UNIVERSITY OF NORTH CAROLINA WILMINGTON

INFORMATION SECURITY PROGRAM

CONTENTS

EXECUTIVE SUMMARY

"Cyber security is the strategic, mission focused, and risk optimized management of information technology and systems which maximizes confidentiality integrity and availability using a balanced mix of technology, policy, and people while perennially improving over time." [1]

Our students, faculty, staff, donors, and affiliates entrust the confidentiality, integrity, and availability of their sensitive information to our protection. We are resolute in pursuit of these objectives. We are guided by policy and law, be it federal, state, local, or University to leverage all reasonable and appropriate controls in the protection of the sensitive information in our care.

The Office of Information Security (OIS) seeks every avenue to foster the growth and development of security awareness and skills throughout the campus and community. The OIS commits itself to the effective protection of the confidentiality, integrity, and availability of information and information systems of UNCW. We strive to make everyone at UNCW a responsible steward of the institution's data.

The creation, preservation and exchange of information is an intrinsic part of the University's teaching, scholarship, and administrative operations. Increasingly information is processed, handled, or stored in an electronic form. The growing availability of digital information offers opportunities to improve our collaborations, and work in new ways. Unfortunately, it also presents us with new threats. The very technologies we use to gather, share, and analyze information also make our institution vulnerable to varied and continually evolving information security risks.

PURPOSE

The purpose of the Information Security Program is to clearly state the University's posture towards the protection of its data and information assets. The comprehensive program provides the objectives and requirements for the implementation and maintenance of effective security at UNCW. This program is also in accordance with North Carolina General Statute § 58-39-145 and 16 CFR § 314.3 - Standards for safeguarding customer information of the Gramm-Leach-Bliley Act ("GLBA").

SCOPE

All University Data, regardless of form or the environment where the data reside, is within scope of this plan. This includes storage on central servers, college or departmental mini-computers, printers, data servers, individual personal computers, mobile devices, vendor systems, and data residing in any other medium, including paper. The Information Security Program also applies to all faculty, staff, students, vendors, affiliated entities, and any person with access to University Data regardless of form or format.

This program outlines the responsibilities of all UNCW organizational units, departments, and individuals. Though the Office of Information Security leads the effort in securing our data and systems, security planning and execution can only be successful through collaboration and combined effort.

[1] Hasib, M. (Third Edition, 2015). *Cybersecurity Leadership*

MISSION

The Office of Information Security supports university success through coordinating campus-wide security services and offering guidance to help safeguard the confidentiality, integrity, availability, and assurance of the institution's information systems and resources.

Measurement of effectiveness is delivered through three primary responsibilities[2]:

- Identification of cyber risk within the context of business priorities and value
- Seamless integration of cybersecurity activities within the fabric of business activities
- Leadership and effective response in the event of a cyber crisis

STRATEGY

The Office of Information Security implements balanced security through a principled and measured approach to reducing information security risk while championing a sustainable and effective security culture in the campus community.

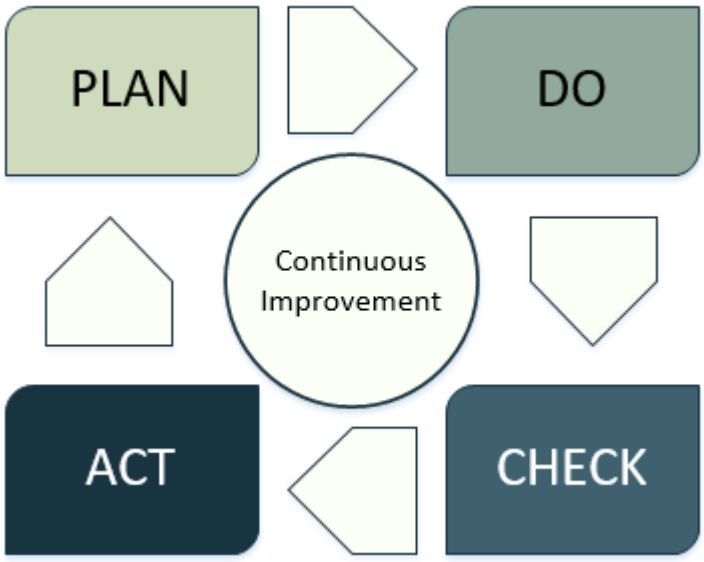
We define our general approach to security sustainment and improvement that can be applied to any system, from an individual practice or control up to a full-blown information security architecture and management system, through a Plan Do Check Act process that delivers continual improvement to our security posture.

Plan – Risk identification, assessment, and treatment identification

Do – Treatment implementation and operation

Check – Risk Review and monitoring

Act – Corrective and preventative actions



INFORMATION SECURITY COMPLIANCE PROGRAM

[2] Thomas J. Parenty, J. J. (n.d.). A Leaders's Guide to Cybersecurity. 2019: Harvard Business Review Press.

Regulations and compliance requirements mandate minimum standards of due care and set the foundation for an effective security program.[3]

The University continuously works to assure our compliance with the requirements and implications of applicable laws and regulations at the Federal, State, and local level. We adhere to the policies set by the System Office and the standards and frameworks adopted by the UNC system.

REGULATORY STANDARDS COMPLIANCE

UNCW periodically assess the process applied in its endeavors to maintain current with legal and contractual obligations surrounding sensitive and critical information assets.

INFORMATION SECURITY STANDARDS AND FRAMEWORK

The University of North Carolina Wilmington, along with its sister institutions within the UNC system, adopted the International Organization for Standardization's ISO/IEC 27002 as the de facto framework for the formulation of our information security related policies. This adoption was communicated in a letter of intent, signed by the then current Chancellor, to the University of North Carolina General Administration (now System Office). As such, this Information Security Program is based on the ISO/IEC 27002 code of practice for security controls and a gap analysis is prepared annually for review by our peer group at the UNC-Information Security Committee.

UNCW SECURITY POLICY

UNCW has a set of security policies dedicated to maintaining compliance with relevant laws and regulations as well as applying adherence to best practices in securing protected and critical data.

The security program is communicated through the 07.100 and 07.300 level policies for UNCW. All policies are publicly viewable on the UNCW website.

07.100.00 RESPONSIBLE USE OF ELECTRONIC RESOURCES

The 07.100 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.

07.300.00 INFORMATION SECURITY

[3] Bonney, B., Hayslip, G., & Stamper, M. (2019). CISO Desk Reference. CISO DRG Joint Venture Publishing.

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.

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.

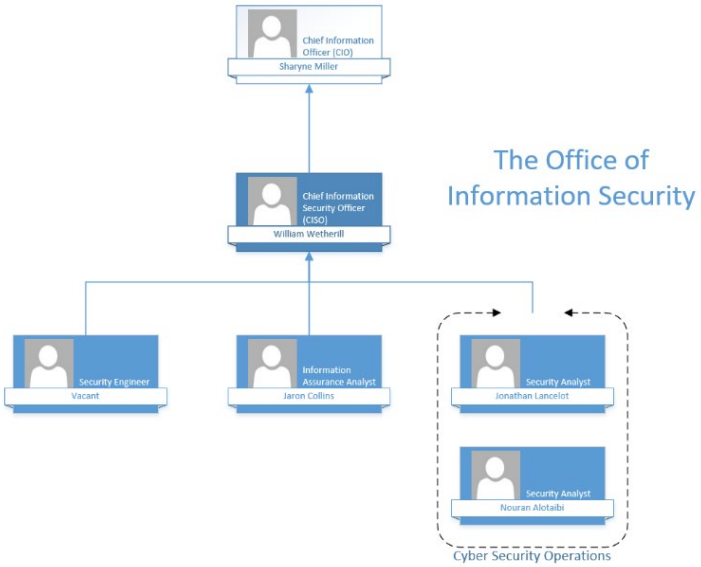
POLICY MANAGEMENT

Per General Statute §116-40.22.d of the North Carolina General Assembly, all policies, notwithstanding any other provision of law, governing or providing for information technology (including security) are established by the UNCW Board of Trustees. Operational policies are subject for approval by the Chancellor and designated authority. This design allows for a more agile operational environment while ensuring executive support and oversight.

ORGANIZATIONAL STRUCTURE

UNCW has established this information security program and designated the Associate Vice Chancellor / CIO as the senior officer, accountable to the Chancellor, who is responsible for information security. The AVC / CIO has established the Office of Information Security with the charge of implementing and managing the information security strategy across the entire enterprise.

The Office of Information Security is composed of the following administrative roles and responsibilities and reports through the Associate Vice Chancellor / CIO.



AVC / CHIEF INFORMATION OFFICER

The Chief Information Officer directs and aligns Information Technology with the goals, mission and values of the University and provides the vision and leadership in delivering quality information technology services and products to campus. The CIO is ultimately responsible for overseeing implantation and periodic evaluation of the information governance and security infrastructure as well as identifying and deploying all reasonable measures to maintain the security, confidentiality, accessibility, and integrity of information resources.

CHIEF INFORMATION SECURITY OFFICER

The Chief Information Security Officer (CISO) is part of the Chief Information Officer (CIO) team, reporting directly to the CIO. The CISO facilitates the application of the security program and leads initiatives to oversee identification and remediation of potential information security risks to the institution. The CISO has the responsibility of protecting and securing the University's information resources and oversees the maturation, accountability, and evaluation of its security posture.

INFORMATION SECURITY ENGINEER (IT SECURITY SPECIALIST)

The Information Security Engineer is responsible for managing and advising on aspects related to the research, design, implementation, and assessment of complex logical security systems and controls. The security engineer works closely with the CISO to ensure alignment with strategy and regulatory need.

The security engineer has an obligation to anticipate new threats and actively work to prevent them from occurring.

INFORMATION ASSURANCE ANALYST

The Information Assurance Analyst role is responsible for the application of the information security risk program, the security assurance & compliance program, portions of the security awareness program, and performs consult regarding security operations and security infrastructure.

INFORMATION SECURITY OPERATIONAL STAFF

The Office of Information Security provides several operational services designed to ensure and protect the day to day activities of campus. Operational staff is composed of all members of the Office of Information Security. The office maintains a Security Operations Center (SOC) for investigating and processing all alerts, requests, and other operational activity as needed.

SYSTEM ADMINISTRATORS AND SUPPORT TECHNICIANS

Employees responsible for the administration and management of IT resources are designated as system administrators and support technicians. In certain circumstances they may be asked to assist the Office of

Information Security based on their expertise and knowledge of systems. It is also expected that these individuals:

- Advise the Office of Information Security should they become aware of a security failure or vulnerability in their systems
- Ensure their processes and systems adhere to all UNCW policies and standards, any contractual requirements, and any requirement or implication of applicable laws and regulations at the Federal, State, and local level
- Promote and grow a culture of information security within their unit or department

HUMAN RESOURCES SECURITY

UNCW maintains a process to ensure that all employees are not only qualified for but understand their roles and the responsibilities of their job duties. The University must safeguard access to its critical and sensitive information and information systems through the appropriate application and revocation of system access upon a position change, responsibility change, or termination of employment.

RISK MANAGEMENT AND REPORTING

UNCW takes a risk-based approach to information security. Through Enterprise Risk Management, the University maintains a process for identifying, assessing, and reporting significant risk to executive leadership.

DATA AND ASSET SECURITY MANAGEMENT

INFORMATION AND SYSTEM CLASSIFICATION

The University of North Carolina Wilmington protects its data and systems based on a classification system that is enforced through policy and standards. This policy and set of standards will establish and maintain security categories for business data and information systems.

ASSET MANAGEMENT

The institution manages an asset program that identifies, tracks, and classifies our most critical and important assets to ensure appropriate protections. The program considers the following when evaluating assets:

- Criticality of the asset to the business of the University
- The level of sensitivity of data in process, or rest on the asset
- The criticality or sensitivity of the business processes that address the asset
- The sensitivity of the environment an asset resides
- Those assets and process that directly connect to the asset in question

ACCESS CONTROLS

The University limits access to information and information systems based on the authority granted, the user, process, type of transaction, software, or system requiring access. Authority is granted as needed and given the least privilege needed to operate. The University maintains access control policies for authorizing revoking access to information systems.

PHYSICAL AND ENVIRONMENTAL CONTROLS

UNCW takes appropriate steps to mitigate the threats associated with the physical environment.

Including, but not limited to:

- Physical access to information systems, equipment, and operating environments should be limited to authorized individuals.
- Preventative measures will be taken to protect critical hardware and wiring.
- Appropriate media-sanitization will be applied prior to disposal, reuse, or release.
- Reasonable process to protect against the unauthorized removal of equipment, information or software will be followed.

ZONES OF TRUST AND CRYPTOGRAPHIC CONTROL

The University adheres to data standards that determine the level of protection appropriate for data no matter the form, be it in transit, at rest, or in process.

Key management associated with encryption will be documented and employed and keys will be protected against unauthorized access.

OPERATIONAL SECURITY

UNCW adopts a formalized operational security policy along with the appropriate procedures and controls to protect systems and data. Operational security may be composed of, but not limited to, the following elements:

- Configuration standards for information systems and applications
- Change control process
- Segregation of duties
- Detection and response to malicious software or behaviors
- Security monitoring and auditing, including logging infrastructure
- Privilege access control
- Data resiliency and continuity

COMMUNICATIONS SECURITY

The University promotes effective information security within information systems by employing purposeful architectural initiatives, software development techniques, encryption, and engineering principles. The University also monitors, controls, and protects University communications (i.e., information transmitted or received by University information systems) at the external boundaries and key internal boundaries of the information systems for confidential data transmissions.

SYSTEM ACQUISITION, DEVELOPMENT, AND MAINTENANCE

Information Security requirements are an integral and established part of development and implementation of information systems. UNCW must address this through processes that:

- Validate the security of purchased software, products, and services
- Validate the security of new or enhancements to information systems
- Address secure coding practices and take into consideration common security vulnerabilities
- Apply security standards for sensitive test data that is applied to sensitive production data
- Restrict access to source code libraries
- Enforce a change management framework to ensure that changes to critical systems do not have negative impact to security or operations
- Ensure change controls are tested, reviewed, and have a rollback plan in case of failure
- Support a patch management strategy and assigned responsibilities for monitoring and promptly responding to vulnerability reports, patch releases, and security bulletins

THIRD PARTY CONTRACTS AND AGREEMENTS

The Institution must appropriately secure the information and technology resources accessed, processed, and managed through third parties. Security requirements must be communicated in all agreements before granting access to sensitive institutional information or assets.

SECURITY AWARENESS AND TRAINING

To ensure all managers and users act responsibly, it is essential they are made aware of the security risks associated with handling information and information systems. The University ensures materials and/or training are provided for applicable laws, regulations, policies, standards, and procedures as appropriate to the access to critical and sensitive information and information systems. The University provides adequate information security training and general security awareness training for users to carry out their assigned duties and responsibilities as well as safely navigate their digital lives on campus.

INFORMATION SECURITY INCIDENT MANAGEMENT

UNCW maintains an effective information security incident management program and ensure personnel are trained and equipped to detect, report, and respond to adverse events. Incident-handling procedures are in place to respond and report security events throughout the incident life cycle with clearly defined

roles and responsibilities. Staff must be trained in legal and compliance requirements surrounding evidence collection. Information Security incident management includes cyber incident management.

INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

UNCW ensures the continuity of operations under extraordinary circumstances. Information Technology Services maintains a Disaster Recovery Plan and Continuity of Operations Plan that includes the maintenance and measure to protect the privacy and security of information resources during an event. The plans are periodically tested, reviewed, and approved by senior ITS staff.

DOCUMENT UPDATES AND REVISION

The Information Security Program is reviewed for revision annually by key stakeholders and any changes approved by the Chief Information Security Officer.

DOCUMENT HISTORY

Version	Description of Revision	Approved by:	Date:
1.0	Original Document	UNCW	07/19/2021

APPENDIX

COMPLIANCE

REGULATION / STANDARD	SUMMARY
Family Educational Rights and Privacy Act (FERPA)(20 U.S.C. S1232g; 34 CFR Part 99)	FERPA is a federal privacy law that gives parents certain protections with regard to their children's education records, such as report cards, transcripts, disciplinary records, contact and family information, and class schedules.
Gramm-Leach-Bliley Act	The Gramm-Leach-Bliley Act (GLB Act or GLBA), also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.
Health Insurance Portability and Accountability Act of 1996	HIPAA is United States legislation that provides data privacy and security provisions for safeguarding medical information.
The North Carolina Identity Theft Protection Act of 2005	The North Carolina Identity Theft Protection Act of 2005 is a series of broad laws passed by the General Assembly of the U.S. state of North Carolina to prevent or discourage identity theft as well as guarding and protecting individual privacy.
Digital Millennium Copyright Act	DMCA criminalizes production and dissemination of technology, devices, or services intended to circumvent measures (commonly known as digital rights management or DRM) that control access to copyrighted works. It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet.
Payment Card Industry Data Security Standard (PCI-DSS)	A set of 12 regulations designed to reduce fraud and protect customer credit card information.
ISO/IEC 27002	Guidelines for organizational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organization's information security risk environment(s).
Communications Assistance for Law Enforcement Act (CALEA)	CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance while protecting the privacy of information outside the scope of the investigation.
The UNC Policy Manual – 1400.1 Information Governance Policy	The UNC System policy manual, section 1400, is intended to foster the development and maintenance of strategically aligned technology resources; consistent governance and management of IT; encourage collaboration; and, in alignment with "Guiding Principles".

The UNC Policy Manual – 1400.2 Information Security Policy	Establish an information security program and designate a senior officer, accountable to the Chancellor, who is responsible for information security.
The UNC Policy Manual – 1400.3 User Identity and Access Control Policy	Evaluate and conduct risk-based implementation of appropriate identity confirmation and access control techniques, such as multi-factor authentication, to control access to University data.

GLOSSARY

Availability: A property that assures that the system has the capacity to meet service needs. It includes timeliness and usability. The property of availability protects against threats of denial of service.

Controls: Mechanisms or procedures that mitigate threats. Among the goals of information security controls are to provide confidentiality, integrity, availability, or privacy to a computer system.

Confidentiality: A property that assures the assets of a computer system are accessible only by authorized parties or entities. The property of confidentiality protects a system from the threat of disclosure. A disclosure threat is the possibility that data will be accessed by unauthorized entities.

Cyber Incident: An occurrence that:

a) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
b) Constitutes a violation or imminent threat of violation of law, security policies, privacy policies, security procedures, or acceptable use policies.

Information resources: 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.

Integrity: A property that assures that unauthorized changes in data cannot occur or can be detected if they do occur. The property of integrity protects against threats of modification and fabrication.

Privacy: A subset of confidentiality. It concerns data about an entity and assures that this data is not made public or is accessible by unauthorized individuals.

Risk analysis: The study of the consequences involved in doing something or not doing it. It improves the basis for information security related decisions and helps justify expenditures for information security.

Threats: Potential occurrences, malicious or otherwise, that can have undesirable effects on assets or resources associated with computer systems.

University Data: All information content related to the business of UNCW (see Data Management Policy).

Vulnerabilities: Characteristics of systems, applications, and processes that make it possible for a threat to potentially occur. They are not necessarily weaknesses in a system and may be otherwise desirable qualities of a system.

UNIVERSITY OF NORTH CAROLINA WILMINGTON

GARY L. MILLER
Chancellor

February 1, 2012

Mr. John Leydon
Vice President for Information Resources and Chief Information Officer
University of North Carolina General Administration
P.O. Box 2688
Chapel Hill, NC 27515-2688

Dear Mr. Leydon:

The University of North Carolina Wilmington conducted a thorough review and vetting of the UNC GA proposal for a unified Information Security Standard via the University of North Carolina Information Technology Security Standard.

We provide you with this correspondence in order to give notice of our intent to adopt the International Organization for Standardization's ISO/IEC 27002 as the de facto framework for the formulation of our information security related policies.

UNCW will provide a report of the crosswalk, gap analysis, and associated risk assessment where there exist variances between the proposed UNC Information Security Standard and our internal policies if appropriate.

Sincerely,

Gary L. Miller
Chancellor

601 SOUTH COLLEGE ROAD • WILMINGTON, NORTH CAROLINA 28403-5931 • 910-962-3030 • FAX 910-962-4050 • millerg@uncw.edu

BIBLIOGRAPHY

Bonney, B., Hayslip, G., & Stamper, M. (2019). *CISO Desk Reference.* CISO DRG Joint Venture Publishing.

Hasib, M. (Third Edition, 2015). *Cybersecurity Leadership.* Tomorrow's Strategy Today, LLC.

Thomas J. Parenty, J. J. (n.d.). *A Leaders's Guide to Cybersecurity.* 2019: Harvard Business Review Press.