North Carolina Central University
Information Security Program

Scope: This document establishes the North Carolina Central University's (NCCU) Information Security Program for the security of all university information that is acquired, transmitted, processed, stored, transferred and/or maintained by NCCU or its affiliates in accordance with provisions set forth in North Carolina General Statute § 58-39-145 and State of North Carolina Statewide Information Security Manual chapter 11. This program is facilitated by the NCCU IT Security and Compliance Officer.

Purpose: The information security department strives to uphold NCCU's reputation, financial assets, customer goodwill, operations uptime, computing resources, personnel productivity, intellectual property and liability protection. Security programs must continually evolve to align to a changing landscape of attacker, methods and alterations in the environment being protected. The purpose of the NCCU information security program is to:

- Establish a university wide approach to ensure the confidentiality, integrity and availability of all information processed, stored or transmitted over the NCCU network whether at rest or in motion.
- Ensure accuracy, security and protection of information in the university's custody, regardless of format.
- Prevent and protect against any anticipated or unanticipated threats and hazards.
- Prevent and protect against the unauthorized access to or use university information, including confidential and personal information.
- Ensure university-wide compliance to applicable laws, regulations, policies and practices.

Applicability: This program applies to all faculty, staff, students, guests and contractors affiliated or doing business with North Carolina Central University.

Program Components: The NCCU Information Security Program consists of:

- Awareness
- Policies
- Training / Professional Development
- Application
- University Initiatives

Awareness and Training

- Cyber Security Awareness Month: http://www.staysafeonline.org/ncsam
- Information Security Newsletter sent each semester to faculty, staff and students
- Information found on the IT Security Website: http://www.nccu.edu/administration/its/internal/it-security.cfm
- Information Security Awareness for Executives: https://library.educause.edu/resources/2005/1/cyber-security-on-campus-executive-awareness-video

Policies and Regulations

70.00.1 - INFORMATION SECURITY POLICY The purpose of this policy is to establish a structure for all Information Security documents, including policies, regulations and rules. The goal of this policy is to establish the overarching policy for all IT assets including but not limited to: computers, servers, network, data or any information assets of North Carolina Central University (“NCCU” or “University”)

The IT regulations and rules provide the additional guidance as it relates to specific technologies and systems. This policy gives NCCU and the Chief Information Officer (CIO) the right to create, modify these or other regulations and rules.

This policy applies to all users of any information system or information system components of NCCU, including all students, faculty, administrators, staff, alumni and visitors of NCCU.

70.00.2 - DATA AND INFORMATION REGULATION The purpose of this Data and Information Regulation is to provide general guidance on the protection of University data and information being processed by manual as well as automated systems and the protection of the records and reports generated by these information processing systems.

Information is a vital component of University operations, and it is important to ensure that persons with a need for information have ready access to that information. It is equally important to ensure that measures have been taken to protect sensitive information against accidental or unauthorized access, modifications, disclosures, or destruction, in order to ensure the security, reliability, integrity, and availability of information. In addition, federal and state laws assign legal responsibility for the correct and appropriate use of information in order to protect a person's right to privacy.

This regulation sets forth the responsibilities for data and information security for all individuals and departments at North Carolina Central University who access, process, or have custody of university data.

Data trustees, stewards and custodians shall ensure that the standards for data security that affect their respective areas of responsibility are effectively implemented. The administrative duties associated with this responsibility shall be assigned by the respective vice chancellors to the owners of the data, who typically are the managers responsible for either the creation or collection of that data and/or the primary user of that information.

70.00.4 - RESPONSIBLE USE REGULATION - Responsible use of University computing and electronic communication resources demonstrates respect for unobstructed access, intellectual property rights, truth in communication, ownership of data, system security and integrity, and individuals' rights. Responsible use includes, but is not limited to, respecting the rights of other users, sustaining the integrity of systems and related physical resources, and complying with all relevant policies, laws, regulations, and contractual obligations.

The computing and electronic communication resources that North Carolina Central University provides for faculty, staff, and students are essential to carrying out the University's primary missions of teaching, research, and public service. Protecting and preserving University computing and electronic communication resources is a cooperative effort that requires each member of the University community to act responsibly and guard against abuses.

The University's computing and electronic communication resources include its servers, networking facilities, e-mail system, personal computers, software, video distribution system, and telephone system. This policy applies to all users of North Carolina Central University computing and electronic communication resources, including faculty, staff, students, guests, individuals not otherwise affiliated with the University, and external organizations and individuals accessing external network services, such as the Internet, through University facilities.

The University provides authorization to use University computing resources with the creation of a user ID and password. Students, faculty, and staff obtain a user ID upon enrollment or employment at the University. The user ID provides access to basic computing services such as the use of email, access to office automation soft- ware, the Internet, and access to systems and information. Departments or units provide access to additional resources as needed or appropriate.

Use of University computing and electronic communication resources is conditioned upon the obligation of each user to adhere to the following standards of responsible use:

NCCU Information Security Preventive Maintenance Checks and Services

• **Network Vulnerability and Sensitive Information Search Scans** – NCCU conducts periodic network vulnerability and sensitive information scans in accordance with State of North Carolina regulatory requirements and Payment Card Industry Data Security Standards (PCI DSS).
• **NCCU Virtual Private Network** (**VPN**) – NCCU provides a secure method of connecting to the NCCU Local Area Network from a remote location.
http://web.nccu.edu/library/about/documents/WebVPN.pdf
• **NCCU Enterprise Virus Protection** - We provide Microsoft Security Essentials Endpoint Protection for faculty, staff and students for free. Microsoft Security Essentials Endpoint Protection offers antivirus and antispyware protection, along with firewall intrusion prevention and device and application control. http://www.nccu.edu/software/
• **Information Security Assessments (internal/external)** - North Carolina General Statute 147.64.6(c) (18) requires the Office of the State Auditor to perform audits of the security practices of the information technology systems within the State. The audit will include but is not limited to the conduct of a network vulnerability assessment. Due to budgetary constraints this function is now the responsibility of the units to be audited. NCCU conducts periodic Information Security Assessments, both internal and external, in accordance with provisions set forth in State of North Carolina Office of the State Auditor’s letter dated March 19, 2010, to the Chancellor of NCCU.

University Initiatives

- **Enterprise Risk Management at NCCU–ERM**’s mission is:

o To foster a collaborative campus environment in which students, faculty, staff and visitors are engaged in a holistic effort to safeguard the health and wellbeing of all while protecting university assets.

o To identify and prioritize risks and to prepare mitigation strategies that coincides with the university’s overall mission.

- **Red Flag Rules Administration (Identity Theft Protection Program)**-The purpose of this program is to detect, prevent, respond to and mitigate suspected or real incidents of identity theft in connection with any Covered Account. This program envisions the creation of policies and procedures in order to achieve compliance. The Board of Trustees delegates to the Program Administrator the authority to develop appropriate and necessary policies and procedures.
http://www.nccu.edu/formsdocs/details.cfm?id=1896

- **Information Security Council**-Incidents of breaches in security have increased exponentially in recent years. A series of national disasters have resulted in a proliferation of laws, regulations and protocols directed at countering the impact of data security risks. Universities, which have historically considered themselves outside of data security discussions, find themselves in a totally different IT landscape today. HIPAA, FERPA, CALEA, PCI and numerous other requirement laden developments make it even more imperative that universities develop coherent, well managed and well-coordinated information security plans. In response to these demands the university has established the NCCU Information Security Council to parallel and, when necessary, integrate with similar efforts at UNC General Administration and in the State Auditor’s Office. The primary purpose of the ISC is to provide guidance to the university community and affiliated organizations regarding how to best ensure that our information resources are protected. The university is committed to ensuring that the institution’s information resources are protected, reliable, confidential and uncorrupted.

- **Computer Security Incident Response Team (CSIRT)**-The purpose of the NCCU CSIRT is to receive, review and respond to Information Technology (IT)security incidents and to collaborate with the university Information Security Council and other appropriate entities in the development of proactive measures to reduce the risks of such incidents. This procedure provides an incident handling process for use when the NCCU network, servers, desktops or other computing devices are compromised. Being prepared for an incident and following the process detailed below will enable support personnel to handle incidents consistently and appropriately.

o The CSIRT operates under the authority of the Chief Information Officer

o The CSIRT reviews all evidence related to a reported IT security incident and makes recommendations regarding the immediate response.

o The NCCU IT Security and Compliance Officer (CSIRT Chair) will confer with the appropriate Director who in turn will provide the appropriate staff person(s) to evaluate and respond to the identified task. The CSIRT team consults with, advises, and informs appropriate directors, managers and network and system administrators. The CSIRT recommends specific mitigation strategies during an incident and receives and evaluates responses from the appropriate managers and directors. Such activities shall be included in the CSIRT Chairman's Incident Report to the CIO.

CSIRT Membership: CSIRT membership is appointed by the CIO in consultation with other Cabinet members. Members are identified as appropriate points of contact for particular functional areas based on their experience, expertise and responsibilities with various operating systems, technologies and applications. Team members only perform CSIRT work as required by circumstances. The duration of participation in the resolution of an incident is limited to the degree possible.

- The core CSIRT membership is composed of:

- IT Security and Compliance Officer (chair)
- Director, Network Services & Telecommunications
- Director, Web Support Services
- Director, Client Services
- Director, Classroom Computer and Event Support
- Director, Enterprise Information Systems

One or more of the core members will participate in the response to a reported event based on their level of expertise. The priority of the member's response and time allocation will be determined by the immediacy, complexity and threat level of the incident.

Floating seats allow others to be incorporated into the active CSIRT team as necessary, when their expertise is needed to assist in event resolution. The call to participate is on a per event basis by initiation from the CSIRT chair. Floating seats on the CSIRT include:

- General Counsel
- Business Affairs representative
- Academic Affairs representative

- Internal Audit representative
- Human Resources representative
- Campus Police representative
- Office of University Relations representative
- Student Affairs representative

The full membership including floating seats will meet at least once a year to review policy and procedures, discuss proactive measures to minimize risk, and participate in a community security awareness program. Members of the CSIRT will be trained at least once annually relative to actions to be taken during an incident and their duties and responsibilities as they pertain to serving on the CSIRT.