ACCEPTABLE USE OF COMPUTING AND ELECTRONIC RESOURCES

The University of North Carolina at Greensboro

Approved by the Chancellor, 05/13/1998

Revised, 08/09/2021

1. PURPOSE

The purpose of this policy is to outline the acceptable use of information systems and information systems infrastructure owned or provided by The University of North Carolina at Greensboro (hereinafter "the University") or which contain University information assets, or which utilize the information system infrastructure maintained by the University.

2. SCOPE

This policy applies to all users of information systems owned or provided by the University; all users of information systems which contain University information assets; and all users of systems that utilize the University information system infrastructure, even if the systems are not University property.

3. DEFINITIONS AND ROLES AND RESPONSIBILITIES

3.1 DEFINITIONS

Information System is a set of programs on an electronic device that process or store data for the use of an individual or organization, and the hardware on which the programs operate. (Common examples include accounting software, database systems, servers, workstations, smart phones, etc.)

Information System Infrastructure is the physical and software systems necessary for the support and operation of information systems. (Common examples include authentication services, networking services, power backup services, etc.)

Administrative Control includes protecting a system through policy, procedure, training, directives from an authority, or similar efforts which instruct and require individuals to take correct actions.

3.2   ROLES AND RESPONSIBILITIES

Chief Information Security Officer is responsible for providing interpretation of this and other related policies and disseminating related information.

System Administrators, Developers and Integrators are responsible for the application of this and related policies to the systems, information, and other information resources in their care.

Users of the University's information resources are responsible for the application of this and related policies to the systems, information, and other information resources which they use, access, transmit or store.

Third-party Affiliates with access to University systems and/or facilities are expected to abide by the University's information security and privacy policies.

Information Technology Services (hereinafter "ITS") is charged with providing the information system infrastructure of the University. Prior approval from ITS is required to utilize an information system infrastructure other than the one maintained by ITS. Users of such systems must self-identify their information system infrastructure inventory with ITS on an annual basis, or upon ITS request.

4.   POLICY

Individuals subject to this policy are responsible for exercising good judgment regarding the use of technology and information systems. Use of these systems is permitted, with the following restrictions and conditions:

a. The use is lawful and not prohibited by University of North Carolina Board of Governors or University policies, including but not limited to those regarding academic integrity, harassment, discrimination, copyright, trademark, patent and invention, and use of State property for private gain, and political activity as published in Section 300.5.1 (https://www.northcarolina.edu/apps/policy/doc.php?id=125) of the UNC System Policy Manual.

b. The use does not violate administrative controls or contractual agreements such as terms-of-use that the University and/or user is subject to.

c. The use does not negatively impact other information systems or information system infrastructure.

d. The use does not circumvent administrative controls or in any way attempt to gain or provide unauthorized access to information systems or data.

e. No user shall send unsolicited mass communications without proper authorization from the manager with jurisdiction over the population to be reached. This includes the sending of "spam" (junk e-mail) or other commercial advertising material to individuals.

f. UNC Greensboro-maintained computing and electronic resources exist to conduct University business. Although reasonable and limited personal use is not prohibited by this policy, such use must not violate University policies, University codes of conduct, or State or Federal law. Any limited personal use of University-maintained computing and/or electronic resources must not interfere with an employee's job performance or activities which directly support the University mission, and unit managers have discretion to further restrict or forbid personal use as they reasonably deem necessary.

g. All use of University information systems must be identified as to the individual or device using the system. Obfuscation or misrepresentation of identity (e.g. shared credentials, spoofed communications, etc.) for any purpose, including the access and use of information systems, is prohibited.

h. Other Conditions of Use:

- By activating one's University computer account, one agrees to receive via email University security breach notifications covered by the N.C. Identity Theft Protection Act and other official University communication.

- All data created or received for work purposes are public records. Public Records are available to the public upon request, unless subject to an exception in the Public Records Act or protected by another law. Additional information can be found in the University's Public Records Policy. (https://policy.uncg.edu/university_policies/public-records-policy-2/) All public records are to be maintained and disposed of according to state approved records retention and disposition schedules.

- No University employee, student or any other user shall have any expectation of privacy in the material or information sent or received using any portion of the University information system infrastructure, information systems, or systems containing

University information assets. For security, legal, investigative, policy compliance, quality of service, and infrastructure maintenance purposes, authorized employees within ITS, and those University employees outside ITS with responsibilities necessitating access, may monitor information system and infrastructure activity and/or content, in the course of discharging their duties. Such duties are carried out in accordance with University policy governing Data Classification (https://policy.uncg.edu/university-policies/data/) and Access to and Retention of Research Data (https://policy.uncg.edu/university-policies/research_data/).

5. COMPLIANCE AND ENFORCEMENT

ITS, in cooperation with other University authorities and administrators, will enforce this Policy, and establish standards, procedures, and protocols in support of the policy.

Any violation of this policy by a University student is subject to the Student Code of Conduct in the Student Policy Handbook. For employees, violation of this policy will be subject to consideration as "misconduct" under EHRA policies (faculty and EHRA non-faculty) or "unacceptable personal conduct" under SHRA policies, including any appeal rights stated therein.

If violation of the policy also results in a violation of law, the violation may also be referred for criminal or civil prosecution.

Additionally, violations of this policy may result in termination or suspension of access, in whole or in part, to University information systems at the discretion of ITS where such action is reasonable to protect the University or the University information infrastructure.

6. ADDITIONAL INFORMATION

6.1 SUPPORTING DOCUMENTS

n/a

6.2 RELATED POLICIES

- Information Security Policy (https://policy.uncg.edu/university_policies/information-security/)
- Data Classification Policy (https://policy.uncg.edu/university-policies/data/)

- Enterprise Systems Policy (https://policy.uncg.edu/university-policies/enterprise_systems/)
- Computing Supported Products (Standards for Computer and Related Technology) (https://policy.uncg.edu/university-policies/technology_standards/)
- Electronic Records Retention Policy (https://policy.uncg.edu/university-policies/electronic_records/)
- Canvas Use Policy (https://policy.uncg.edu/university-policies/canvas/)
- Copyright Compliance for Users of UNCG Technology (https://policy.uncg.edu/university-policies/copyright_compliance/)
- Public Records (https://policy.uncg.edu/university_policies/public-records-policy-2/)
- Student Policy Handbook (https://osrr.uncg.edu/wp-content/uploads/2020/09/Student-Code-of-Conduct-8-27-2020-1.pdf)

6.3   RESOURCES

- UNCG Public Records information website (https://generalcounsel.uncg.edu/public-records/)

6.4   APPROVAL AUTHORITY

The Chancellor is responsible for approval of this Policy.

6.5   ADDITIONAL CONTACTS FOR INFORMATION AND REPORTING

● Responsible Executive: Donna R. Heath, Vice Chancellor for Information Technology Services and Chief Information Officer (CIO), drheath@uncg.edu

● Responsible Administrator: Casey J. Forrest, Chief Information Security Officer (CISO), cjforrest@uncg.edu

REVISIONS

Revision Date	Revision Summary
05/13/1998	Formerly Computer Use Policy for University Employees and Computer Use Policy for University Students
07/19/2004	
03/10/2009	

Revision Date	Revision Summary
08/09/2021	