INFORMATION SECURITY
07.300.00

Authority:	Board of Trustees
History:	Approved by the Board of Trustees February 8, 2019; Approved by the Board of Trustees August 3, 2007; revised July 18, 2007; reformatted May 25, 2005; approved by the Board of Trustees October 28, 2004; effective October 28, 2004.
Source of Authority:	UNC System Office Policy Manual, Chapter 1400 "Information Technology" International Organization for Standardization ISO/IEC 27002
Responsible Office:	Information Technology Services

I. Purpose

A. This document states the overarching policies for the security of the University of North Carolina Wilmington's information resources. This is not a comprehensive document covering all aspects of information security, but instead focuses on a select set of core controls vital to the campus community. These policies are intended to establish a framework of principles and operational procedures to ensure the security of information resources consistent with the mission and goals of the university.

B. These policies reinforce the essential role that information plays in the academic and administrative functions of the institution. These policies also complement the mission framing the university's IT strategy.

II. Scope

The 07.300 series of policies applies to every user of the university's information technology resources including, but not limited to, students, faculty, staff and visitors.

"Information technology resources" means information owned or possessed by the university, or related to business of the university, regardless of form or location, and the hardware and software resources used to electronically store, process or transmit that information owned, leased or used by the university and its partners.

III. Policy

A. General Statement

The information technology resources of the university are powerful tools, shared among all members of the campus community and designed to support the teaching, learning, instructional, research, administrative, service and other activities of the university. These resources are intended to be utilized in useful and productive ways. Individuals using these

resources are expected to do so wisely and carefully, with respect to and consideration of the rights, needs and privacy of others. Information technology resources and the data they support are used by and accessible to a large number of authorized users. However, since these are typically networked resources they are also subject to unauthorized intrusion, access and attack. It is essential, therefore, that all users understand and follow policies concerning authorized and responsible use. These policies are designed to preserve and protect users, data, other assets, the university, and the information technology resources and communication systems.

The UNCW CIO will provide, at least annually, an IT Security update to the UNCW Board of Trustees Audit, Risk & Compliance Committee.

B. The 07.300 policies are designed to:

1. Provide topic-specific policies which mandate information security controls to address the needs of campus.

2. Ensure consistency between access rights and information classification policies.

3. Ensure that information receives an appropriate level of protection in accordance with its importance to the university.

4. Prevent unauthorized physical access, damage and interference with the university's information processing facilities.

5. Define the rules for acceptable use of information and assets associated with information.

6. Ensure proper and effective use of cryptographic (encryption) controls.

7. Prevent the exploitation of technical vulnerabilities.

IV. Enforcement / Addressing Concerns

A. The university reserves the right to place restrictions on the use of its information technology resources in response to evidence of violations of university policies, rules, regulations, codes, or local, state, or federal laws and regulations. Actions that violate these policies can result in immediate disabling, suspension and/or revocation of the account owner's privileges, pending review for further action. Such unauthorized or illegitimate use of information technology resources, including computer accounts, resources or facilities, may subject the violators to appropriate disciplinary, criminal and/or legal action by the university and/or the state. If evidence is established, the university authorities responsible for overseeing these policies and codes will be consulted on the appropriateness of specific actions.

B. Individuals who have concerns about the conduct of a member of the university community or the propriety of a given situation or activity should notify their department chair, dean, director or an administrator in their supervisory chain at a level sufficient to allow objectivity in evaluating the subject of concern. If action is deemed warranted by this official, the matter shall be referred to the appropriate vice chancellor or senior officer. Prior to taking action, the

vice chancellor or senior officer responsible for the situation or activity at issue shall consult with the CIO, who shall, as appropriate, consult with the university's general counsel.

C. When concern about a given situation or activity involves an imminent threat to individuals, systems or facilities, users are to immediately communicate the concern directly to the University Police.

D. Concerns involving gender-based discrimination, harassment or sexual misconduct must be reported in accordance with Policy 02.205 Unlawful Discrimination, Harassment, and Sexual Misconduct. Concerns involving minors must be reported immediately to the University Police.

V. Review and Disclaimer

A. This is not a comprehensive document covering all aspects of responsible use. It is not possible to anticipate all the conditions and circumstances associated with the use of these resources. This document and its policies seek to link established codes of conduct for the use of information technology resources by members of the university community.

B. This is a dynamic document that is continuously reviewed by Information Technology Services and all other interested parties whose input is solicited and taken seriously.