

## **GLOSSARY OF TERMS**

### **UNIVERSITY OF TENNESSEE INFORMATION SYSTEMS SECURITY**

**Applicable Laws of the State of Tennessee and the Federal Government** – Any law in the state of Tennessee or from the federal government that applies to security and information systems, information systems resources, or electronic information transmission technologies.

**Applications and Systems Assessment Process** – The process by which assigned personnel from the Information Security Office perform vulnerability assessments on information systems resources.

**Audit and Consulting Services** – The department responsible for proactive reviews of computer systems and services for compliance with information systems security standards and policies, other internal university policies and standards, and the requirements of external regulatory bodies.

**Campus/Institute Security Lead** – The person assigned by the Position of Authority for Information Systems for Each Respective Campus or Institute who is responsible for information systems security for that respective campus or institute.

**Chief Information Officer** – The person responsible for University of Tennessee's information systems planning and direction.

**Computer System** – An electronic device that uses common storage and executes code for designated data manipulation that is user-written. This includes all portable devices including, but not limited to, laptop computers, personal digital assistants, all mobile email devices, and the associated storage devices.

**Contingency planning** – Outlines the process of establishing strategies to minimize the effects of a disruption and ensure timely resumption of operations.

**Defense in Depth** – The creation of layers of security as a mechanism to protect information systems resources.

**Electronic Information** – Refers to information in electronic form and the computer systems on which the information resides. This does not apply to information in paper form.

**Family Educational Rights and Privacy Act (FERPA)** – The Family Educational Rights and Privacy Act of 1974, commonly referred to as the Buckley Amendment, protects the rights of students by controlling the creation, maintenance, and access to educational records. It guarantees students' access to their academic records while prohibiting unauthorized access by others.

**Gramm-Leach-Bliley Act (GLBA)** – Requires financial institutions to protect the confidentiality and integrity of their customer's information.

**Hacking** – Unauthorized use of an information system or network including attempts to bypass security mechanisms.

**Health Insurance Portability and Accountability Act (HIPAA)** – Creates a standard for healthcare providers and institutions to protect the confidentiality and integrity of personal health information.

**Incident Response** – Is the process where information systems professionals respond to information systems resources compromises, vulnerabilities, and attacks.

**Information Security Office** – The entity that is responsible for the information systems security oversight and administration for the University of Tennessee.

**Information Systems Resources** – Includes any computers, computer systems, network devices, telephony systems, or software applications.

**Information Systems Security Awareness and Education Program** – Provides documentation, information, guidelines, and direction related to information systems security protection methods, principles, and responsibilities for all users of information systems resources.

**Information Systems Security Council (ISSC)** – Provides the direction and guidance for information systems security for the University of Tennessee. This council reviews and approves all policies as related to information systems security that apply to the University of Tennessee.

**Network Infrastructure** – Refers to the architecture in terms of equipment and connections that comprise a network. It includes fixed equipment consisting of wireless transceivers, routers, antennas, switches, cabling, management information systems, and other equipment. This does not include workstations, printers, or file, print, or application servers.

**Office of Public/University Relations** – The office, under the leadership of the Vice president for Public Relations and Government Relations, produces communication vehicles for high profile university initiatives such as student recruitment and alumni relations, while also serving the communication needs of other university departments. In addition the office provides overall public relations coordination for marketing and communications offices at the Chattanooga campus, the Martin campus, the Health Science Center in Memphis, the Institute of Agriculture, the Institute for Public Service, and the Space Institute.

**Personally Identifiable Information:** The information comprising personal information governed by this policy is defined as an individual's first name or first initial and last name, in combination with any one or more of the following:

- Social security number,
- Driver's license number, or
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

**Position of Authority for Information Systems for Each Respective Campus, Institute, School, Division, or Unit (POA)** – The person assigned by each respective campus chancellor or institute vice-president as the information systems authority for that respective location. This position is responsible for the creation of procedures, guidelines, best practices, and standards that define the implementation of information systems security policies at the respective location. The Position of Authority for Information Systems at each respective location includes representation from the following:

- Chattanooga Campus
- Health Sciences Center
- Knoxville Campus
- Martin Campus
- Institute of Agriculture
- Institute for Public Service

- Space Institute

**University of Tennessee Policy Advisory Group** – The group responsible for ensuring the consistency of University of Tennessee policies and ensuring that conflicts between policies are resolved.

**Users** – Refers to all students, faculty, staff and others while accessing, using, or handling the University of Tennessee’s information systems resources. Others includes, but is not limited to, subcontractors, visitors, visiting scholars, potential students, research associates, grant and contract support personnel, media representatives, guest speakers, and non-university entities granted access.