UTIA GLOSSARY OF INFORMATION TECHNOLOGY TERMS

Last Reviewed: April 21, 2018 **Last Updated:** April 21, 2018

Accessible – Accessible refers to the concept that people with disabilities are able, including with the help of assistive technologies, to access and use a product or system. For example, an "accessible" website may be designed so that the text can be enlarged by the user, rather than having a fixed font size, or may be designed so that it can be interpreted and "read aloud" by screen reader software used by individuals who are blind or have low vision.

Accessible Information, Materials, & Technology – Accessible information, materials, and technology refer to that which has been designed, developed, or procured to be usable by, and therefore accessible to, individuals with disabilities, including those who use assistive technologies.

Active Directory (AD) – Active Directory is a directory service that Microsoft developed for Windows domain networks. Objects held within a domain can be grouped into Organizational Units (OUs). This makes it easy to apply group policies (GPOs) for securing the operating system's administrative functions.

Affiliate – An affiliate, when listed in the Institute's security plans and procedures, is someone outside the Institute who has a legitimate and approved business need to access Institute IT assets or data. An example could include someone at the county level who works with the County Director or Extension Agent and has an approved business need to share documents for a period of time.

Assistive Technologies – Assistive technologies are adaptive, rehabilitative devices that promote greater independence for individuals with disabilities. Examples include, but are not limited to, special input devices (e.g., head or foot mouse, puff-and-sip switches, and speech recognition), screen-reading software, and screen magnifiers.

Authentication – Authentication is the process of verifying the identity of an individual, device, or process.

Authentication Credentials – Authentication credentials are typically the combination of a user name and authentication factor(s). (see Authentication)

Authorization – Authorization, in the context of access control, determines what a user can do after successful authentication. Authorization, in the context of payment card transactions, occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.

Business Critical – A business critical IT asset is one whose failure may result in an inability to provide essential services(s), further resulting in loss of business, finances, and/or reputation of the Institute.

Cardholder Data (CHD) – Cardholder data is any personally identifiable data associated with a credit card. At a minimum, CHD consists of the full primary account number (PAN), but may also consist of the full PAN plus any of the following: cardholder name, expiration date, and/or service code.

Cardholder Data Environment (CDE) – The cardholder data environment consists of the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data, including any connected system components.

Change Advisory Team (CAT) – The CAT is the team responsible for assessing, prioritizing, and approving changes. The Institute's CAT will be assigned by the Deans and will have one representative from each of the following: CASNR, Extension, Vet Med, AgResearch, and Departments.

Change Control – Change control (change management) is the controlled identification and implementation of required changes with regard to the Institute's IT assets, which focusing on how people and teams are affected by the impending changes.

Change Owner – The Change Owner is the user or system administrator who initiates the RFC. This person(s) will meet with the CAT to discuss the RFC and associated details.

CIA – Confidentiality, Integrity, and Availability, also known as the CIA triad, is the model designed to guide policies for information security within an organization.

Compromise – A compromise, also known as data breach, is an intrusion into a computer system that can lead to an unauthorized disclosure or theft, modification, or destruction of cardholder data.

Configuration Management – Configuration Management comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems. (see SCCM)

Controls – Controls, or more specifically IT security controls, are safeguards or countermeasures put in place to avoid, detect, counteract, or minimize security risk to the Institute's IT assets, physical property, and data.

Cryptographic Key – A cryptographic key is a string of bits used by a cryptographic algorithm to transform plaintext into ciphertext (known as encryption) and ciphertext into plaintext (known as decryption). This key remains private and ensures secure communication.

Data Breach – A data breach is a security incident in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or otherwise used by an unauthorized source.

Data Classification – Data classification is the classification of data based on its level of sensitivity and the impact to the Institute should be data be disclosed, altered, or destroyed without authorization. Data classification helps determine what baseline security controls are appropriate for safeguarding that data. The Institute uses three classifications: low, moderate, or high.

Data Flow Diagram – A data flow diagram uses a graphical representation to show how data flows through an application, network, and/or system.

Defense In Depth – Defense in depth is the coordinated use of multiple security countermeasures to protect the integrity of the Institute's IT assets.

Denial-of-Service Attack – A denial-of-service attack, or DoS attack, is a cyberattack that is meant to shut down an IT asset or network, making it inaccessible to its intended users. DoS attacks flood the target with traffic, or send the target information that causes a crash.

Distributed Denial-of-Service Attack – A distributed denial-of-service attack, or DDoS, occurs when multiple systems flood the bandwidth or resources of a targeted system. This kind of attack is often the result of multiple compromised systems flooding the targeted system with traffic.

DoD Wipe – a DoD wipe is one software-based method of media sanitization that uses random characters to overwrite all data residing on a hard drive.

Encryption – Encryption is the process of converting information into a form that only authorized parties can read with the use of a specific cryptographic key.

eCommerce – eCommerce is an electronic transaction containing payment card and/or cardholder data.

ePHI – ePHI, or electronic protected health information, refers to any protected health information (PHI) that is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred, or received in electronic form.

FERPA – FERPA, the Family Educational Rights and Privacy Act, is a Federal law that protects the privacy of student education records. This law applies to all schools receiving funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records, with those rights transferring to the student when he/she reaches the age of 18 or attends a school beyond the high school level.

File Integrity Monitoring – File integrity monitoring is the technique or technology under which specific files or logs are monitored to detect if they have been modified. When critical files or logs are modified, alerts should be sent to the appropriate Information Security Office.

File-Level Encryption – File-level encryption can be the hardware or software used for encrypting the full contents of specific files.

Firewall – A firewall is a hardware and/or software technology that protects network resources for unauthorized access. A firewall permits or restricts traffic between networks based on a set of firewall rules.

Flaw Remediation – Flaw remediation is incorporated into configuration management as an emergency change in order to address flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling in an expeditious manner.

GDPR – GDPR (General Data Protection Regulation) is a regulation in EU law on data protection and privacy for all individuals within the European Union.

GLBA – GLBA (Gramm-Leach-Bliley Act), also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals. GLBA protects data used in all aspects of the administration of the Title IV Federal student financial aid programs.

Group Policy – Group Policy, or GPO, is feature of the Microsoft Windows. Group Policy provides centralized management and configuration of the Windows operating systems through the Active Directory environment. (see Active Directory)

HIPAA – HIPAA (Health Insurance Portability and Accountability Act of 1996) is a United States legislation that provides data privacy and security provisions for safeguarding medical information. HIPAA is regulated by the Department of Health and Human Services' Office of Civil Rights.

Host – A host is an IT asset that is accessible over the network.

Incident – An incident can be a suspicious computer activity, compromised IT resource, suspected breaches of Institute data, and/or misuse of IT assets according to Institute and University policies and applicable federal and state laws.

Information Owner – An information owner is the person who initiates the creation or storage of information and is the initial owner.

Information System – An information system, or system, consists of computer hardware and software used to collect, filter, process, create, and distribute data.

Information System Owner – The information system owner is responsible for the procurement, development, integration, modification, or operation and maintenance of the information system.

Intellectual Property – Intellectual property refers to a work or invention that is the result of creativity or research to which the owner has rights and may apply for patent, copyright, trademark, etc.

IPS/IDS – IPS/IDS, or Intrusion Protection System and Intrusion Detection System, are two network security tools often used together for Defense in Depth.

IT Assets – An IT asset is any Institute-owned information, system, software, or hardware that is used in the course of business.

Least Privilege – Least privilege is the principle of having the minimum access and/or privileges necessary to perform the roles and responsibilities of the job function.

Load Balancer – A load balancer is a device that acts as a reverse proxy and distributes network or application traffic across a number of servers, increasing capacity (concurrent users) and reliability of applications.

Malicious Code – Malicious code describes any code in any part of a software system or script that is intended to cause undesired effects, security breaches, or damage to a system. Malicious code cannot be efficiently controlled by conventional antivirus software alone.

Malware – Malware is malicious software used to disrupt computer operations, steal sensitive data, and/or gain access to certain systems. Malware includes viruses, worms, Trojan horses, spyware, adware, etc.

Media – Media includes, but is not limited to, paper, hard drives, random access memory (RAM), read-only memory (ROM), disks, flash drives, memory devices, phones, mobile computing devices, and all-in-one printers.

Media Sanitization – Media sanitization is the process of irreversibly removing data from media or permanently destroying the media. For example, paper media can be shredded using a crosscut shredder, while a hard drive can be DoD wiped so the drive can be reused, or degaussed so the drive is completely destroyed.

Merchant – A UTIA department/office/organization that collects payments, electronically or manually, via payment card OR is otherwise involved in storing, processing, transmitting, or receiving payment card or cardholder data.

NetReg – NetReg is the network registration tool with which Institute IT assets must be registered in order to gain network access. NetReg contains information such as hardware address, primary user, owner, location, and classification.

Network Segmentation – Network segmentation isolates system components that store, process, or transmit sensitive data from systems that do not.

NIST – NIST, or National Institute of Standards and Technology, provides the cybersecurity framework used by the Institute for creating and maintaining security plans and procedures.

Patch – Software patches are important for fixing existing problems with software that noticed after the initial release. Most patches are security fixes, while others deal with specific functionality for programs.

Patch Management – Patch management is a strategy for handling patches or upgrades for software applications and technologies.

Payment Application – A payment application is a software application that stores, processes, or transmits CHD electronically. Payment applications include Point of Sale systems and eCommerce systems.

PCI DSS – PCI DSS refers to the Payment Card Industry Data Security Standards and is the industry standard for requirements and guidelines for achieving compliance when accepting credit card payments at the Institute.

Penetration Testing – Penetration testing, or pen testing, is the practice of testing a computer system, network, or web application to find vulnerabilities that an attacker could exploit. This is also referred to as ethical hacking.

Personally Identifiable Information – Personally Identifiable Information, or PII, is that information used to identify or trace an individual's identity. This can include but is not limited to full name, address, date of birth, social security number, biometric data, etc.

PHI – PHI (Protected Health Information) is under US law and is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

Phishing email – Phishing emails are typically fraudulent email messages that appear to come from a legitimate source, such as the HelpDesk, your bank, etc. The purpose of a phishing attempt is to obtain sensitive information such as usernames, passwords, bank accounts, credit card information, or other such information.

Policy – A policy contains the rules governing the acceptable use of computing resources, security practices, and guiding development of operational procedures. *(Note: The Institute's IT security policies are called IT security plans.)*

Procedure – A procedure is the "how to" for a policy and describes how the policy is to be implemented.

Protected Health Information – Protected health information (PHI) under US law is any oral or recorded information in a medical record that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a health care service. PHI can include demographic information, medical history, test and laboratory results, insurance information, treatment, etc.

Qualys – Qualys is a network security and vulnerability management tool used by the Institute.

Ransomware – Ransomware is a type of malware that prevents or limits users from accessing IT assets by locking the screen and/or files. Ransomware is often downloaded from a malicious or compromised website or is dropped into email attachments. When ransomware has been installed, the user is notified via a screen message saying payment must be remitted in order to regain access to the computer and/or files.

Redact – Redact is to edit or obscure information in a document for legal or security purposes.

Request for Change (RFC) – An RFC is a formal request for the implementation of a change. The RFC provides details on the size and likely impact of a change, and is submitted for review and approval by the CAT.

Risk Assessment – Risk assessment is the on-going process of reviewing the possible treats to the Institute's IT assets. These threats are weighted by the likelihood of occurrence, and then multiplied by their effect on the operation.

Risk Management – Risk management is defined by NIST as encompassing three processes: risk assessment, risk mitigation, and evaluation and assessment.

Risk Mitigation – Risk mitigation is the systemic reduction on the extent of exposure to a risk and/or the likelihood of its occurrence.

Role Based Access Control (RBAC) – Role based access control is an implementation for restricting system access to authorized users based on role.

SCCM (System Center Configuration Manager; Configuration Manager) – SCCM is a systems management software product from Microsoft used for managing large groups of computers. SCCM provides remote control, patch management, software distribution, operating system deployment, network access protection. SCCM also provides hardware and software inventory.

Separation of Duties – Separation of duties of the practice of dividing steps in a function among different individuals, so one individual cannot threaten the process. It is a measure of checks and balances.

Spam – Spam refers to irrelevant of inappropriate messages sent on the Internet to a large number of recipients.

System –A system, or IT system, is one that is used to collect, filter, process, create, and distribute data.

System Characterization – System characterization establishes the scope of the risk assessment effort, delineates the operational authorization boundaries, and provides information essential to defining the risk.

System Classification – System classification is the process of identifying the type of data that is stored, processed, or viewed on the Institute's IT assets. This classification is critical for protecting the data by putting the appropriate security controls in place, as well as for responding in the most efficient and appropriate method when certain IT assets are compromised.

Third-party provider – A third-party provider is a non-Institute employee who the Institute has outsourced for a particular need. This provider has a defined interaction, including scope and duration, with the Institute. This service is usually defined in an approved contract.

Threat – A threat is any circumstance or event with the potential to adversely impact the Institute's operations, assets, or personnel through and information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Trade Secrets – A trade secret is a formula, process, design, method, or compilation of information not generally known or reasonably attainable by others, which provides a business with a competitive edge.

Trojan Horse – A Trojan horse is any malicious computer program used to hack into a computer by misleading users of its true intent.

Two-Factor Authentication – Two-factor authentication is a two-step process to verify the identity of a user trying to access a system or network. These factors include: 1) something you know, such as a password, passphrase, or PIN; 2) something you have, such as a token or smart card; and 3) something you are, such as biometric data. For two-factor authentication, you must use at least two of these three factors, and cannot use two of the same factor (i.e., a username and a password).

Usability – Usability refers to how easily, effectively, and efficiently users can use a product or system to achieve their goals, as well as how satisfied they are with the experience.

User – A user, as in IT user, is a person who uses IT assets like computers, network services, etc. "User" includes but is not limited to students, faculty, staff, Tennessee State University (TSU) employees, county funded employees, seasonal workers, externs, interns, volunteers, contractors, third-party agents, representatives, and other visitors using Institute-owned IT assets.

UT Location – UT location (or location) refers to any physical site with a University of Tennessee presence, including but not limited to University campuses, institutes, and centers.

Vulnerability – A vulnerability is a weakness in a system that can result in a compromise or data breach.

Vulnerability Assessment – A vulnerability assessment is the process that defines, identifies, and classifies the security vulnerabilities in a computer or network infrastructure.

Vulnerability Scanner – A vulnerability scanner is a program used to scan networks, servers, desktops, and/or web applications for security vulnerabilities. The scan detects vulnerabilities and potential vulnerabilities.

Web Application – A web application is generally accessed through a web browser or through web services.

For more information, contact Sandy Lindsey, CISO, at (865) 974-7292, or email sandy@tennessee.edu.