

## REG 08.00.02 – Use of IT Resources 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: December 10, 2024.

### Related Policies:

**POL 08.00.01 – Use of IT Policy**

**REG 04.25.05 – Information and Communication Technology**

**Accessibility**

**REG 08.00.03 – Data Management Regulation**

**REG 08.00.10 – Anti-Virus Software Requirements**

**REG 08.00.11 – Online Course Material Host Requirements**

**RUL 08.00.13 – Network Printer Security Standard**

**RUL 08.00.14 – System and Software Security Patching Standard**

**RUL 08.00.15 – Third-Level URL Naming Standard**

**RUL 08.00.16 – NC State University Security Standards for Sensitive Data and Systems**

**RUL 08.00.17 – Cybersecurity Incident Response Procedure**

**RUL 08.00.18 – Endpoint Protection Standard**

**REG 11.00.01 – Family Educational Rights and Privacy (FERPA)**

**NC Law Governing Privacy of Employee Personal Records (N.C.G.S. Chapter 115C Article 21.A)**

**NC State Privacy Statement**

### Additional References:

**FAQ – Use of IT Resources Regulation**

Contact Info: Chief Information Security Officer, Office of Information Technology ([security@help.ncsu.edu](mailto:security@help.ncsu.edu))

### 1. Purpose

1.1. The purpose of this Regulation is to support, further define and implement **POL 08.00.01 – Use of Information Technology** at NC State University, hereinafter referred to as “NC State” or “the university.”

1.2. IT Resources: This Regulation specifies acceptable uses of the university’s Information Technology Resources (hereafter referred to as “IT Resources”) as defined in POL 08.00.01, which refers to all relevant regulatory and institutional responsibilities and specifies the potential consequences for violating this Regulation.

- 1.2.1. IT Resources. According to the Use of IT Resources Policy, “IT Resources” means any information technology resources (hardware, software and content including but not limited to electronic networks, systems, computers, devices, telephones, applications, data, and files residing in any of these) that are used for university purposes, regardless of whether owned by the university, a third party or personally owned.

## 2. Scope

This Regulation governs the use of all IT Resources and applies to Covered Individuals, which includes all faculty, staff, students and anyone with access to IT Resources. For the purposes of clarity, this Regulation applies to third party and personally owned devices to the extent they are included in the [POL 08.00.01 definition of IT Resources](#).

## 3. Regulation Statement

All use of IT Resources must comply with all applicable statutes, rules and regulations (U.S. and foreign); university obligations to vendors or other third parties; and all university [Policies, Regulations and Rules \(PRRs\)](#).

## 4. Account Holder Responsibilities

4.1. Users of IT Resources must take appropriate information security precautions to protect and secure university data – regardless of location –, as identified in Section 3, Regulation.

4.2. University accounts are to be used only by authorized account holders, and account holders must not allow or assist with unauthorized access – neither to their accounts nor any university IT Resources.

4.3. Individuals are responsible for promptly reporting the theft, loss or unauthorized disclosure of university information.

4.4. Account holders are responsible for all activities performed with their accounts, and must promptly report any suspected compromise of their accounts.

4.5. Individuals are allowed access only to the IT Resources required to perform their duties and roles.

4.6. Departments may request guest and temporary accounts for authorized use of IT Resources by non-university individuals. The department that requested the guest or temporary accounts must ensure that its account users understand and adhere to NC State [POL 08.00.01](#) as well as this Regulation.

## 5. Privacy and Monitoring

5.1. The university respects all statutes, rules and regulations governing privacy. The university also has a legal obligation to manage data, information, and public records created in the course of conducting university business. Therefore, users should have no expectation of privacy when using IT Resources, as the university has an obligation to access university records as set forth in Section 5.3 and could access personal information that is used on IT Resources.

Users who want to ensure that the university does not access their personal information are advised to refrain from using university-owned devices to conduct personal business and also to refrain from using their personal devices to conduct university business.

5.2. The university has the right to examine content on all IT Resources, regardless of ownership.

5.3. The university may access any IT Resource for the following purposes:

- 5.3.1 University internal auditors – in accordance with NC General Statute §116-40.7(b) and the Internal Audit Charter – have unrestricted, independent access to examine any relevant records, data, or university information that the internal auditor deems necessary to carry out the internal auditor’s duties.
- 5.3.2 To ensure the security and operating performance of the IT Resources.
- 5.3.3 To ensure compliance with any items in Section 3, Regulation.
- 5.3.4 To comply with discovery rules relating to an actual, threatened, or potential lawsuit; a subpoena; or a court order.
- 5.3.5 To address an immediate or imminent threat to health, safety or interruption to university operations.
- 5.3.6 To process public records requests.
- 5.3.7 Supervisors have the authority to access university-owned IT Resources of their employees to the extent reasonably necessary for business-continuity purposes. Employees shall work with their supervisors to provide access to their personally owned IT Resources only to the extent necessary to access university-owned data.
- 5.3.8 To conduct official university investigations.
- 5.3.9 For other examinations requested by a Vice Chancellor or a Dean and then approved by the Vice Chancellor for Information Technology (or their delegate, as documented in writing) or the Chancellor, in consultation with the Vice Chancellor and General Counsel.

## 6. Asset and Data Management

6.1. University-owned IT Resources must be registered and maintained within an inventory management system of record approved by the Vice Chancellor for Information Technology. Exceptions must be submitted to Security and Compliance per Section 12, Exceptions.

6.2. Sensitive data, as defined in REG 08.00.03 – [Data Management Regulation](#), must be stored only in locations authorized by the associated data stewards.

6.3. The university reserves the right to limit or remove access to IT Resources in order to adhere to Section 3, Regulation.

## 7. Email

7.1. Users must maintain and use only university email accounts for university business and not use any personal account to conduct university business.

7.1.1. Enter and keep an official university email address (and not a personal account) as their business email in the university directory.

7.1.2. Auto-forwarding between university email accounts is allowed. Auto-forwarding to personal accounts is not allowed. Users may forward individual messages to any email address if they follow university policies, standards, and procedures.

Note: Dual appointments should be submitted for an exception.

7.2. All written content used for university business and communicated via IT Resources must be accurate and identify the sender correctly. Exceptions to this requirement are permitted when one of the following authorities approves an alternate name or title for a university business purpose:

- 7.2.1. Dean, department head or director
- 7.2.2. Associate Vice Chancellor, Vice Chancellor or Chancellor

7.3. When conducting university business, employee email signatures must contain only job-related information. All signature blocks must be consistent with official [university branding guidelines](#).

7.4. IT Resource account holders may broadcast an email message only for a work-related need.

## **8. Personal Use of University-owned IT Resources**

8.1. Users may use IT Resources for occasional, inconsequential personal use without any expectation of privacy, provided they comply with the following conditions:

- 8.1.1. The use must not disrupt, negatively impact, or interfere with the information security, functionality, availability or performance of IT Resources.
- 8.1.2. The use must not negatively inhibit, impact or detract from the authorized individual's work performance or the work performance of others.
- 8.1.3. The use must not seek or result in a university employee's commercial gain or private profit.
- 8.1.4. The use must not violate the regulation statement above (Section 3).
- 8.1.5. The use must not state or imply that they are acting as a representative of, or expressing views on behalf of, the university.
- 8.1.6. The use must not result in any direct cost to the university.
- 8.1.7. Any personal web pages or personal collections of electronic material made available to others must include this disclaimer: "The material located on this site is not endorsed, sponsored or provided by or on behalf of North Carolina State University."
- 8.1.8. Personal websites hosted on university-owned IT Resources must not be used for commercial purposes.

8.2. If a user leaves the university for any reason, including death, they or their representatives will not have any access to that personal information.

8.3. Employees (faculty and staff) are prohibited from viewing pornography on any university device and on the university's network. Students are prohibited from viewing pornography on any university devices.

Note: Please see N.C. General Statute § 143-805 for the definition of pornography and allowed exemptions including research and other university functions.

## **9. Use of IT Resources for Commercial and Advertising Purposes**

9.1. Use of IT Resources for paid advertising or commercial purposes is allowed only for authorized university business and must include the ability for recipients to opt out of future communication.

## 10. IT Resource Licensing Requirements

10.1. Each unit is responsible for maintaining proof of licensing for their IT Resources unless another unit has licensed the IT Resources on their behalf. Regardless of who manages the licenses, each unit must maintain records of usage where required by the agreement or license.

10.2. As stated in Section 3, "Regulation," Covered Individuals are responsible for understanding the terms of all applicable licensing requirements.

10.3. University-owned IT Resource licenses must be approved by the Office of Information Technology and are subject to [Procurement and Business Services](#) rules, regardless of cost.

## 11. Application of Public Records Law

11.1. The university is required by [North Carolina Public Records law \(N.C.G.S. 132-1\)](#) to maintain all Public Records in accordance with the [UNC System Records Retention and Disposition Schedule](#).

11.2. Covered Individuals are required to maintain all records, documents, data, emails, and any information created or received for university business purposes, whether processed or stored on university devices, personal devices, or any devices owned by a third party.

11.3. Covered Individuals must provide access to items (including decryption and entry of passwords) when requested by a university official (for example, a supervisor, a University Records Officer or other university administrator) to meet public records law requirements.

## 12. Exceptions

12.1. Exception requests must be submitted in writing to the IT Exception process, where criteria questions are answered that would then route to the appropriate stakeholder(s) and approver(s). They must state the following at a minimum:

- 12.1.1 The requirement(s) that need an exception
- 12.1.2 Any compensating controls that are in place which will mitigate risk of unmet requirements
- 12.1.3 The duration requested for the exception, not to exceed 1 year

12.2. Any exceptions that are approved must be re-submitted annually if they are needed for more than one year.

## 13. Glossary

13.1. Acronyms

- **IT:** Information Technology
- **PRR:** [Policies, Regulations and Rules](#)

13.2. Term Definitions

- **Broadcast.** The transmission of a message to a large number of people, for example, an email or text message.

- **Covered Individuals.** All faculty, staff, students and individuals with any access to IT Resources.
- **Paid Advertising.** Advertising or promotional information provided in exchange for money or other benefits; excludes simple acknowledgment of sponsorship by an outside entity.
- **Public Records.** All records made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions. Such records may include documents; papers; letters; maps; books; photographs; films; sound recordings; electronic records such as emails, text messages, instant messages, databases, calendars and other documents or communications that exist in an electronic format; magnetic or other tapes; and artifacts or other documentary material, regardless of physical form or characteristics. Excludes personal records such as personal email messages.
- **IT Resources.** See [POL 08.00.01](#) for definition.