REG 08.00.02 – Computer Use Regulation

Authority: Issued by the Chancellor. Changes or exceptions to administrative regulations issued by the Chancellor may only be made by the Chancellor.

History: First Issued: January 8, 1999. Last Revised: February 19, 2019.

Related Policies:

NCSU POL 08.00.01 – Computer Use

NCSU REG 01.25.02 – Copyright Infringement Policy Statement

NCSU REG01.25.12 – University Record Retention & Disposition Regulation

NCSU REG 07.30.14 – Home Use of Equipment

NCSU REG 08.00.03 – Data Management Procedures

NCSU REG 01.25.05 – Procedure for Formatting, Adopting, and Publishing Policies, Regulations, and Rules (PRR Protocol)

NCSU REG – 08.00.10 Anti-Virus Software Requirements

NCSU RUL 02.61.02 – Confidentiality of Library Records and Data

Additional References:

Computer Use Regulation Summary and Use Guidelines

NCSU Trademark Licensing Office

NCSU Administrative Password Standard

NCSU Mobile Device Security Guidelines

Advancement Data Use & Donor Privacy Guidelines

Contact Info: Director of Security & Compliance, Office of Information Technology (919-513-1194)

1. INTRODUCTION

North Carolina State University's (hereinafter "University") Information Technology (IT) resources consist of assets such as computer equipment, software, networks, computer system accounts and other digital assets and resources that primarily support the academic and administrative functions of the University. These assets are either owned by the University or used by the University under contract with an external provider. The use of these assets are governed by federal and state laws as well as University policies, regulations and rules

2. GENERAL USE OF IT RESOURCES AND REGULATORY LIMITATIONS

2.1. University computer accounts are for the exclusive use of the individual to whom they were assigned, and users may not allow or facilitate unauthorized access to University computer accounts or IT resources by others. For example, users may not allow unauthorized access to restricted resources by sharing their password or by setting up a web proxy, an anonymous remailer or other methods.

2.1.1. Students and employees of the University receive computer accounts and are authorized users of IT resources unless access privileges have been revoked under University procedures.

2.1.2. Departments may establish guest and temporary accounts for authorized use of University IT resources by non-university personnel. The department that is responsible for the guest and temporary accounts must ensure that **NCSU POL08.00.01 – Computer Use Policy** and this regulation is understood and adhered to by the users of the accounts.

2.2. Use of University IT resources must comply with federal and state laws, and University policies, regulations and rules.

2.3. Use of IT Resources provided to the University under a contract with an external provider are also subject to the terms and conditions of the contract with the provider.

2.4. The University may examine the content of both personal and work-related electronic information stored or archived on University IT resources. The examination may be requested by the Chancellor, a Vice Chancellor or a Dean (or their delegates) and then approved by the Vice Chancellor for Information Technology and/or the Vice Chancellor and General Counsel. In addition, the University Internal Auditor, in accordance with NC General Statute §116-40.7(b) and the Internal Audit Charter, shall have unrestricted, independent access to examine any records, data, or information of the University or constituent institutions that the internal auditor believes to be necessary to carry out the internal auditor's duties. An examination of these records may be undertaken for any of the following purposes:

2.4.1. To ensure the security and operating performance of its IT resources.

2.4.2. To ensure compliance with University policies, regulations or rules, or state or federal law.

2.4.3. To perform audit-related activities.

2.4.4. To comply with E-discovery rules relating to an actual, threatened or potential lawsuit, with a subpoena, or with other court orders.

2.4.5 To address an imminent threat to health or safety.

2.4.6. To conduct authorized University investigations.

2.5. Computer users should have no expectation of privacy with regard to any*personal* material stored or archived on University IT resources. Although University staff will respect personal privacy where practical, users who want to ensure that their personal materials are not subject to university access are advised to use their own personal, non-university equipment, networks and storage. .

2.5.1 Computer users should have no expectation of privacy with regard to any University records/data stored on, archived on, or passing over personal IT resources. University staff will respect personal privacy where practical; however, the University may monitor and examine personal IT resources which contain University records/data for the reasons specified above in Section 2.4. This includes, but is not limited to, the application of Section 6.3 of this Regulation.

2.6. The University may authorize confidential passwords or other secure access identification.

2.7 The University may use active measures to detect compromised machines and identify vulnerable services so long as the active methods are low risk and concerns are reported to appropriate users.

2.8. For information related to university business, a supervisor or other designated university official may have appropriate access for work-related purposes. No permission or approval from the user is needed for such access. If personal and business information are not clearly separated, the designated university official may examine all information to the extent needed to separate and access business information for work-related purposes. Deans, Vice Chancellors and Vice Provosts may approve rules to exclude personal files from storage on network drives, in which case all files and data on the affected systems may be treated as information related to University business.

2.9. Authorized University personnel may examine server/desktop "log" information to identify computer users and the electronic addresses to which they have connected (e.g., Web sites or e-mail) to the extent consistent with privacy laws and necessary for University business purposes.

2.10. The University reserves the right to limit or revoke access to University IT resources when University policies, regulations or rules, or state or federal law are violated or where University contractual obligations or University operations may be impeded. Attempts will be made to notify the affected user(s).

2.11. All material prepared and utilized for purposes of University business and posted to or sent over University IT resources must be accurate and must correctly identify the sender, unless a University administrator (department head or higher) approves anonymity for a University business purpose.

2.12. Any traffic on the University's IT resources may be monitored by designated university personnel for research purposes. Access to information content should be consistent with University policies, regulations or rules, or state or federal law, and the purpose for which the traffic is being monitored.

2.13. When conducting University business, employees' e-mail signature lines should contain job-related information such as name, job title, professional credentials, office location, mailing address, and telephone number, and may include University slogans, statements and branding.

2.14. University computers must be registered with NC State in University-approved domains. It is prohibited to register a non-University approved domain for any computer that is connected to the NC State network without approval of the Vice Chancellor for Information Technology or his/her designee. If such approval is given, it must be made clear that this domain is using NC State IT resources for delivery.

2.15 Software will be used only in accordance with its license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup or archival purposes, may be a violation of copyright law. Requirements and procedures related to departmental software licensing are further discussed in Section 7.

2.16. Users of IT resources, including computer systems, must take appropriate security precautions to protect and secure data residing in or on assigned university accounts or other IT resources. These precautions include ensuring that security patches are applied to software products, and adhering to any university security guidelines, standards or regulations for any device (university-owned or personal) that accesses university data and services. A violation of any University security guideline, standard or regulation shall be considered a violation of this regulation as outlined in Section 5.

3. PERSONAL USE OF IT RESOURCES

3.1. Authorized users may access University IT resources for occasional, inconsequential personal uses, with no expectation of privacy, if the following conditions are met:

3.1.1. The use does not disrupt, negatively impact, or interfere with the security, functions, availability or performance of University IT resources (such uses including, but not limited to, network overload, spam email, or excessive, simultaneous video streams).

3.1.2. The use does not otherwise negatively inhibit, impact or detract from the authorized users' work performance or the work performance of other employees.

3.1.3. The use does not seek or result in a university employee's commercial gain or private profit, except as allowed under applicable University intellectual property or external activities for pay regulations.

3.1.4. The use does not violate any University licensing agreements or any law or University policy on copyright and trademark.

3.1.5. The user exercises care not to communicate or imply that they are acting as a representative of, or expressing the views of the University.

3.1.6. The use does not otherwise violate University policies, regulations or rules, or state or federal law.

3.1.7. The use does not involve unauthorized passwords or the abuse of identifying data and/or tools that attempt to circumvent system security or that in any way attempt to gain unauthorized access.

3.1.8. The use does not result in any direct cost to the University.

3.1.9. Any creation of a personal World Wide Web (WWW) page or a personal collection of electronic material that is available to others must include a disclaimer that reads as follows:

"The material located at this site is not endorsed, sponsored or provided by or on behalf of North Carolina State University."

4. USE OF IT RESOURCES FOR COMMERCIAL, ADVERTISING AND BROADCAST PURPOSES

4.1. No paid advertising will be allowed on official University web sites. However, an NC State web site may contain a simple acknowledgment of sponsorship by an outside entity in the following form: "Support for this web site [or university unit] has been provided by _____." The acknowledgment may include the sponsorship's logo only if permission is granted by the sponsor, and the use of the logo does not imply commercial endorsement by the University.

4.1.1. An "official University web site" is any World Wide Web (WWW) address that is sponsored, endorsed or created on authority of a University department or administrative unit. Web sites on University servers are either "University web sites" or personal web sites allowed by the University.

4.1.2. "Paid advertising" means advertising or promotional information provided in exchange for legal consideration, including money or other valuable benefits.

4.2. Personal web pages that are hosted on University-owned computers may not contain paid advertising.

4.3. While University employees may post messages to newsgroups, blogs, chatrooms or other Internet resources dedicated to advertising, the messages may not refer readers to a University telephone number or university e-mail address.

4.4. University computer account holders may not "broadcast" e-mail messages without prior approval from the Chancellor, Provost, Vice Chancellor for Finance and Administration, Vice Chancellor for Information Technology or their designees. "Broadcast" means transmission of an unsolicited message to a significant number of computer accounts on a University server or servers; the intent is to prevent mass mailings from tying up employee time and computer resources. The use of e-mails by university units to reach their constituency will not be considered "broadcast" e-mail under this section. The use of authorized university e-mail lists for their intended purpose will not be considered "broadcast" e-mail under this section.

4.5. Registered marks of the University as designated by the NCSU Trademark Licensing Office may be used in the Web sites of University computer account holders on the conditions that (a) they are not used for or related to private profit or commercial purposes, and (b) they do not mislead or confuse viewers as to whether the Web page is University-sponsored.

4.6. The Chancellor or designee may approve specific exceptions to the prohibition on paid advertising.

5. VIOLATION OF POLICIES, REGULATIONS OR RULES

5.1. Any violation of applicable policies, regulations or rules regarding use of IT Resources by employees may be "misconduct" under EHRA policies (faculty and EHRA non-faculty), or "unacceptable personal conduct" under SHRA policies. For students, violations are "misconduct" under the applicable student disciplinary code. For approved guests, violations will result in appropriate action depending on their affiliation. Violators are subject to appropriate disciplinary procedure, and violations of law may also be referred for criminal or civil prosecution. Sanctions may include revocation of access privileges in addition to other sanctions available under the regular disciplinary policies.

5.2. Apart from disciplinary procedures, an authorized University system administrator (or designees such as the system administrator's supervisor or a university Help Desk representative) may suspend a user's access privileges or suspend services to a computer for as long as necessary to protect the University's IT resources, to prevent an ongoing threat of

harm to persons or property, or to prevent a threat of interference with normal University functions. As soon as practicable following the suspension of access privileges, the system administrator must take the following actions:

5.2.1. The user must be sent written or electronic notice of the suspension of access and the reasons for it, along with notice of the time, date, location and person with which the suspension may be discussed.

5.2.2. The user must be given an opportunity to meet with the system administrator or his/her designee in a timely manner to discuss the suspension and present any reasons the user has why the suspension should be lifted. The system administrator must reconsider his or her suspension decision in light of the information received at this meeting.

5.2.3. Following the meeting, the user must be sent a written or electronic copy of the system administrator's decision upon reconsideration, and must be notified that he/she may appeal to the system administrator's immediate supervisor if the user is dissatisfied with the outcome of the meeting.

6. APPLICATION OF PUBLIC RECORDS LAW

6.1. Duty to preserve records: All information created or received for University work purposes and contained on University IT resources, University electronic mail (e-mail) systems, or on privately owned devices are public records and are available to the public unless an exception to the applicable public records law applies. As with hard-copy documents, e-mail users are responsible for the retention of e-mail messages that have lasting or archival value in accordance with applicable public records law and NC State University's published guidelines regarding records retention and disposition. This personal responsibility is heightened when a user sends or receives email that requires permanent or long-term retention that exceeds the retention period used by a University centralized email archive.

6.2. Additional duty regarding records requests and potential litigation: Any University employee or authorized guest (e.g., volunteers and students serving in a University office) who receives notice of a public record request, possible lawsuit or other legal claim must promptly (a) notify the Office of General Counsel of the request or possible claim and (b) locate and preserve all relevant records.

6.3. Duty to provide access to information content: Employees and approved guests with a network account or University computing device must provide appropriate assistance for access to information content (including decryption and entry of passwords). This assistance should only be provided when an identified University official (e.g., supervisor, person in employee's supervisory hierarchy) needs access to any of the University's records/data the employee may have stored on University machines, systems or storage devices, or on non-university machines, systems or storage devices. Any failure to provide an identified University official access to information content on University machines, systems or storage devices, or non-university machines, systems or storage devices that may contain the University's records/data shall be considered a violation of this regulation as outlined in Section 5.

7. SOFTWARE LICENSING REQUIREMENTS AND PROCEDURES

7.1. It is the responsibility of each department to maintain proof of licensing for all software utilized in their department including those packages supported by the Office of Information Technology, Security and Compliance (S&C) unit.

7.2. Licenses for software supported by S&C may be obtained via the S&C website. Departments will be issued IDTs to reimburse S&C for the purchase of the applicable software licenses. These IDTs will serve as the department's proof of license.

8. ADDITIONAL RULES

8.1. Additional rules on computer use may be adopted by various divisions/departments to meet specific administrative or academic needs. Any adopted requirement must:

8.1.1. Comply with applicable federal and state laws;

8.1.2. Be consistent with the policies and regulations of NC State University and the University of North Carolina;

8.1.3. Be adopted and posted in writing or electronically in a manner that is available to all affected users in accordance with NCSU REG 01.25.05 – Procedure for Formatting, Adopting, and Publishing Policies, Regulations, and Rules (PRR Protocol); and

8.1.4. Be filed with the General Counsel and the Vice Chancellor for Information Technology.

Audience: Faculty, Staff, and Students.
Category: Information Technology.

Policies, Regulations & Rules

NC STATE UNIVERSITY

NORTH CAROLINA STATE UNIVERSITY

RALEIGH, NC 27695

919.515.2011