# OPERATIONAL SECURITY
07.300.02

| | |
|---|---|
| **Authority:** | Chief Information Officer (CIO) |
| **History:** | Updated May 12, 2022; Approved by CIO July 20, 2021 |
| **Sources of Authority:** | UNC System Office Policy Manual, Chapter 1400 "Information Technology"; International Organization for Standardization ISO/IEC 27002 |
| **Related Links:** | 07.100.00 Responsible Use of Information Technology Resources<br>07.200.00 Responsible Management of Information Technology Resources |
| **Responsible Office:** | Information Technology Services |

## I. Purpose

The purpose of this policy is to define operational security standards in order to ensure that information and information processing facilities are protected against threats to the following:

**Confidentiality**: Ensuring information is accessible only to those authorized to have such access.

**Integrity**: Safeguarding the accuracy and completeness of information and processing methods.

**Availability**: Ensuring authorized users have access to information and associated assets when required.

UNCW is dedicated to the protection of data, monitoring of the university's network for possible threats or malicious activity, and to the integrity of operational systems through the prevention of exploitation of vulnerabilities. UNCW's information security posture is achieved by implementing a suitable set of controls, which can be in the form of policies, standards, guidelines, practices, procedures, position papers, organizational structures, and software functions.

## II. Security Management

Information and information technology are fundamental components of UNCW's mission and strategy. Security management involves establishing policies, controls, and other measures to effectively mitigate the risk of losses related to information and the systems that store, process, and transmit information. The Office of Information Security in partnership with IT Governance and campus leadership will establish policies, standards, and guidelines to provide authentication and authorization of any and all users of UNCW's IT resources to provide proper accountability for information and access to the environment.

Risk can be transferred, accepted, or reduced through mitigation. Information security risk management identifies and seeks to mitigate information-related threats to UNCW's critical business processes, which if realized would impair the University's capability to fulfill its mission

and key objectives. Each security document must be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

## III. Policy

### A. Responsibilities

1. Operating instructions, incident response procedures and business continuity documentation must be developed by the appropriate authority. The maintenance and management of all systems dedicated to information processing must be documented, documentation reviewed, and followed on a consistent and regular basis.
2. All access granted to critical or sensitive information or information systems will be reviewed for appropriateness per job function by the relevant supervisory authority. Whether managed by ITS or otherwise, access controls will adhere to UNCW Policy 07.300.01 "Identity and Access Controls", including an auditable log of provisioning and reviews of access.

### B. General Controls

1. Malicious software counter measures must be deployed to all university owned devices where possible.
    a) An exception in the form of a compensatory control may be used if a local countermeasure does not exist for the device and with explicit approval by the Chief Information Officer and Chief Information Security Officer.
2. Users of university owned devices must report any security incident to the Technology Assistance Center or ITSecurity@uncw.edu upon discovery.
3. All users working on personal devices are strongly encouraged to utilize an anti-malware solution.
4. Users of any device who access university network resources must refrain from downloading, launching, or transmitting any form of malicious software which may result in damaging university processes or resources.
5. Users are prohibited from disseminating false information or initiating anything which threatens other users or university resources.
6. Users and resources are prohibited from conducting activities inclusive of, but not limited to, network reconnaissance, illicit access gain, malicious program execution, privilege escalation, defense evasion, and sensitive data exfiltration without formal approval from the Chief Information Security Officer.
7. Users are prohibited from willfully circumventing any security control.
8. ITS reserves the right to facilitate the containment of malicious software or processes on any UNCW owned device.
9. ITS reserves the right to remove or reset access for any account in noncompliance with policy or with reasonable evidence of malicious action.
10. ITS reserves the right to remove or restrict access for any device in noncompliance with policy or with reasonable evidence of malicious action.

### C. Change Control

1. Changes to any university owned production systems must be presented to the ITS Change Advisory Board for approval and review per the change control procedure.
2. Before a change can be formally approved, the proponents of the change must present an assessment of the risk involved with implementing the changes and discuss what preventative measures, if any, may be taken to minimize or deter possible risk factors.
3. Before a change can be formally approved, the Change Advisory Board must determine the appropriate level of communication, if any, to affected parties.
4. A description of testing and remediation efforts to be applied in case a proposed change results in failure must be provided to the Change Advisory Board before a change can be formally approved.
5. Exceptions to the above will be accepted for emergency changes and changes approved by the Change Advisory Board as a standard change.

D. Administration of Software Controls

1. Proper testing procedures must be in place and followed before any changes to devices. These testing procedures must include consideration for security impact and operational impact.
2. UNCW reserves the right to eliminate any software or service on any device which is believed to be malicious or behaves in a way which undermines security measures or processes.

E. Backups

1. All UNCW server systems must be backed up at an appropriate interval.
2. All UNCW server systems data backups will be stored in a secure, protected, and when feasible, off-site location.
3. Periodic reviews must be conducted to test the quality of restored data and the efficacy of the restoration process.
4. All UNCW business data must be stored in appropriate storage facilities or media.

F. Security Monitoring and Auditing

1. Monitoring and auditing of university owned systems is a centralized process administered by ITS.
2. All university owned systems are subject to monitoring and auditing through policy and software.
    a) All university owned systems may be required by ITS to send security and audit events to centrally managed logging infrastructure
    b) Users of university owned systems may not willfully alter the functionality of logging and monitoring software or policy on systems.

3. Logging must be enabled on all university owned systems. All mission-critical system logs must be periodically reviewed for inconsistencies or unauthorized access to the system.
4. All University servers must log security and audit events to centrally managed logging infrastructure.
5. Log storage must be secured against tampering and unauthorized access using appropriate security controls.
6. Logs must be retained for an appropriate amount of time and be made available for use or review during the retention period.
7. All University servers must synchronize with an appropriate time management service.

G. Vulnerability Management

1. All university supported software, devices, and operating systems must be patched and updated in a timely manner.
2. Users must ensure that all state-owned computer resources are connected to campus infrastructure at least monthly to receive timely updates to operating systems and supported software.
3. Sensitive systems must be patched within a reasonable timeframe of availability after having undergone validation and testing.
4. Any UNCW owned device that is connected to the university's network is subject to scanning. Scanning may be used to determine whether proper patch levels and system configurations are in place. Additional scans may be run to determine other potential security vulnerabilities or used to test data integrity and accessibility.
5. The results and findings from scans must be properly documented and shared with the Office of Information Security.
6. All state-owned systems must adhere to configuration standards to allow centralized scanning.
7. Vulnerability scanning may not be conducted by anyone other than those with explicit approval from the CIO. Special considerations may be made for university research and coursework. All scanning for academic purposes must be on approved infrastructure.

H. Configuration Management

Configuration management is the process of collecting and documenting specific information regarding each information resource toward gaining better control and oversight.

1. ITS centrally develops, documents, and maintains baseline configuration of the information systems under UNCW purview. Baseline configurations serve as a basis for all builds, releases, and/or changes to information systems. Maintaining baseline configurations requires creating new baselines as information systems change over time. To the maximum extent possible, baseline configurations are dictated by

2. standards bodies to ensure that the level of protection is commensurate with the identified risks.
3. It is recommended that any consumer device with an operating system that connects to the UNCW network:
    a) Apply all critical operating system and security patches within the previous 30 days.
    b) Utilize an up-to-date anti-malware with current data files and signatures.
4. Baseline configurations must be reviewed at least once every calendar year, as well as, when configuration changes are made due to critical security patches, upgrades, and emergency changes (e.g., unscheduled changes, system crashes, and replacements of critical components). Any and all security patching and emergency changes are subject to the Change Management Policy
5. ITS baseline configurations must be maintained for development and test environments and managed separately from the operational (production) baseline configurations.
6. Exceptions to baseline configurations must be reviewed and approved through the exceptions for noncompliance process.

I. Security Assessments and Evaluation

A security assessment and evaluation is a technical and non-technical review of safeguards and controls.

1. All university processes and technology are subject to security assessment or evaluation as necessary to identify and document any unmitigated risks that may affect information or information systems and to provide recommended mitigations to identified risks as well as to ensure regulatory compliance and compliance with UNCW policies. Technical evaluations may include vulnerability scanning and periodic penetration testing.

J. Intrusion and Penetration Testing

1. All university systems are subject to vulnerability and penetration testing.
2. Penetration testing is only permitted with the explicit approval of the CIO and is only to be conducted by an approved and agreed upon administrator of the test, whether that is an internal tester, or an independent third party hired for the purpose of penetration testing.
3. If any testing occurs outside of the approval of the CIO it will be considered unauthorized access to restricted systems and may result in disciplinary measures.

K. Vendor Management

1. UNCW protects against supply chain threats through a vetting process that ensures UNCW-defined security safeguards can be met before information resources

2. or services are purchased. This vetting process includes acquisition strategies, supplier reviews, vendor security assessments, contracts, other agreements, and routine attestations by vendors.

L. Training and Awareness

1. Any individual handling university owned data must have completed Information Security training as deemed appropriate by their supervisor, department, or other appropriate authority.
2. Additional security training may be required based on sensitivity of role or compliance requirement.

M. Network Restrictions

1. Any device connected the UNCW network or UNCW services may be quarantined, and/or disconnected, for any reason, including, but not limited to: potential malware, adverse impact to the network, or excessive bandwidth utilization.
2. In addition to the above restrictions, any UNCW owned device may also be rendered unusable for any of the reasons outlined previously and may be subject for network restrictions for having a configuration not in alignment with ITS standards.

N. Exceptions for Noncompliance

1. All resources connected to the university network are expected to comply with security policies and standards which are designed to establish the controls necessary to protect university information and information systems. Any noncompliance can jeopardize systems in aggregate. A control deficiency in a single process or information system can jeopardize other processes or systems. Bad data may be inherited, privacy can be compromised, or a vulnerability be exploited resulting in an intrusion into or damage of UNCW systems. In such cases where compliance cannot be achieved an exception must be documented and approved.
2. Approved exceptions must have an expiration date of no more than one year and each exception request must be periodically reviewed to determine if the exception is still warranted.