Scope: This document establishes the University of North Carolina Wilmington’s Information Security Program for the security of all university information that is acquired, transmitted, processed, stored, transferred and/or maintained by UNCW 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 UNCW IT Security Officer.

Purpose: Information security strives to uphold UNCW’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 UNCW 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 UNCW 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 with the University of North Carolina Wilmington.

Program Components: The UNCW Information Security Program consists of:

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

Awareness

- UNCW Systems Administrators’ Information Security Forum
- Cyber Security Awareness Month: http://www.staysafeonline.org/ncsam
- Information Security Newsletter sent each semester to faculty, staff and students
- IT Security Website: http://www.uncw.edu/itsd/besafe/
• Information Security Awareness for Executives:  
http://www.educause.edu/Resources/Browse/ExecutiveSecurityAwareness/31370

Policies

• **07.100 (Responsible Use of Electronic Resources)** - This document provides guidelines for the responsible and appropriate use of the university’s electronic computing and communication resources and services. Requiring the responsible use of university electronic resources is necessary to:
  ▪ Ensure business continuity capability (administrative as well as teaching and learning) in an effective and efficient manner without interruption of service.
  ▪ Ensure proper stewardship of university resources and that resources are not utilized for personal gain.
  ▪ Ensure optimum security and integrity of systems and data.
  ▪ Ensure the protection of personal identity of faculty, staff and students.
  ▪ Ensure that resources of the university are not utilized to cause harm to any entity or individual.
  ▪ Ensure 100% legality in every aspect of the use of electronic resources at the university

• **07.200 (Responsible Management of Information Technology Resources)** - This document states the overarching policies and guidelines for the responsible management and administration of the University of North Carolina Wilmington’s information technological resources. This is not a comprehensive document covering all aspects of responsible management, but instead focuses on a select set of core resources vital to the user community. These policies and the specific related provisions are intended to establish a framework of principles and operational procedures to ensure the efficient management of IT resources consistent with the mission and goals of the University.
  
  These policies and procedures reinforce the essential role that information technology plays in the academic and administrative functions of the institution. These policies also complement the principles framing the university’s IT strategy:
  ▪ Universal access
  ▪ User-centered supportive environment
  ▪ Sustainable quality IT infrastructure
  ▪ Baseline standardization
  ▪ Technology literacy

• **07.300 (Network and Data Security Policy)** - This document provides the guidelines to establish a security framework to protect the university networks, computing systems and data. Through this policy, the university will encourage the application of industry-wide best practices to assure that:
  ▪ Confidentiality, availability and integrity of university institutional data will be maintained at all times.
- Stewardship and custodial responsibility of all university institutional data will be defined and that data owners and custodians identify and protect such data in accordance with State and Federal laws and regulations.
- The level of security applied to networks, systems and data is appropriate for the level of risk associated with disclosure, corruption, improper modification or loss of University institutional data.

**Training / Professional Development**
- Computing 101 and 201 available to all faculty and staff ([http://uncw.edu/itsd/help/computingatUNCW.html](http://uncw.edu/itsd/help/computingatUNCW.html))
- Information Security and You Presentations available to all faculty and staff ([http://uncw.edu/hr/documents/Fall2010-TrainingCatalog.pdf](http://uncw.edu/hr/documents/Fall2010-TrainingCatalog.pdf))

**Application**
- **Network Scans** – UNCW 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).
- **UNCW Virtual Private Network (VPN)** – UNCW provides a secure method of connecting to the UNCW Local Area Network from a remote location. [http://uncw.edu/ITSD/help/VPN.html](http://uncw.edu/ITSD/help/VPN.html)
- **UNCW Enterprise Virus Protection** - We provide Symantec Antivirus protection and Symantec Endpoint Protection for faculty, staff and students for free. Symantec Endpoint Protection offers antivirus and antispyware protection, along with firewall intrusion prevention and device and application control. [http://uncw.edu/ITSD/help/antivirus.html](http://uncw.edu/ITSD/help/antivirus.html)
- **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. UNCW 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 UNCW.

**University Initiatives**
- **Chancellor’s Council on Safety and Security** - The University of North Carolina Wilmington’s enduring commitment to safety is demonstrated by the university’s seven strategic goals, one of which is “to enhance the quality of the university’s environment and provide a sustainable campus that is attractive, functional and, above all, safe. UNCW is committed to providing a safe learning and work environment where all students, faculty and staff can thrive.” To this end, Chancellor Rosemary established the Safety and Security Council in October 2006 and charged the Council with reviewing and
coordinating policies, procedures, protocols, services and programs relative to safety and security at UNCW.

  o Capstone event - Chancellors Safety and Security Forum:
    http://uncw.edu/emergencyandsafety/safetysymposium.html

• **Institution Risk Management at UNCW** – IRM’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 well being 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.
  o http://www.uncw.edu/ba/irm/index.html

• **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.

• **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 UNCW 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 UNCW 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 UNCW 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.
The CSIRT operates under the authority of the Vice Chancellor of Information Technology Systems Division (VCITSD).

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

The IT Security 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 VCITSD.

**CSIRT Membership:** CSIRT membership is appointed by the VCITSD 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 Officer (chair)
- Director, Integrated Enterprise Solutions
- Director, Client Tech Services
- Director, Operations Systems Admin.
- Director, Network and Communications
- Computer Consultant Manager
- Technology Assistance Center Manager
- Webmaster
- One network specialist
- One Unix specialist
- One Windows specialist
- One systems/database analyst

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:

- University Counsel representative
- Business Affairs
- Academic Affairs
- Internal Audit representative
- Human Resources representative
- Campus Police representative
- Marketing and Communications (Public Relations rep)
- 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.