I. BACKGROUND AND PURPOSE

Academic, research and administrative functions of the University of the University of North Carolina System (UNC System) rely on technology that is trustworthy and accessible in order to fulfill the mission of the institution. This document is required by and authorized by UNC Policy 1400.2.

This document formalizes the requirements for reporting information security incidents relevant to the University of North Carolina System Office (UNC System Office). The objective of this document is to ensure the secure operation of UNC System Office information resources, to minimize any negative consequences of information security incidents, and to improve the ability of UNC System Office to promptly restore operations affected by such information security incidents. It ensures that affiliates promptly and appropriately report information security incidents.

II. POLICY AND PROCEDURE STATEMENT

Every UNC System Office affiliate has a shared responsibility for the security of UNC System Office technology systems and information to which they have access resulting from their affiliation with the UNC System.

Each affiliate of the UNC System is responsible for promptly reporting suspected or known information security incidents (see definition below) to the UNC System Office Department of Information Technology (DoIT).

**Reporting procedure:** Report the issue or concern via email to help@northcarolina.edu. Do not include any confidential or sensitive information in the email. Describe the type of sensitive information or concern, request a telephone call back and provide a telephone number. If the matter is urgent, mark the email as “High Importance.” The UNC System Office employee who responds will collect information in a secure manner.

III. COVERAGE AND SCOPE

This document applies to all affiliates, and all individuals or entities using any UNC System Office information resources. It also applies to any UNC System Office information resources managed by other organizations that use such information resources to provide services to the UNC System Office, such as an application hosted by a software vendor.
Violations of this or any other UNC System Office policy (including regulations, procedures or standards) may result in the revocation or limitation of information resources privileges as well as other disciplinary and administrative actions, up to and including dismissal, and violations may be referred to appropriate UNC Constituent Institutions and/or external authorities.

IV. DEFINITIONS

Information resources: Information owned or processed by the UNC System Office, or related to the business of the university system, regardless of form or location, and the hardware and software resources used to electronically store, process or transmit that information. Information resources include data, software and physical assets. See UNC Policy 1400.1.

Information security incident (also referred to as “incidents” or “incident” within this document): Any unauthorized access, acquisition, use, disclosure, modification or destruction of information resources; interference with information software or hardware resources; or a violation of the acceptable use policy. An information security incident may include, but is not limited to, any of the following:

- unauthorized access of a university information resource;
- any disclosure or exposure of sensitive or confidential information;
- any unapproved use, transmission, or storage of UNC System data that violates secure storage and file exchange as specified in the Data Classification, Storage, and Sharing policy;
- any disruption or attack impacting UNC System Office information resources; or
- a loss or theft of a UNC System Office information resource.

UNC Constituent Institutions: One of the degree/diploma-granting institutions that comprise the University of North Carolina as well other affiliated organizations unless otherwise specified by properly authorized written agreements.

Chief Information Security Officer (CISO): The CISO is the DoIT employee who leads information security incident response efforts.

UNC System Affiliates: Every user of UNC System Office information resources, every UNC System Office staff member, every UNC Constituent Institution staff member, temporary employee, student, alumnus, contractor, vendor and visitor who accesses UNC System Office, information systems or devices is responsible for reporting incidents as described above.

V. INFORMATION SECURITY INCIDENT COMMUNICATIONS AND PRECAUTIONS

Communication is an essential part of effective information security incident response. Once an information security incident is declared by the CISO, the CISO will coordinate appropriate information sharing.

If the CISO determines that the incident may have been caused by the negligence or misconduct of a System Office employee, the CISO will contact System Office Human Resources to determine appropriate next steps, which may include, but are not limited to, placing applicable employees on administrative leave in order to conduct a workplace investigation, temporarily suspending employee system access, and/or reclamation of laptops, phone, and other University electronic property in possession of the applicable employees.
All external communications with the media or the public related to any information security incident must be approved by the UNC System Office Communications departmental staff.

VI. SANCTIONS

Sanctions for Prohibited Actions: A violation of this policy may be considered unacceptable personal conduct as provided in the policies applicable to the employee’s appointment type and subject to appropriate disciplinary or related administrative action, up to and including dismissal. Students who fail to follow this policy may be referred to appropriate student conduct venues. Vendors that fail to follow this procedure may be subject to termination of relevant business relationships or other sanctions.

VII. AUTHORITY, REVIEW, AND APPROVAL

This procedure is required by and authorized by UNC Policy 1400.2. The Chief Information Officer (CIO) has approval authority for changes to this document and the Chief Information Security Officer has approval authority for dependent documents such as detailed incident management process documentation. Review of this procedure document will occur at least every two years.

VIII. REFERENCES

University of North Carolina System Office, Internal Procedures: Data Classification, Storage, and Sharing (Origination Date: January 1, 2018).


University of North Carolina System Office IT Policies, Procedures, and Guidelines are available at: https://myapps.northcarolina.edu/it/it-policies/

More detailed documents that supplement this procedure are shared with appropriate groups and are maintained by the Chief Information Security Officer.

END OF DOCUMENT