alerts.

Privilege: A right granted to an individual, a program, or a process.

Privileged access controls: Includes unique user IDs and user privilege restriction mechanisms such as directory and file access permission, and role-based access control mechanisms.

Privileged user: An individual who has the ability to perform administrator level functions associated with managing user access, security functions, change application/system controls and parameters, etc. Also known as a power user or system, network, or application administrator.

Protected health information (PHI): Individually identifiable health information (i.e., paper based) that is created by or received by the organization, including demographic information that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual

Recovery point objective (RPO): The point in time to which data must be restored in order to resume processing transactions. RPO is the basis on which a data protection strategy is developed.

Recovery time objectives (RTO): The period of time within which systems, applications, or functions must be recovered after an outage (e.g., one business day). RTOs are often used as the basis for the development of recovery strategies, and as a determination as to whether or not to implement the recovery strategies during a disaster situation.

Recurring training: Ad-hoc training typically takes the form of emails, handouts, signs, etc. This training is not recorded, nor does it require a signature from those who see or read the training.

Remediation: The act or process of correcting a fault, finding, or deficiency.

Remote access: Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the internet) from a remote work site. See also the Information Access Management policy/procedure.

Remote maintenance: Maintenance activities conducted by individuals communicating through an external network (e.g., the internet).

Remote work site: A work site other than the organization's official workplace. Remote work site shall mean the employee's residence or any remote office location approved by the organization as a suitable place to work, such as public venues (e.g., airports, planes, trains, hotel room, restaurants, and coffee shops).

Repurpose: To give an asset a new purpose or reuse (i.e., reissuing a computer to a new user).

Restricted areas: Areas for which access must be limited to only those workforce members who have been properly authorized based on their need-to-know and job responsibilities. Restricted areas include areas such as the data center, telephone closets, wiring closets, asset storage/staging areas, records room, file rooms, etc.

Risk: The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of occurrence.

Risk assessment/analysis: Risk assessment and analysis are often used interchangeably. Within this procedure, the terms are used as follows:

- Risk assessment: The process of identifying and prioritizing risks to the confidentiality, integrity, and availability of covered information. Risk assessments are meant to identify risks, not analyze or remediate risks.
- Risk analysis: The analysis of risks identified during a risk assessment, determining the likelihood of occurrence and impact, then deciding what controls will be implemented to reduce the risk to an acceptable level. A thorough and accurate risk analysis will consider all relevant losses that would be expected if security measures were not in place or not performing as expected, including loss or damage of data, corrupted data systems, and anticipated ramifications of such losses or damage.

Risk management: The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, resulting from the operation or use of an information system, and includes (1) the results of a risk analysis; (2) the implementation of a risk mitigation strategy; (3) employment of techniques and procedures for the

continuous monitoring of the security state of the information system; and (4) documenting the overall risk management program.

Risk mitigation: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. The risk mitigation process includes cost-benefit analysis.

Risk monitoring: Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.

Risk tolerance: The level of risk the organization is willing to assume in order to achieve a potential desired result.

Role: The category or class of a person or persons performing a type of job, defined by a set of similar or identical responsibilities.

Role based access (RBAC): Access control based on user roles (i.e., a collection of access 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 organization. A given role may apply to a single individual or to several individuals.

Sanitization: Removal or the act of overwriting data to a point of preventing the recovery on the device or media that is being sanitized. Sanitization of a device's sensitive information is typically done before re-issuing it to another workforce member, donating, or returning any leased equipment to the lending company.

Secure baseline configuration: A set of security specifications for a system, or configuration item (CI) 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. The secure baseline configuration is used as a basis for future builds, releases, and/or changes.

Secure configuration management (SecCM): The management and control of configurations for an information system and components to enable security and facilitate the management of risk.

Security hardening: Configuring a device to make it more secure such as changing, removing or disabling default (i.e., out-of-the-box) settings, disabling unnecessary services, increasing access controls, enabling encryption, etc.

Service level agreement (SLA): An agreement between an ITS service provider and a customer. The SLA describes the ITS service, documents service level targets, and specifies the responsibilities of the ITS service provider and the customer. A single SLA may cover multiple ITS services or multiple customers.

Social engineering: An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks. Also, a general term used to describe methods used by

malicious individuals to trick others into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.

Spyware: A type of malicious code (software) that is secretly installed into an information system to gather information on individuals or organizations without their knowledge.

Storage: The means by which information is stored (when data is at rest). Examples of storage are CD-ROM, hard-drive, flash/thumb drive, database, shared folder, smartphone, hard-drive, memory stick, etc.

System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

System owner: Person, business unit, department, or organization having responsibility for the development, procurement, integration, modification, operation and maintenance (system and security), and/or final disposition of an information system.

System profile: Detailed security description of the physical structure, equipment component, location, relationships, and general operating environment of an information system.

System security plan: Formal document prepared and maintained by the system owner that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, secure baseline configurations, configuration management plan, and incident response plan.

Technical controls: The security controls that are incorporated into system hardware and software (e.g., access controls, encryption, integrity, audit controls, non-repudiation).

Technical security incident: The attempted or successful unauthorized access, use, disclosure/loss/theft, modification, or destruction of information meant to interfere or compromise business operations. Examples include but are not limited to the following:

- A system or network breach or attack by an internal or external entity (includes breaches that are inadvertent or malicious).
- Unauthorized disclosure of covered information (e.g. email, exposed on a public web server, etc.).
- Unauthorized change or destruction of covered information (i.e. deletion or alternation of data).
- Human initiated denial of service (i.e. hacker).
- Logical breach of security controls (i.e. hacker).

Teleworking/telecommuting: Working at a location other than the organization's main office (see remote work site)

Third party: Term used to describe an entity/company/organization that provides consulting, legal, real estate, education, communications, storage, processing, and many other services. Third parties can also be referred to as vendors, suppliers, service providers, and business associates. Not all third parties may have access (direct or indirect) to covered information.

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

Threat assessment: Process of formally evaluating the degree of threat to an information system, covered information, or the organization, and describing the nature of the threat.

Transmission: The means by which information is moved/transmitted from one point to another.

Trusted network: A network that is resilient to attack and that the confidentiality, integrity, and availability of the system and its data are protected. For example, the organization's internal network is considered "trusted."

Unescorted access: Approved physical access to restricted areas without the need of supervision.

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: The process of identifying technical computer/network/system security vulnerabilities, as well as weaknesses in policies and practices related to the operation of these systems.

Workforce: Employees, volunteers, trainees, consultants, contractors, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such entity, whether or not they are paid by the organization.

Unsecured covered information: Covered information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of approved technology.

Untrusted network: A network that cannot maintain or cannot be confirmed to have the ability to maintain the confidentiality, integrity and availability of information that is communicated over it (i.e., internet).

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

REFERENCE DOCUMENTS/LINKS:

National Institute of Standards and Technology (NIST) Interagency Report (IR) (NISTIR) 7298, Revision 2 - Glossary of Key Information Security Terms.