Knoxville Campus Policy: IT00004-K Information Security	
Version 1	Effective Date: 06/14/2018

Office of Information Technology

Information Security

University Information Security Plans

UTK Baseline Controls
Minimum list of security controls that are required here on the UTK Campus.
(Updated 04/05/2018)

UTK Security Program Plan
This plan details the information security risks UTK faces, and the resulting controls it is responsible for.
(Updated 04/05/2018)

System Security Plan Template
Provides the framework for the creation of departmental security plans.
(Updated 04/05/2018)

Security Program Management Methodology
PowerPoint presentation explaining Information Security Methodology.
(Updated 04/05/2018)

UTK Incident Response Plan
Provides guidance regarding notification and responses to security-related events. In addition to incidents such as cyber-intrusions or unauthorized disclosure of sensitive information, this plan also specifies the requirements for dealing with suspected information technology abuses.

Media Protection Standard
This document outlines the Media Protection standards that constitute the campus standard. Each campus unit is bound to this standard.
(Updated 04/19/2018)

University Policies

Information Technology Policies
Information Technology Policies is a direct link to the complete list of Information Technology Policies listed below. You can click the link above to access the list of policies, or click the links below to access an individual policy.

IT0110 – Acceptable Use of Information Technology Resources

This policy governs the use of the university's information technology resources in an atmosphere that encourages free exchange of ideas and an unwavering commitment to academic freedom.

IT0115 – Information and Computer System Classification

This policy provides policies for information, and information system categorization, and establishes Federal Information Processing Standard 199 (FIPS 199) as the University of Tennessee's Information Categorization model.

IT0120 – Secure Network Infrastructure

This policy provides the definitions for creation and maintenance of a secure systems infrastructure, including both wired and wireless technologies.

IT0121 – Information Security Plan Creation and Data Breach Notification Procedures

This policy provides policies for establishing information security plans and data breach notification procedures.

IT0122 – Security incident, Reporting, and Response

This document establishes policy for incident identification, reporting, and response.

IT0123 – Security Awareness, Training, and Education

This document establishes policy for maintaining the security skills of the organizational users, IT personnel, and security staff.

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Health Insurance Portability and Accountability Act (HIPPA)

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addressed the security and privacy of health data.

Gramm-Leach Bliley Act (GLB Act)

The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act" or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.