Policy 5.1

Information Technology Conditions of Use

Responsible Official:	Enterprise CIO and Sr. Vice Provost, Information Technology
Administering Division/Department:	Office of Information Technology
Effective Date:	March 31, 2007
Last Revision Date:	September 29, 2022

Policy Sections:

Overview

Computers, networks, and software applications are powerful tools that can facilitate Emory's core missions in teaching, learning, research, and service. Access and utilization of these tools is a privilege to which all University faculty, staff, students, and authorized guests are entitled. This policy documents the responsibilities that accompany

Policy Details

General Principles:

- Emory's information technology (IT) resources are provided for uses consistent with the University's missions of teaching, learning, research, and service or for related administrative support.
- The use of Emory's IT resources must be consistent with other University policies, government regulations and laws.
- IT resources are not to be used for private financial gain or for supporting non-Emory related businesses.
- Users of Emory IT resources are expected to read and abide by all relevant IT policies and standards and to complete any prescribed IT security training.

Information Security Requirements:

- Users of Emory's IT resources may not:

  Share their passwords or other access credentials;
  Attempt to hack, bypass, or violate security controls or conduct unauthorized testing of IT resources for security vulnerabilities;
  Access, modify, or share sensitive data or information obtained fromrma5480lac[V6t7ies;

Personal Usage:

- Limited and reasonable personal use of Emory's IT resources is acceptable and allowed, as long as it does not:

  Interfere with the fulfillment of an employee's responsibilities;
  Adversely impact or conflict with any activities that support Emory's mission or operations;
  Result in any measurable cost to Emory;
  Violate any other applicable University policies.

Network Protection and Monitoring:

- Authorized Emory staff may without notice:
  Monitor, inspect, or copy network communications, IT resources, and the data they contain. Use of the Emory network and/or IT resources constitutes consent to such monitoring;
  Assess IT resources connected to the Emory network for security vulnerabilities;
  Take emergency protective actions such as restricting user access rights or access to IT resources or the network;
  Block potentially malicious network communications;
  Block the viewing, downloading, or distribution of any content to the extent that doing so is required by federal or state law, regulation, or policy, or is required to carry out Emory's mission or operations.

Sanctions:

- Failure to comply with this policy may have legal consequences and may result in:

  Suspension or termination of access;
  Disciplinary actions (up to and including termination of employment) in accordance with applicable university policy.

Definitions

Related Links

- Current Version of This Policy:

Subject	Contact	Phone	Email
Clarification of Policy	Brad Sanford	404-727-2630	brad.sanford@emory.edu

Revision History

- Version Published on: Sep 29, 2022 *(Updated Responsible Official and Administering Division)*
- Version Published on: Jul 07, 2017 *(Incorporation of changes requested by OGC)*
- Version Published on: Mar 13, 2016 *(Updated web links)*
- Version Published on: Mar 15, 2011 *(Major Revision / Re-write)*
- Version Published on: Mar 29, 2007 *(Original Publication)*