Policy Number: VI.04
Policy Level: Operating Policy
Originally Issued: January 25, 2016
Revised: February 8, 2017
Reviewed: February 7, 2018
Revised: May 15, 2018
Reviewed: October 7, 2020
Reviewed: November 5, 2021
Reviewed: November 3, 2022
Policy Owner: President
Policy Implementation: Chief Information Officer
SACSCOC Standard: 12.5

Incident Response/Recovery and Data Backup

I. Policy Statement and Purpose

Athens State University students, faculty, and staff rely on information technology resources and services to operate and manage University business and academic functions. Information technology services support critical functions of the University and has established protocols to ensure security, confidentiality, integrity, and data protection and back-up.

In accordance with Athens State University's mission, this policy establishes the requirement for the development and implementation of an Incident Response/Recovery and Data Backup process to address critical system failures and catastrophic disasters.

II. Incident Response and Recovery Plan

Information Technology Services (ITS) is responsible for developing an Incident Response and Recovery Plan (IRRP). The IRRP defines the resources and processes necessary for an appropriate response to and recovery from any incident affecting the critical technology infrastructure and data to allow the University to maintain a continuity of services and business processes. ITS will coordinate as necessary for inter-departmental and external assistance to ensure the necessary resources and personnel are identified and notified of their inclusion in the IRRP.

III. Data Backup

ITS is responsible for the backup of the databases, processes, and configurations used to manage and support the Banner Enterprise Resource Planning (ERP) system and other mission critical resources and functions. Individual departments are responsible for notifying ITS of any department data stored at the Enterprise level that have specific data backup and retention requirements specified by governing laws, regulations and/or policies.

The data backup process must be designed such that mission critical data can be restored in part or whole as required for the continuity of business processes. The frequency and extent of backups are based on how frequently the data changes and overall data recovery requirements.

The backup of individual workstations is the responsibility of individual users. ITS can recommend backup processes and hardware for individual workstation backups and assist in installing and configuring backup solutions for the users.

IV. Responsibility for this Operating Policy

Policy Owner

As part of the initial approval of this policy by the President and subsequent to the original dissemination of the policy, the President is the policy owner for the ongoing evaluation, review, and approval of this policy. Subsequent reviews and revisions to this policy must be in accordance with approved operating policy procedures and processes.

This policy will be reviewed annually or more frequently as needed by the Policy Owner. Revisions will be reviewed/affirmed by the Cabinet and approved by the University President. This policy will be updated/published in the University's Policy Library.

Responsibility for Policy Implementation

The President has assigned the responsibility of implementing this policy to the Chief Information Officer.