Albany State University

UNIVERSITY SYSTEM OF GEORGIA™

University Policy
Enterprise Information Security

Introduction

The Enterprise Information Security Policy was created to comply with University System of Georgia (USG) information technology policies. Pursuant to the USG Information Technology Handbook, (USG Information Technology Handbook, version 2.5, section 5.1, 2017). ASU is required to establish and maintain appropriate internal policies, processes, standards, and procedures in order uphold the confidentiality, integrity, and availability of the information and the resources used to process or store information. These policies, processes, standards, and procedures are paramount to computing at ASU.

Purpose

This Enterprise Information Security policy and associated detailed policies are intended to provide a comprehensive set of security guidelines that will ensure that all is being reasonably done to provide appropriate and consistent protection of the University's information systems assets.

Scope

The Enterprise Information Security policy applies to all individuals utilizing University technology resources, including but not limited to students, faculty, staff, external contractors, affiliates, and visitors. Additionally, any remote access (e.g., ISP access, VPN connection, etc.) onto the ASU enterprise network or associated domains will have the same effect as direct access via ASU-provided equipment or facilities.

Policy

- ASU must do what is reasonably possible to protect its information systems assets from anything except authorized and intended use.

- ASU must do what is reasonably possible to ensure the confidentiality, Integrity and availability of the information assets that support its mission and goals.

- ASU must operate in accordance with all applicable federal, state, and local laws.

Definitions (Optional)

Definitions associated with this policy are available in the Information Technology and Data Security Terms Glossary.

Procedures

As required by information in References Section and the associated detailed policies.

Accountability

The entire University community (students, faculty, staff, external contractors, retirees, and visitors) are responsible for protecting ASU's information assets and for using its resources in an effective, efficient, ethical, and lawful manner.

The individual policies and procedures address key areas of information security and, when combined, provide for an extensive framework that supports the open use of technology while also protecting ASU's critical information assets. Every person handling information or using University information systems must adhere to information security policies and procedures.

Exceptions

Exceptions to the ASU VPN Remote Access Policy, other than those previously discussed, are evaluated on a case-by-case basis by the Vice President and Chief Information Officer.

Contacts

Responsible Office**:**	Office of Vice President of Information Technology Services & Chief Information Officer (CIO)
Contact Information:	Information Technology Services Office of Information Security Phone: 229-430-3006 Email: infosec@asurams.edu

References

USG Information Technology Handbook, version 2.5, section 5.1, 2017: http://www.usg.edu/information_technology_services/it_handbook/

Last Update

July 31, 2018