ACCEPTABLE USE POLICY (AUP)

Area:	Information Technology	Number:	
Applies to:	University Community	Issued:	November 11, 2010
Sources:		Revised:	May 18, 2020
		Reviewed:	
Policy Owner:	Chief Information Officer	Page(s):	2

I. Purpose

This policy establishes that Georgia Southern and its users have an obligation to abide by standards that support the appropriate and ethical use of University resources. The use of these resources is a privilege granted by Georgia Southern University to authorized users only. This policy defines acceptable technology and information use practices, promotes an understanding of responsible use of university IT resources, seeks to protect the University's IT resources, and preserves the relevant policies, regulations and laws. The policy is not intended to be exhaustive, and Georgia Southern University reserves the right to limit, restrict, or extend privileges and access to its information technology resources.

This policy will be administered and enforced by the Chief Information Officer or duly authorized designee.

II. Policy Statement

Georgia Southern University provides access to technology resources for students, faculty, staff, and other users as authorized by the University. The technology resources of Georgia Southern University, including but not limited to, facilities, hardware, software, networks, data, information, and user accounts, are the property of Georgia Southern and should not be used in a manner that violates university policies, state and federal laws, and all contractual and license agreements.

III. Exclusions

There are no exclusions or exceptions to this policy.

IV. Procedures

The following guidelines establish the obligation by which the institution and users must abide to promote ethical and appropriate use of campus resources.

- Use only those resources for which you have authorization.
- Use of any university information technology resource is restricted to those having proper authorization to use that resource. It is a violation of the law and university policy to assist in, encourage, or conceal from authorities any unauthorized use, or attempted unauthorized

use, of any of the University's computers or network facilities.

- Passwords to any information technology resource shall only be issued to authorized users. Password recipients are responsible for the protection of their access credentials and shall not distribute them to other users.
- Protect the access and integrity of those resources.
- Users must take appropriate steps to secure protected, confidential and sensitive information, including personal identifying information such as social security numbers and birth dates.
- Abide by all applicable local, state, and federal laws and University policy in respect to copyrights and intellectual property rights of others.
- Use resources for their intended purpose.
- University information technology resources shall not be used for personal political gain or as a vehicle of election to a public office.
- Respect the privacy and personal rights of others.
- Do no harm.

Georgia Southern University will handle reports of misuse and abuse of information and information technology resources in accordance with existing policies and procedures issued by appropriate authorities. Depending on the individual and circumstances involved this could include the offices of Human Resources, Provost, Dean of Students, Legal Affairs, and/or appropriate law enforcement agencies.

Failure to comply with Georgia Southern University information technology policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

If the determination of relation to the mission or determination of incidental personal use is unclear, the Chief Information Security Officer will coordinate with campus administration and the unit involved to help determine whether the activity in question is an appropriate use of resources.