THE UNIVERSITY OF TENNESSEE

System-wide Policy: IT1516 - Information Technology Service Provider Management and Application Software Security Management	
Version: 1	**Effective Date: 01/23/2025**

SECTION 1. Policy Statement

I. Objective

This policy provides guidance and structure for the University to establish an IT Service Provider program that manages inventory, classifies each IT Service Provider, ensures that IT Service Provider contracts include security requirements, and securely decommissions IT Service Providers. This policy also provides guidance and structure for University to establish and maintain a secure application development process including a process to accept and address reports of software vulnerabilities.

II. Information Technology Service Provider Management Policy

The Central IT Department must communicate the requirements and processes for Information Technology (IT) Service Provider management to the campus community annually to engage campus communities and individuals in the shared responsibility of secure IT Service Provider management. In all cases within this policy where the Central IT Department is required to create a process to implement an IT security control, training and guidance must also be provided to the campus or institute community related to the control itself and the associated process.

1. The Central IT Department, in coordination with the Procurement and Contracts Offices, will create a process to complete and maintain an inventory of IT Service Provider that includes:

a. Name of IT Service Provider.

b. Signature authority for the contract.

c. Business Unit or Units leveraging the platform.

d. IT Service Provider classifications as defined by the Central IT Department that demonstrate the level of trust with each vendor in their use.

e. Point of contact for IT Service Provider.

f. Point of contact within the University managing the IT Service Provider relationship.

g. Requirement that the IT Service Provider inventory be reviewed and updated annually, or when IT Service Provider changes occur.

h. Data on the IT Service Provider platform and the respective Data Owners.

2. The Central IT Department will create a process to classify each IT Service Provider according to attributes such as:

a. Business function.

b. Geographical location.

c. Data sensitivity.

d. Data volume.

e. Availability requirements.

f. Applicable regulations.

g. Inherent risk or mitigated risk.

h. Nature of the deployment of the service.

Implementation Group 2 and 3 Controls

Note that Implementation Group 2 (IG2) controls are not required to be implemented until January 1, 2027, and Implementation Group 3 (IG3) by January 1, 2029.

1. The Central IT Department will create a procedure to establish formal IT Service Provider management (IG2) that includes:

a. Classification, inventory, assessment, monitoring, and decommissioning of IT Service Providers.

b. Review and update the policy annually.

2. The Central IT Department will create a process for classification considerations of IT Service Providers to include one or more characteristics, such as Data sensitivity, Data volume, availability requirements, applicable regulations, inherent risk, and mitigated risk. The process will also include update and review of classifications annually.

3. The Central IT Department will create a process, in collaboration with the Procurement Office, to ensure IT Service Provider contracts and Data usage agreements include security requirements (IG2) that are appropriate for the categorization of the Data. Example requirements may include minimum Security program requirements, Security Incident and/or Data breach notification and response, Data encryption requirements, and Data disposal commitments.

a. The process will ensure that these Security requirements are consistent with the University's IT Service Provider management policy.

b. The process will also include a review of IT Service Provider contracts annually or when renegotiated to ensure contracts are not missing security requirements.

c. The Data Owner(s) and Data Custodian(s) must be included in the process.

4. The Central IT Department will create a process to assess IT Service Providers consistent with the University's IT Service Provider management policy (IG3). The assessment scope may vary based on classification(s), and may include review of standardized assessment reports, such as Service Organization Control 2 (SOC 2) and Payment Card Industry (PCI) Attestation of Compliance (AoC), customized questionnaires, or other appropriately rigorous processes. The process will also include reassessment of IT Service Providers annually, at a minimum, or with new and renewed contracts.

5. The Central IT Department will create a process to monitor IT Service Providers consistent with the University's IT Service Provider management policy (IG3) including periodic reassessment of IT Service Provider compliance, monitoring IT Service Provider release notes, and dark web monitoring.

6. The Central IT Department will create a process to securely decommission IT Service Providers (IG3).

7. Data on IT Service Providers (e.g., cloud services) must be disposed of by first requesting the appropriate methods to permanently delete Data stored in their Systems, and then performing those actions according to the received instructions.

8. The Central IT Department must analyze if cloud IT Service Providers used by the University are effectively backing up University Data, and if that Data must be considered within the University Data Recovery Plan as defined in System-wide Policy: IT0311 - Information Technology Data Access, Management, and Recovery. This includes evaluation that the appropriate language is included in the cloud IT Service Provider contract. Data Owners must be consulted as a part of this process.

9. Every cloud platform and/or cloud service used by the University must be appropriately configured in accordance with University standards (reference System-wide Policy: IT4912 - Information Technology Secure Configuration Management) and CIS benchmarks or allow for vendor supplied hardening guides if CIS doesn't have a benchmark for a specific service and must meet security requirements for their individual purpose.

10. The Central IT Department will create a process that ensures that all cloud-based services have a malware defense program (reference the System-wide Policy: IT7810 - Information Technology Vulnerability Management, Audit Log Management, and Malware Defense Policy for more information).

11. All cloud-based IT Service Providers will provide documentation that they have a written incident response plan that is tested at least annually (reference the System-wide Policy IT0017 - Information Technology Incident Response Management for more information).

III. Application Software Security Management Policy

The Central IT Department must communicate the requirements and processes for application software security management to the campus community annually to engage campus communities and individuals in the shared responsibility of secure application software security management. In all cases within this policy where the Central IT Department is required to create a process to implement an IT security control, training and guidance must also be provided to the campus or institute community related to the control itself and the associated process.

1. For all application development, following the Open Worldwide Application Security Project (OWASP) standard unless a different secure software development standard is contractually required.

Implementation Group 2 and 3 Controls

Note that Implementation Group 2 (IG2) controls are not required to be implemented until January 1, 2027, and Implementation Group 3 (IG3) by January 1, 2029.

2. The Central IT Department will create a process to establish and maintain a secure application development process for all applications developed for the University (IG2). Address such items as:

a. Secure application design standards.

b. Secure coding practices.

c. Developer training.

d. Vulnerability management.

e. Security of third-party code.

f. Application security testing procedures.

g. Review and update documentation annually.

3. The Central IT Department will create a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report (IG2). The process is to include such items as:

a. A vulnerability handling policy that identifies reporting process

b. Responsible party for handling vulnerability reports.

c. A process for intake, assignment, remediation, and remediation testing.

d. Use a vulnerability tracking System that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities.

e. Review and update documentation annually.

4. The Central IT Department will create a process to perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code and allows development teams to move beyond just fixing individual vulnerabilities as they arise (IG2).

5. The Central IT Department will create a process to establish and manage an updated inventory of IT Service Provider components used in development, often referred to as a "bill of materials," as well as components slated for future use (IG2).

a. This inventory is to include any risks that each IT Service provider component could pose.

b. Evaluate the list at least monthly to identify any changes or updates to these components and validate that the component is still supported.

6. The Central IT Department will create a guideline for the campus community to use up-to-date and trusted third-party software components (IG2). The guideline will include:

a. Choose established and proven frameworks and libraries that provide adequate security.

b. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.

7. The Central IT Department will create a process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed (IG2). The process will include:

a. Setting a minimum level of security acceptability for releasing code or applications.

b. Review and update the System and process annually.

8. The Central IT Department must develop guidelines to use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components (IG2) and does not allow in-house developed software to weaken configuration hardening.

9. The Central IT Department must develop guidelines to maintain separate environments for production and non-production environments of Systems (IG2).

10. The Central IT Department will ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities (IG2).

a. The Central IT Department must develop a process to conduct training at least annually.

b. The Central IT Department must develop a process to design in a way to promote Security within the development team and build a culture of Security among the developers.

11. The Central IT Department must develop guidelines to apply secure design principles in application architectures (IG2). Secure design principles include:

a. The concept of least privilege and enforcing mediation to validate every operation that the User makes.

b. Promoting the concept of "never trust User input."

c. Ensuring that explicit error checking is performed and documented for all input.

d. Minimizing the application infrastructure attack surface.

e. The Central IT Department must develop guidelines to leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging (IG2). Use only standardized, currently accepted, and extensively reviewed encryption algorithms.

12. The Central IT Department must develop guidelines to apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed (IG3).

13. The Central IT Department will conduct application Penetration Testing (IG3).

14. The Central IT Department will conduct Threat Modeling. Threat Modeling is the process of identifying and addressing application Security design flaws within a design before code is created (IG3).

IV. Exceptions

The University's Chief Information Officer is authorized to grant exceptions to the University's Information Technology Policies. Campus or institute CIOs/DTLs are authorized to grant exceptions to campus or institute processes and procedures.

SECTION 2. Reason for the Policy

This policy establishes the requirements for Information Technology (IT) Service Provider management and application software security management as described in CIS Control 15 (Service Provider Management)

and CIS Control 16 (Application Software Security) for the University of Tennessee in support of System-wide Policy: IT0001 – General Statement on Information Technology Policy. All Users must familiarize themselves with System-wide Policy: IT0001.

SECTION 3. Scope and Application

This policy applies to all Users of IT Resources owned, operated, or provided by the University of Tennessee, including its campuses, institutes, and administration (University and/or campuses).

SECTION 4. Procedures

Each campus/institute will adopt procedures related to this policy.

SECTION 5. Definitions

See IT0001 – General Statement on Information Technology Policy for definitions of terms.

SECTION 6. Penalties/Disciplinary Action for Non-Compliance

Any violation of this policy may subject the User to discipline as a violation of one or more provisions of the general standard of conduct in the student handbook or to discipline under the Code of Conduct (HR0580 – Code of Conduct) in the Human Resources Policy and Procedures.

The University may temporarily or permanently remove access to its information technology Resources if an individual violates this policy.

SECTION 7. Responsible Official & Additional Contacts

Subject Matter	Office Name	Telephone Number	Email/Web Address
Policy Clarification and Interpretation	System Chief Information Officer and System Chief Information Security Officer	(865) 974-4810 or (865) 974-0637	cio@tennessee.edu or iso@tennessee.edu
Policy Training	System Chief Information Security Officer	(865) 974-0637	iso@tennessee.edu

[Text Wrapping Break]_____

SECTION 8. Policy History

Revision 1:

_____

SECTION 9. Related Policies/Guidance Documents

A. University Policies

a. IT0001 – General Statement on Information Technology Policy

b. IT0002 – Acceptable Use of Information Technology Resources

c. IT0003 – Information Technology Security Program Strategy

d. IT0004 – Information Technology Risk Management

e. IT0005 – Data Categorization

f. IT0014 – Security Awareness Training Management

g. IT0017 – Information Technology Incident Response Management

h. IT0102 – Information Technology Asset Management

i. IT0311 – Information Technology Data Access, Management, and Recovery

j. IT0506 – Information Technology Account and Credential Management

k. IT1318 – Information Technology Network Monitoring and Defense and Penetration Testing

l. IT4912 – Information Technology Secure Configuration Management

m. IT7810 – Information Technology Vulnerability Management, Audit Log Management, and Malware Defense

B. Center for Internet Security Critical Security Controls Navigator

https://www.cisecurity.org/controls/cis-controls-navigator/

_____

System-wide Policy: IT1516 - Information Technology Service Provider Management and Application Software Security Management	
Version: 1	**Effective Date: 01/23/2025**