THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Issuing Office(s)
Information Technology Services
Responsible University Officer(s)
VC for Information Technology and CIO

UNIVERSITY POLICY

Title

UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL POLICY ON INFORMATION SECURITY

Introduction

PURPOSE

This policy defines the framework upon which the information security program operates and gives direction for Information Security-related Policies, Standards, and Procedures to address specific areas of operation.

SCOPE OF APPLICABILITY

All University Constituents and units.

Policy

POLICY STATEMENT

The University has a rich, complex, distributed, diverse, and dynamic information technology environment. Academic, research, and administrative functions of the University rely on technology that is trustworthy and accessible in order to fulfill the mission of this institution. Ongoing and evolving challenges to the integrity, reliability, and availability of University systems require a robust information security program.

Each University Constituent has responsibility for the security of University technology and University data to which they have access resulting from their affiliation with or relationship to the University. The UNC-Chapel Hill information security program is designed to involve each person in training, awareness, reporting, protecting sensitive information, and implementing security controls.

The University information technology security program is based upon the framework outlined in the International Standards Organization (ISO) and International Electrotechnical Commission (IEC) standard 27002. The framework is appropriately interpreted by The University's Chief Information Officer (CIO) and Chief Information Security Officer (CISO) who have determined that this framework conforms to the needs of this higher education institution. The University information technology security program is also informed by security principles and best practices provided by a variety of other sources, including those established by industry organizations and professional associations.

The University IT security program is also subject to applicable regulations, such as the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and North Carolina ID Theft Protection Act (NCID).

The CISO shall recommend appropriate policies in keeping with applicable law and best practices. The CISO shall promulgate standards and procedures for the University to implement policy and support a robust information security program that enables the University to operate securely and effectively.

EXCEPTIONS

Exceptions to specific elements of the information security program should be requested through the processes identified in related information security policies, standards, and procedures.

Definitions

Sensitive Information: Information classified as Tier 2 or Tier 3 in the UNC-Chapel Hill Information Classification Standard.

University Constituent: UNC-Chapel Hill faculty, staff, students, retirees and other affiliates, contractors, distance learners, visiting scholars and others who use or access UNC-Chapel Hill resources.

Related Requirements

EXTERNAL REGULATIONS AND CONSEQUENCES

Health Insurance Portability and Accountability Act (HIPAA)
Family Educational Rights and Privacy Act (FERPA)
North Carolina Identity Theft Protection Act (NCID)
NC Public Records, NCGS Chapter 132

COMPLIANCE

Failure to comply with this policy may put University information assets at risk and may have disciplinary consequences for employees, up to and including termination of employment. Students who fail to adhere to this policy may be referred to the UNC-Chapel Hill Office of Student Conduct. Contractors, vendors, and others who fail to adhere to this policy may face termination of their business relationships with UNC-Chapel Hill.

Violation of this policy may also carry the risk of civil or criminal penalties.

UNIVERSITY STANDARDS AND PROCEDURES

Please see http://its.unc.edu/about-us/how-we-operate/ for the following Information Technology Policies, Standards, and Procedures:

- Information Security Controls Standard
- Vulnerability Management Policy and Standard
- Password Policy for General Users, Password Policy for Administrative Users, and accompanying Standards
- Information Classification Standard
- Security Liaison Policy
- Acceptable Use Policy
- Onyen Policy
- Transmission of Sensitive Information Policy and Standard

Contact Information

POLICY CONTACT(S)

1. ITS Policy Office
   Title: ITS Policy Office
   Unit: ITS
   Email: its_policy@unc.edu
   Phone: 919-962-HELP

OTHER CONTACTS

Guidance on Specific Requests	Deputy CIO, CISO	919-962-HELP	help.unc.edu

Important Dates

- Effective Date and title of Approver:
  a. Effective Date: 6/30/2010
  b. Approver: Chief Information Officer

- Revision and Review Dates, Change notes, title of Reviewer or Approver:
  a. Last Revised Date: 10/24/2017
  b. Revised by: Chief Information Officer
  c. Substantive Revisions:
     i. Complete revision