INFORMATION TECHNOLOGY SERVICES

EAST TENNESSEE STATE UNIVERSITY

The ETSU Information Technology Council (ITC) has proposed an Information Security Policy that has been out for public comment for 30 days. The policy stats that ETSU information security will implement security best practices as outlined by the National Institute of Standards and Technology (NIST) 800-53. These guidelines are standard for federal agencies and include 17 categories/families containing 240 controls. Therefore, ETSU may not need to implement every control in each family included in the standard but this standard provides a very good foundation for which to base our information security best practices. The following is a list of the Control Families along with one example of a control for each. Hopefully this will provide some clarity and context for the Information Security Policy brought forward by ITC.

NIST SP 800-53 CONTROLS	
FAMILY: Access Control (25)	
AC-17	Remote Access
	1. Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the access control policy and associated access controls; and 2. Reviews and updates the current: 1. Access control policy [*Assignment: organization-defined frequency*]; and 2. Access control procedures [*Assignment: organization-defined frequency*]. **EX. The organization:** **(a) Authorizes the execution of privileged commands and access to security-relevant information via remote access only for [*Assignment: organization-defined needs*]; and** **(b) Documents the rationale for such access in the security plan for the information system.**
FAMILY: Awareness and Training (5)	
AT-2	Security Awareness Training
	The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. [*Assignment: organization-defined frequency*] thereafter. **EX. The organization includes practical exercises in security awareness training that simulate actual cyber-attacks.**
FAMILY: Audit and Accountability (16)	
AU-6	Audit Review, Analysis, and Reporting
	a. Reviews and analyzes information system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity]; and

	b. Reports findings to [Assignment: organization-defined personnel or roles]. **EX. The organization employs automated mechanisms to integrate audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.**
FAMILY: Security Assessment and Authorization (9)	
CA-2	Security Assessments
	a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and 3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to [Assignment: organization-defined individuals or roles]. **EX. The organization employs assessors or assessment teams with [Assignment: organization-defined level of independence] to conduct security control assessments.**
FAMILY: Configuration Management (11)	
CM-7	Least Functionality
	The organization: a. Configures the information system to provide only essential capabilities; and b. Prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined prohibited or restricted functions, ports, protocols, and/or services]. **EX. The organization:** **(a) Reviews the information system [Assignment: organization-defined frequency] to identify unnecessary and/or non-secure functions, ports, protocols, and services; and** **(b) Disables [Assignment: organization-defined functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure].**
FAMILY: Contingency Planning (13)	
CP-2	Contingency Plan
	The organization: a. Develops a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by [Assignment: organization-defined personnel or roles]; b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; c. Coordinates contingency planning activities with incident handling activities; d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency]; e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and g. Protects the contingency plan from unauthorized disclosure and modification.

	EX. The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.
FAMILY: Identification and Authentication (11)	
IA-2	Identification and Authentication (Organizational Users)
	The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). **EX. The information system implements multifactor authentication for network access to privileged accounts such that one of the factors is provided by a device separate from the system gaining access and the device meets [Assignment: organization-defined strength of mechanism requirements].**
FAMILY: Incident Response (10)	
IR-2	Incident Handling
	The organization: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly. **EX. The organization coordinates with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross-organization perspective on incident awareness and more effective incident responses.**
FAMILY: Maintenance (6)	
MA-6	Timely Maintenance
	The organization obtains maintenance support and/or spare parts for [Assignment: organization-defined information system components] within [Assignment: organization-defined time period] of failure. **EX. The organization performs predictive maintenance on [Assignment: organization-defined information system components] at [Assignment: organization-defined time intervals].**
FAMILY: Media Protection (8)	
MP-6	Media Sanitization
	The organization: a. Sanitizes [Assignment: organization-defined information system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures] in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. **EX. The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].**
FAMILY: Physical and Environmental Protection (20)	
PE-19	Information Leakage
	The organization protects the information system from information leakage due to electromagnetic signals emanations. **EX. The organization ensures that information system components, associated data communications, and networks are protected in accordance with national emissions and TEMPEST policies and procedures based on the security category or classification of the information.**
FAMILY: Planning (9)	

PL-8	Information Security Architecture
	The organization: a. Develops an information security architecture for the information system that: 1. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; 2. Describes how the information security architecture is integrated into and supports the enterprise architecture; and 3. Describes any information security assumptions about, and dependencies on, external services; b. Reviews and updates the information security architecture [Assignment: organization-defined frequency] to reflect updates in the enterprise architecture; and c. Ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions. **EX. The organization designs its security architecture using a defense-in-depth approach that:** **(a) Allocates [Assignment: organization-defined security safeguards] to [Assignment: organization-defined locations and architectural layers]; and** **(b) Ensures that the allocated security safeguards operate in a coordinated and mutually reinforcing manner.**
FAMILY: Personnel Security (8)	
PS-3	Personnel Screening
	The organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening]. **EX. The organization ensures that individuals accessing an information system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.**
FAMILY: Risk Assessment (6)	
RA-5	Vulnerability Screening
	The organization: a. Scans for vulnerabilities in the information system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported; b. Employs vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: 1. Enumerating platforms, software flaws, and improper configurations; 2. Formatting checklists and test procedures; and 3. Measuring vulnerability impact; c. Analyzes vulnerability scan reports and results from security control assessments; d. Remediates legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk; and e. Shares information obtained from the vulnerability scanning process and security control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies). **EX. The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.**
FAMILY: System and Services Acquisition (22)	
SA-22	Unsupported System Components
	The organization: a. Replaces information system components when support for the components is no longer available from the developer, vendor, or manufacturer; and b. Provides justification and documents approval for the continued use of unsupported system components required to satisfy mission/business needs.

	EX. The organization provides [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]] for unsupported information system components.
FAMILY: System and Communications Protection (44)	
SC-42	Sensor Capability and Data
	The information system: a. Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]; and b. Provides an explicit indication of sensor use to [Assignment: organization-defined class of users]. **EX. The organization prohibits the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems].**
FAMILY: System and Information Integrity (17)	
SI-13	Predictable Failure Prevention
	The organization: a. Determines mean time to failure (MTTF) for [Assignment: organization-defined information system components] in specific environments of operation; and b. Provides substitute information system components and a means to exchange active and standby components at [Assignment: organization-defined MTTF substitution criteria]. **EX. The organization takes information system components out of service by transferring component responsibilities to substitute components no later than [Assignment: organization-defined fraction or percentage] of mean time to failure.**