



EAST TENNESSEE STATE
UNIVERSITY

University-Hosted Enterprise Resource Planning Backup

Policy Name: University-Hosted Enterprise Resource Planning Backup

Policy Purpose

This policy specifies the process to prevent data loss from the university-hosted Enterprise Resource Planning (ERP) system and ensure data availability and integrity should ERP data restoration be required.

Applicability

This policy is applicable to employees.

Responsible Official, Office, and Interpretation

The Office of Information Technology Services and Information Technology Council are responsible for the review and revision of this policy. For questions about this policy, please contact Office of Information Technology Services. The Chief Information Officer in consultation with the Office of University Counsel, has the final authority to interpret this policy.

Defined Terms

A defined term has a specific meaning within the context of this policy.

Air-Gapped Storage Environment

Refers to a system or network that is physically isolated from other networks, specifically the Internet, to protect it from unauthorized access, cyber threats, and malware.

University Hosted Enterprise Resource Planning (ERP) System

The software system used to manage core student related university business processes and associated data. This does not include cloud hosted Software-as-a-Service.

Machine Image

A template of a complete state of a machine, including its operating system, applications, configurations, and data. The template can then be shared to multiple machines to streamline deployment and backup/recovery processes.

Policy Name: University-Hosted Enterprise Resource Planning Backup

Policy

Daily backup copies of data, software, and Machine Images from the ERP system shall be created and maintained in an Air-Gapped Storage Environment to ensure data integrity and security. At least one backup location must be situated a minimum of 50 miles off-site, in accordance with applicable regulatory requirements and Tennessee STS Enterprise Information Security Policy. Backup locations and detailed recovery procedures are outlined in the ITS Business Continuity Plan. Daily data backups shall be retained as independent, versioned copies for a minimum of 90 days. Machine Images must be created prior to any patching activity and retained for at least two version iterations.

Recovery Testing.

Restoration procedures for ERP system data and Machine Images must be tested annually in accordance with the recovery time objective defined in the ETSU Business Continuity Plan and a test recovery point objective specified by the Chief Information Officer (CIO).

Annual restore test reports must be submitted to the CIO for review. Any issues identified during testing shall be addressed through documented remediation activities. Following remediation, restore testing must be repeated to verify the effectiveness of corrective actions, and the results must be formally documented. Recovery from local and off-site backups of ERP data and Machine Images will be performed annually. A summary report of each restore test must be submitted to the CIO for review.

Policy Name: University-Hosted Enterprise Resource Planning Backup

Procedures

N/A

Applicable Forms and Websites

N/A

Authority and Revisions

Authority: FOCUS ACT, TCA § 49-8-203 et. seq; Tennessee STS Enterprise Information Security Policy 4.3 and 12.1; National Institute of Standards and Technology CP-4 and CP-10.

Previous Policy: Enterprise Resource Planning System Backup

The ETSU Board of Trustees is charged with policy making pursuant to TCA § 49-8-203, et seq. On March 24, 2017, the Board delegated its authority to ETSU's President to establish certain policies and procedures for educational program and other operations of the University, including this policy. The delegation of authority and required process for revision to this policy can be found on the [Policy Development and Rule Making Policy webpage](#).

To suggest a revision to this policy, please contact the responsible official indicated in this policy. Before a substantive change to the policy section may take effect, the requested changes must be: (1) approved by the responsible office; (2) reviewed by the Office of University Counsel for legal sufficiency; (3) posted for public comment; (4) approved by either Academic Council or University Council; and (5) approved by ETSU's President.