Glossary

This glossary contains words, phrases and acronyms that your will find useful in understanding your ISS program.

The terms in this glossary are taken from several sources:

ISS Industry Template package	
HIPAA	Represented by
NITC	Represented by

Term	Definition
Ability to add attributes	One possible capability of a digital signature technology, for example, the ability to add a time stamp as part of a digital signature.
Acceptable use	The acceptable practices employees incorporate into their daily activities.
Access	The ability or the means necessary to read, write, modify, or communicate data/ information or otherwise make use of any system resource.
Access authorization	Information-use policies/ procedures that establish the rules for granting and/or restricting access to a user, terminal, transaction, program, or process.
Access control	A method of restricting access to resources, allowing only privileged entities access. Types of access control include, among others, mandatory access control, discretionary access control, time-of-day, classification, and subject-object separation.
Access controls	The protection of sensitive communications transmissions over open or private networks so that it cannot be easily intercepted and interpreted by parties other than the intended recipient.
Access establishment	The security policies, and the rules established therein, that determine an entity's initial right of access to a terminal, transaction, program, or process.
Access level	A level associated with an individual who may be accessing information (for example, a clearance level) or with the information which may be accessed (for example, a classification level).
Access modification	The security policies, and the rules established therein, that determine types of, and reasons for, modification to an entity's established right of access to a terminal, transaction, program, or process.

Accountability	The property that ensures that the actions of an entity can be traced uniquely to that entity.
Administrative procedures to guard data integrity, confidentiality and availability	Documented, formal practices to manage (1) the selection and execution of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.
Agency	Any government entity, including state government, local government, or third party entities under contract to the agency.
Alarm, event reporting, and audit trail	(1) Alarm: In communication systems, any device that can sense an abnormal condition within the system and provide, either locally or remotely, a signal indicating the presence of the abnormality. (188) NOTE: The signal may be in any desired form ranging from a simple contact closure (or opening) to a time-phased automatic shutdown and restart cycle. (2) Event reporting: Network message indicating operational irregularities in physical elements of a network or a response to the occurrence of a significant task, typically the completion of a request for information. (3) Audit trail: Data collected and potentially used to facilitate a security audit.
Applications and data criticality analysis	An entity's formal assessment of the sensitivity, vulnerabilities, and security of its programs and information it receives, manipulates, stores, and/or transmits.
Assigned security responsibility	Practices put in place by management to manage and supervise (1) the execution and use of security measures to protect data, and (2) the conduct of personnel in relation to the protection of data.
Assure supervision of maintenance personnel by authorized, knowledgeable person	Documented formal procedures/instruction for the oversight of maintenance personnel when such personnel are in the vicinity of health information pertaining to an individual.
Asymmetric encryption	Encryption and decryption performed using two different keys, one of which is referred to as the public key and one of which is referred to as the private key.
Asymmetric key	One half of a key pair used in an asymmetric (``public-key'') encryption system. Asymmetric encryption systems have two important properties: (1) the key used for encryption is different from the one used for decryption (2) neither key can feasibly be derived from the other.

Audit controls	The mechanisms employed to record and examine system activity.
Authentication	The process of proofing the user is positively identified usually with a password.
Authorities	The privileges set up for employees to have access to the areas of the system they need to do their job.
Authorization	The process of setting up users with their privileges.
Authorization control	The mechanism for obtaining consent for the use and disclosure of health information.
Automatic logoff	After a pre-determined time of inactivity an electronic session is terminated.
Availability	The property of being accessible and useable upon demand by an authorized entity. Ensuring that information and services are available when required.
Awareness training for all personnel (including management)	All personnel in an organization should undergo security awareness training, including, but not limited to, password maintenance, incident reporting, and an education concerning viruses and other forms of malicious software.
Biometric	A biometric identification system identifies a human from a measurement of a physical feature or repeatable action of the individual (for example, hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature).
"Black hat"	Another name for a hacker.
"Black night"	With this method, passwords may be taped in a conspicuous spot because they have been altered using some standard approach, such as bump the first letter up the alphabet one letter, bump the second letter down one letter, etc.
Centralized Reporting	Having a central area for all suspicions and incidents to be reported.
Certification	The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external accrediting agency.

Chain of Trust Partner Agreement	Contract entered into by two business partners in which it is agreed to exchange data and that the first party will transmit information to the second party, where the data transmitted is agreed to be protected between the partners. The sender and receiver depend upon each other to maintain the integrity and confidentiality of the transmitted information. Multiple such two-party contracts may be involved in moving information from the originator to the ultimate recipient, for example, a provider may contract with a clearing house to transmit claims to the clearing house; the clearing house, in turn, may contract with another clearing house or with a payer for the further transmittal of those same claims.
Classification	Protection of data from unauthorized access by the designation of multiple levels of access authorization clearances to be required for access, dependent upon the sensitivity of the information.
Clearing House	A public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard data elements.
Combination locks changed	Documented procedure for changing combinations of locking mechanisms, both on a recurring basis and when personnel knowledgeable of combinations no longer have a need to know or a requirement for access to the protected facility/system.
Condensed format	In the template package, the abbreviated format for publishing a rule.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities or processes. Protecting the sensitive information from unauthorized disclosure or intelligible interception.
Context-based access	An access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The ``external'' factors might include time of day, location of the user, strength of user authentication, etc.
Contingency plan	A plan for responding to a system emergency. The plan includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster. Contingency plans should be updated routinely.
Continuity of signature capability	The public verification of a signature shall not compromise the ability of the signer to apply additional secure signatures at a later date.

COPPA	Children's Online Privacy Protection Act
Copyright	There are many copyright laws dealing with software and document copying that address the bootlegging and stealing of information.
Counter signatures	It shall be possible to prove the order of application of signatures. This is analogous to the normal business practice of countersignatures, where some party signs a document which has already been signed by another party.
Cracker	Like a hacker, only more deviant.
Critical Systems	Those systems or system components (hardware, data, or software) that if lost or compromised would jeopardize the ability of the system to continue processing.
Cyber Crime	Any criminal activity that uses cyberspace (the internet network) as the communication vehicle to commit the criminal act. With the exponential growth of Internet connections, the opportunities for the exploitation of any weaknesses in ISS are multiplying. Cyber crime may be internal or external. Internal is easier to penetrate. The term has evolved over the past few years since the adoption of Internet connections on a global scale with hundreds of millions of users. Legal systems around the world are scrambling to introduce laws to combat cyber crime.
Data	A sequence of symbols to which meaning may be assigned.
Data authentication	The corroboration that data has not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature.
Data backup	A retrievable, exact copy of information.
Data backup plan	A documented and routinely updated plan to create and maintain, for a specific period of time, retrievable exact copies of information.
Data integrity	The property that data has not been altered or destroyed in an unauthorized manner.
Data storage	The retention of health care information pertaining to an individual in an electronic format.
Decryption	The process by which encrypted data is restored to its original form in order to be understood / usable by another computer or persons.
Denial of Service	Abbreviated DoS, it is an internet attack against a web site whereby a client is denied the level of service expected.

DES/ AES	DES - Data Encryption Standard AES - Advanced Encryption Standard
Digital signature	An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
Disaster	Any event that threatens the destruction of information or availability of computer systems. A disaster may affect the physical security of computer systems, including equipment failures, fire, flood, other natural calamities, or theft of equipment. A disaster may involve destruction or information or availability of computer systems due to system failure, human error, or intentional acts including computer crimes.
Disaster recovery	The process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
Disaster recovery plan	Part of an overall contingency plan. The plan for a process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
Discretionary access control	Discretionary Access Control (DAC) is used to control access by restricting a subject's access to an object. It is generally used to limit a user's access to a file. In this type of access control it is the owner of the file who controls other users' accesses to the file.
Disposal	The final disposition of electronic data, and/or the hardware on which electronic data is stored.
Disclosure	Revealing information that should not be known to the receiver of the information.
Documentation	Written security plans, rules, procedures, and instructions concerning all components of an entity's security.
Downloading	Receiving files from a source to your system.
“Dumpster-diving”	Going through the trash to try to recover passwords printed on papers.
E-commerce	Doing business through the internet.
E-mail	The exchange and/ or sharing of messages, attachments, and calendar and scheduling information.
Electronic data Interchange	(EDI) Inter-company, computer-to-computer transmission of business information in a standard format. For EDI purists, ``computer-to- computer'' means direct transmission from the

	originating application program to the receiving, or processing, application program, and an EDI transmission consists only of business data, not any accompanying verbiage or free-form messages. Purists might also contend that a standard format is one that is approved by a national or international standards organization, as opposed to formats developed by industry groups or companies.
Electronic signature	The attribute that is affixed to an electronic document to bind it to a particular entity. An electronic signature process secures the user authentication (proof of claimed identity, such as by biometrics (fingerprints, retinal scans, hand written signature verification, etc.), tokens or passwords) at the time the signature is generated; creates the logical manifestation of signature (including the possibility for multiple parties to sign a document and have the order of application recognized and proven) and supplies additional information such as time stamp and signature purpose specific to that user; and ensures the integrity of the signed document to enable transportability, interoperability, independent verifiability, and continuity of signature capability. Verifying a signature on a document verifies the integrity of the document and associated attributes and verifies the identity of the signer. There are several technologies available for user authentication, including passwords, cryptography, and biometrics.
Emergency mode operation	Access controls in place that enable an enterprise to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
Emergency mode operation plan	Part of an overall contingency plan. The plan for a process whereby an enterprise would be able to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
Encryption	Transforming confidential plain text into cipher text to protect it. Also called encipherment. An encryption algorithm combines plain text with other values called keys, or ciphers, so the data becomes unintelligible. Once encrypted, data can be stored or transmitted over unsecured lines. Decrypting data reverses the encryption algorithm process and makes the plain text available for further processing. The process by which data is temporarily re-arranged into an unreadable or intelligible form for confidentiality, transmission or other security purpose.
Entity authentication	(1). The corroboration that an entity is the one claimed. (2). A communications/network mechanism to irrefutably identify authorized users, programs, and processes, and to deny access to unauthorized users, programs and processes.

Equipment control (into and out of site)	Documented security procedures for bringing hardware and software into and out of a facility and for maintaining a record of that equipment. This includes, but is not limited to, the marking, handling, and disposal of hardware and storage media.
Evidence	The trail of symptoms left during and after an incident.
External Reporting	The act of reporting incidents outside of your organization: law enforcement, security companies and such.
Facility security plan	A plan to safeguard the premises and building(s) (exterior and interior) from unauthorized physical access, and to safeguard the equipment therein from unauthorized physical access, tampering, and theft.
FERPA	Family Education Rights and Privacy Act
Formal mechanism for processing records	Documented policies and procedures for the routine, and non-routine, receipt, manipulation, storage, dissemination, transmission, and/or disposal of health information.
Full format	In the template package, the entire format for publishing a rule.
GLB	Gramm-Leach-Bliley (Act) –Privacy Legislation that governs disclosure and protection of Non-public personal information by Financial institutions
Hacker	An individual whose primary aim is to penetrate the security defenses of large, sophisticated computer systems. A truly skilled hacker can penetrate a system right to the core and withdraw again without leaving a trace of the activity. Hackers are a threat to all computer systems which allow access from outside your organization's premises. The worlds primary target, the pentagon, is attacked on an average of 1 every 3 minutes.
Hardware/software installation & maintenance review and testing for security features	Formal, documented procedures for (1) connecting and loading new equipment and programs, (2) periodic review of the maintenance occurring on that equipment and programs, and (3) periodic security testing of the security attributes of that hardware/software.
Highly restricted	Classification level for information.
HIPAA	Health Insurance Portability and Accountability Act
Identification	The process of identifying a user with a unique identifier.

IIHI	Individually Identifiable Health Information
Incident	An event of security breach and violation.
Incident Response Team	The group of people responsible for mobilizing and reacting to reported suspicions and incidents.
Independent verifiability	The capability to verify the signature without the cooperation of the signer. Technically, it is accomplished using the public key of the signatory, and it is a property of all digital signatures performed with asymmetric key encryption.
Individual use	The responsibility of the employee to comply with rules and policies.
Information availability	Ensuring that information and services are available when required.
Information confidentiality	Protecting the sensitive information from unauthorized disclosure or intelligible interception.
Information non-repudiation	Providing transfer and receipt of an unforgeable electronic transaction.
Information	Data to which meaning is assigned, according to context and assumed conventions.
Information access control	Formal, documented policies and procedures for granting different levels of access to health care information.
Information security	The protection of data against accidental or malicious destruction, modification, or disclosure. 
Integrity	Safeguarding the accuracy and completeness of information and processing methods. 
Integrity controls	Security mechanism employed to ensure the validity of the information being electronically transmitted or stored.
Internal audit	The in-house review of the records of system activity (for example, logins, file accesses, security incidents) maintained by an organization.
Internal Reporting	The act of reporting incidents outside of your organization: law enforcement, security companies and such.
Internal Use Only	Classification level for information.
Internet	

Interoperability	The applications used on either side of a communication, between trading partners and/or between internal components of an entity, being able to read and correctly interpret the information communicated from one to the other.
Inventory	Formal, documented identification of hardware and software assets.
Intruder	A violator that access systems with unauthorized access to intentionally cause damage or other harassing acts to systems.
IS	Information Systems department for technical staff.
ISS	Information Systems Security
Key	An input that controls the transformation of data by an encryption algorithm.
Kiddie Scripts	A hacker that is less technical.
Logon/ logoff	The processes by which users start and stop using a computer system.
Maintenance of record of access authorizations	Ongoing documentation and review of the levels of access granted to a user, program, or procedure accessing health information.
Maintenance records	Documentation of repairs and modifications to the physical components of a facility, for example, hardware, software, walls, doors, locks.
Malicious Software	The general name for any software that compromises your system, like a virus.
Mandatory Access Control (MAC)	A means of restricting access to objects that is based on fixed security attributes assigned to users and to files and other objects. The controls are mandatory in the sense that they cannot be modified by users or their programs.
Media controls	Formal, documented policies and procedures that govern the receipt and removal of hardware/software into and out of a facility.
Media Security	Security for diskettes, CDs, and other such media that contain information.
Message	A digital representation of information.
Message authentication	Ensuring, typically with a message authentication code, that a message received (usually via a network) matches the message sent.
Message authentication	

code	Data associated with an authenticated message that allows a receiver to verify the integrity of the message.
Message integrity	The assurance of unaltered transmission and receipt of a message from the sender to the intended recipient.
Modem	The equipment that sends information to and from other communications devices.
Multiple signatures	It shall be possible for multiple parties to sign a document. Multiple signatures are conceptually, simply appended to the document.
Need-to-know procedures for personnel access	A security principle stating that a user should have access only to the data he or she needs to perform a particular function.
Network Security	Security of your network and its connections to other networks, internet, and such.
Nonrepudiation	Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents. Providing transfer and receipt of an unforgeable electronic transaction. 
Object Reuse	The reassignment of data to the same media. Data overwriting. Concern: to not have residual data.
Operating, and in some cases, maintenance personnel have proper access authorizations	Formal, documented policies and procedures to be followed in determining the access level to be granted to individuals working on, or in the vicinity of, health information.
Organization	Refers to any state agency, university, or other government facility.
Password	Confidential authentication information composed of a string of characters. A private string of characters that is used to authenticate an identity.
Periodic security reminders	Employees, agents and contractors should be made aware of security concerns on an ongoing basis.
Personally Identifiable Information	(PII) Information that connects or points to a specific person, like

	SSN.
Personnel clearance procedure	A protective measure applied to determine that an individual's access to sensitive unclassified automated information is admissible. The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. Effective screening processes are applied in such a way as to allow a range of implementation, from minimal procedures to more stringent procedures commensurate with the sensitivity of the data to be accessed and the magnitude of harm or loss that could be caused by the individual.
Personnel security	The procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances.
Personnel security policy/procedure	Formal, documentation of policies and procedures established to ensure that all personnel who have access to sensitive information have the required authority as well as appropriate clearances.
Physical access controls (limited access)	Those formal, documented policies and procedures to be followed to limit physical access to an entity while ensuring that properly authorized access is allowed.
Physical safeguards	Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Also covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities.
Piggybacking	Entering secured premises illegally behind another person who has legal access.
PII	(Personally Identifiable Information) Information that connects or points to a specific person, like SSN.
PIN (Personal Identification Number)	A number or code assigned to an individual and used to provide verification of identity.
Policy	The highest level of policy structure from which standards and rules are generated.
Policy/guideline on work station use	Documented instructions/procedures delineating the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings, of a specific computer terminal site or type of site, dependant upon the

	sensitivity of the information accessed from that site.
Privacy	The securing of information that should not be made public.
Procedures	A chronological event, usually contains steps to follow. Procedures can be with and without rules. Most of the procedures are in the Security Officer Instruction Guide, complete with working papers. In the template guides, the procedures are technology-dependent. You can add your procedures in the full format for any rule.
Procedure for emergency access	Documented instructions for obtaining necessary information during a crisis.
Procedures for verifying access authorizations prior to physical access	Formal, documented policies and instructions for validating the access privileges of an entity prior to granting those privileges.
Proto-hacker	Not quite a hacker, but someone that can penetrate systems and leave messages to prove how smart they are. They aspire to be hackers, but have not yet acquired the necessary skills to get past serious security measures without setting off alarm systems.
Provider	A supplier of services as defined in section 1861(u) or (s) of the HIPAA.
Public key	One of the two keys used in an asymmetric encryption system. The public key is made public, to be used in conjunction with a corresponding private key.
Public records	Records that are not private, this revealing the person(s) or place.
Remote Access	The act of getting access to internal systems from another location.
Removal from access lists	The physical eradication of an entity's access privileges.
Removal of user account(s)	The termination or deletion of an individual's access privileges to the information, services, and resources for which they currently have clearance, authorization, and need-to-know when such clearance, authorization and need-to-know no longer exists.
Report procedures	The documented formal mechanism employed to document security incidents.
Response procedures	The documented formal rules/instructions for actions to be taken as a result of the receipt of a security incident report.
Risk	Someone or something that creates or suggests a hazard. The probability that a particular threat will exploit a particular vulnerability.

Risk analysis	Risk analysis, a process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place. The process of identifying assets and threats, prioritizing the threat vulnerability and identifying appropriate safeguards.
Risk management	Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk.
Role-based access control	Role-based access control (RBAC) is an alternative to traditional access control models (e.g., discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. With RBAC, rather than attempting to map an organization's security policy to a relatively low-level set of technical controls (typically, access control lists), each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.
Rule	The lowest level of policy in the template package.
Safeguards	Protective measures implemented to ensure asset are available and protected.
Sanction policy	Organizations must have policies and procedures regarding disciplinary actions which are communicated to all employees, agents and contractors, for example, verbal warning, notice of disciplinary action placed in personnel files, removal of system privileges, termination of employment and contract penalties. In addition to enterprise sanctions, employees, agents, and contractors must be advised of civil or criminal penalties for misuse or misappropriation of health information. Employees, agents and contractors, must be made aware that violations may result in notification to law enforcement officials and regulatory, accreditation and licensure organizations.
Secure work station location	Physical safeguards to eliminate or minimize the possibility of unauthorized access to information, for example, locating a terminal used to access sensitive information in a locked room and restricting access to that room to authorized personnel, not placing a terminal used to access patient information in any area of a doctor's office where the screen contents can be viewed from the reception area.
Security	Security encompasses all of the safeguards in an information system, including hardware, software, personnel policies,

	information practice policies, disaster preparedness, and the oversight of all these areas. The purpose of security is to protect both the system and the information it contains from unauthorized access from without and from misuse from within. Through various security measures, a health information system can shield confidential information from unauthorized access, disclosure and misuse, thus protecting privacy of the individuals who are the subjects of the stored data.
Security awareness training	All employees, agents, and contractors must participate in information security awareness training programs. Based on job responsibilities, individuals may be required to attend customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security.
Security configuration management	Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and other measures, practices and procedures of the organization so as to create a coherent system of security.
Security incident procedures	Formal, documented instructions for reporting security breaches.
Security management process	A security management process encompasses the creation, administration and oversight of policies to ensure the prevention, detection, containment, and correction of security breaches. It involves risk analysis and risk management, including the establishment of accountability, management controls (policies and education), electronic controls, physical security, and penalties for the abuse and misuse of its assets, both physical and electronic.
Security policy	The framework within which an organization establishes needed levels of information security to achieve the desired confidentiality goals. A policy is a statement of information values, protection responsibilities, and organization commitment for a system. It is recommended that security policies apply to all employees, medical staff members, volunteers, students, faculty, independent contractors, and agents. A statement of the goals, responsibilities, and accepted behaviors required for maintaining a secure environment. Security policies set the direction, give broad guidance and demonstrate senior management support for security-related facilities and actions across the organization.
Security Standard	A set of tasks, responsibilities, or guidelines that provide metrics to policies. Security procedures are standards that are very specific in

	nature, applying to group or individual systems. Procedures are directive in nature, whereas policies provide principles.
Security testing	A process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment. This process includes hands-on functional testing, penetration testing, and verification.
Sensitive Information	That information which must be protected to insure only authorized access or if lost or compromised might negatively affect the owner of the information or require substantial resources to recreate.
"Shoulder-surf"	To look over the shoulder of another user to obtain the password.
Sign-in for visitors and escort, if appropriate	Formal, documented procedure governing the reception and hosting of visitors.
Social Engineering	Involves the manipulation of people rather than technology to successfully breach an organizations security. Social engineering remains the single greatest security risk, despite advances in technology, and many of the most damaging security penetrations are the result of social engineering, not electronic "hacking" or "cracking".
Standard	The medium level of policy on the template package.
State Data Network (SDCN)	Any data communications facility contracted for or provided by the State of Nebraska, including State-provided Internet access and network connections to state computers.
Stealth-bombs	Malicious code that is disguised as something else. It may be received as a “normal” e-mail, or perhaps as an amusing screen saver. Stealth-bombs deliver their “payload” surreptitiously and the results can be excessive.
Subject/object separation	Access to a subject does not guarantee access to the objects associated with that subject. Subject is defined as an active entity, generally in the form of a person, process, or device that causes information to flow among objects or changes the system state. Technically, a process/domain pair. Object is defined as a passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are: records blocks, pages, segments, files, directories, directory trees, and programs, as

	well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc.
Suspicion	The suspicion that an incident could be occurring. It is not an incident yet.
Systems Development	The IS department programming and systems design technical staff.
Tailgate	Coming into a secured access entry point on the heels of an authorized person.
Technical security mechanisms	The processes that are put in place to guard against unauthorized access to data that is transmitted over a communications network.
Technical security services	The processes that are put in place (1) to protect information and (2) to control and monitor individual access to information.
Techno-Crime	Term used by the law enforcement agencies to denote criminal activity which uses technology, not as a tool to commit the crime, but as the subject of the crime itself. Techno-crime is usually premeditated and results in deletion, corruption, alteration, theft, or copying data. These criminals will usually probe their preys system for weaknesses and will almost always leave an electronic “calling card” to ensure their pseudo-identity is known. This type of crime is a real possibility from anywhere in the world, leaving few, if any “finger prints”. This term is also used for a hacker or cracker that breaks into a computer system with the sole intent of defacing and or destroying its contents. They can deploy “sniffers” on the internet to locate soft (insecure) targets and then execute a range of commands using a variety of protocols. The best weapon against such attacks is a firewall which hide and disguise your agency’s presence on the internet.
Techno-Vandalism	Term used by the law enforcement agencies to denote criminal activity which uses technology, not as a tool to commit the crime, but as the subject of the crime itself. Techno-crime is usually premeditated and results in deletion, corruption, alteration, theft, or copying data. These criminals will usually probe their preys system for weaknesses and will almost always leave an electronic “calling card” to ensure their pseudo-identity is known.
Telephone callback	A method of authenticating the identity of the receiver and sender of information through a series of ``questions'' and ``answers'' sent back and forth establishing the identity of each. For example, when the communicating systems exchange a series of identification codes as part of the initiation of a session to exchange information, or when a host computer disconnects the initial session before the authentication is complete, and the host calls the user back to

	establish a session at a predetermined telephone number.
Termination procedures	Formal, documented instructions, which include appropriate security measures, for the ending of an employee's employment, or an internal/external user's access.
Testing and revision	(1) Testing and revision of contingency plans refers to the documented process of periodic testing to discover weaknesses in such plans and the subsequent process of revising the documentation if necessary. (2) Testing and revision of programs should be restricted to formally authorized personnel.
Threat	An event with potential to cause unauthorized access, modification, disclosure, or destruction of information resources, applications or systems. Intent to do something bad to someone or something. Indication of an impending undesirable event. An expression of intention to inflict evil, injury, or damage.
Time-of-day	Access to data is restricted to certain time frames.
Time-stamp	To create a notation that indicates, at least, the correct date and time of an action, and the identity of the person that created the notation.
Token	A physical item that's used to provide identity. Typically an electronic device that can be inserted in a door or a computer system to obtain access.
Training	Education concerning the vulnerabilities of the health information in an entity's possession and ways to ensure the protection of that information.
Transportability	A signed document can be transported (over an insecure network) to another system, while maintaining the integrity of the document.
Trojan Horse	Useful program with hidden malicious software.
Turn in keys, token or cards that allow access	Formal, documented procedure to ensure all physical items that allow a terminated employee to access a property, building, or equipment are retrieved from that employee, preferably prior to termination.
Unclassified/ Public	Classification level of information.
Unique user identification	The combination name/number assigned and maintained in security procedures for identifying and tracking individual user identity.

User authentication	The provision of assurance of the claimed identity of an entity.
User-based access	A security mechanism used to grant users of a system access based upon the identity of the user.
User education in importance of monitoring log in success/failure, and how to report discrepancies	Training in the user's responsibility to ensure the security of health care information.
User education concerning virus protection	Training relative to user awareness of the potential harm that can be caused by a virus, how to prevent the introduction of a virus to a computer system, and what to do if a virus is detected.
User education in password management	A type of user training in the rules to be followed in creating and changing passwords and the need to keep them confidential.
User ID	Users of Electronic Assets. Any employee, business partner, contractor, consultant, or customer who is authorized to use the information technology assets of a state agency or institution.
Value of Information	The cost of collection, cost of reconstruction and legal or operational consequences if information is lost or compromised.
Virus	A software program which replicates itself and spreads onto various data storage media (floppy disks, magnetic tapes, etc.) and/or across a network. The symptoms of virus infection include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system.
Virus checking	A computer program that identifies and disables: another ``virus'' computer program, typically hidden, that attaches itself to other programs and has the ability to replicate. (Unchecked virus programs result in undesired side effects generally unanticipated by the user.) (1) A type of programmed threat. A code fragment (not an independent program) that reproduces by attaching to another program. It may damage data directly, or it may degrade system performance by taking over system resources which are then not available to authorized users. (2) A code embedded within a program that causes a copy of itself to be inserted in one or more other programs.
Vulnerability	A weakness in the system, application, infrastructure, control or design flaw that can be exploited to violate system integrity.
Warning Banner	The screen notice that describes your access issues.

Workstation/ Office	An employees work area.
Worm	Malicious software.
Zeroization	The act of erasing information from media and equipment.