AUDIT AND ACCOUNTABILITY STANDARD

Standard Title:	**AUDIT AND ACCOUNTABILITY STANDARD (NSU-AU)**
Standard Number:	**38-10.3**
Standard Reference:	**COV SEC530 INFORMATION SECURITY STANDARD**
Control Family:	**AUDIT AND ACCOUNTABILITY (AU)**
Approval Date:	**05/28/2024**
Responsible Office:	**Office of Information Technology**
Responsible Executive:	**Chief Information Officer**

Applies to: All employees, students, visitors, and contractors, in all academic and operational departments and offices at all Norfolk State University locations, and to all university information technology and data, whether owned and operated by the university, or used for university business through contractual arrangements.

STANDARD STATEMENT

All individuals to whom this standard applies shall comply with the Norfolk State University Information Security Standards and protect all IT systems and data to which they have access commensurate with sensitivity and risk. All university information technology and data whether owned and operated by the university, or used for university business through contractual arrangements shall be managed and protected in accordance with the provisions of the Norfolk State University Information Security Standards.

TABLE OF CONTENTS PAGE NUMBER

STANDARD STATEMENT 1
DEFINITIONS 1
CONTACT(S) 3
STAKEHOLDER(S) 3
AUDIT AND ACCOUNTABILITY (AU) 3
EDUCATION AND COMPLIANCE 5
EXCEPTIONS 6
REVIEW SCHEDULE 6
RELATED DOCUMENTS 6

DEFINITIONS

Authorization: The process of verifying that a requested action or service is approved for a specific entity.

Authorize: A decision to grant access, typically automated by evaluating a subject's attributes.

Authorized: A system entity or actor that has been granted the right, permission, or capability to access a system resource.

Data Owner: An individual, who defines, manages, and controls the use of data and ensures compliance with the Information Security Standards with respect to the data.

Events: event is an observable occurrence in a system.

Information Security: The policies, standards, guidelines, processes, activities, and actions taken to protect the confidentiality, integrity, and availability of information systems and the data they handle commensurate with sensitivity and risk.

Information Security Incident: means an adverse event or situation, whether intentional or accidental, that poses an enterprise impact or threat to the integrity, availability, or confidentiality of university data or systems or requires reporting based upon regulatory requirements.

Information Technology (IT) System: An interconnected set of IT resources under the same direct management control.

Sensitive System: A system that processes any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on NSU interests, the conduct of NSU programs, or the privacy to which individuals are entitled. Please refer to the 32-02 - Data Classification Policy

Sensitive Information/Data: Any data of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on COV interests, the conduct of agency programs, or the privacy to which individuals are entitled. Please refer to the 32-02 - Data Classification Policy

System Administrator: An individual or entity that implements, manages, and/or operates a system at the direction of the System Owner, Data Owner, and/or Data Custodian.

System Owner: An individual or entity responsible for the operation and maintenance of an IT system.

Technological Resources: Technological resources include but are not limited to: computers and terminals, software, printers, networks and equipment, telecommunication equipment and services such as telephones, facsimile machines, modems, basic and long distance calling service, and voicemail; television and radio systems and equipment; computer information systems; and, data files and/or documents managed or maintained by the University which reside on disk, tape or other

media. Technology resources also include multimedia equipped classrooms, computer classrooms, computer laboratories, computer offices, and computer furnishings operated or maintained by NSU.

Users: Faculty, staff and students as well as others who have been authorized to use Norfolk State University's technological resources, (e.g., contractors, interns, volunteers, etc.).

CONTACT(S)
The Office of Information Technology (OIT) officially interprets this standard. OIT is responsible for obtaining approval for any revisions as required through the appropriate governance structures. Questions regarding this standard should be directed to OIT Security.

STAKEHOLDER(S)
University Faculty & Staff
Students
Others who have been authorized to use Norfolk State University's technological resources.

AUDIT AND ACCOUNTABILITY (AU)
NSU-AU-1 EVENT LOGGING

Control:

a. Identify the types of events the system is capable of logging in support of the audit function;

b. Specify the event types for logging with the system;

c. Coordinates the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

d. Allow System Owner, Data Owner, or Chief Information Security Officer to select event types; and

e. Review and update the event types selected for logging on an annual basis and following an environmental change.

NSU-AU-2 CONTENT OF AUDIT RECORDS

Control: Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

NSU-AU-3 AUDIT LOG STORAGE CAPACITY

Control:

a. Allocate audit log storage capacity to accommodate the retention requirements identified in this standard.

b. Transfer audit logs at least once every 30-days to a different system, system component, or media other than the system or system component conducting the logging.

NSU-AU-4 RESPONSE TO AUDIT LOGGING PROCESS FAILURES

Control:

a. Alert designated organizational officials in near real-time in the event of an audit logging process failure; and

b. Take the following additional actions: investigate the cause of the disruption, take appropriate corrective actions, and shall record disruptions.

NSU-AU-5 AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING

Control:

a. Review and analyze system audit records at least every 30 days for indications of inappropriate or unusual activity and the potential impact of the inappropriate or unusual activity;

b. Reports findings to designated organizational officials;

c. Adjust the level of audit record review, analysis, and reporting within the system when there is a change in risk based on law enforcement information, intelligence information, or other credible sources of information;

d. Integrate audit record review, analysis, and reporting processes using organization-defined automated mechanisms;

e. Provide and implement the capability to centrally review and analyze audit records from multiple components within the system;

f. Integrate analysis of audit records with analysis of vulnerability scanning information; performance data; system monitoring information to further enhance the ability to identify inappropriate or unusual activity; and

g. Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness as required.

NSU-AU-6 TIME STAMPS

Control:

a. Use internal system clocks to generate time stamps for audit records; and

b. Record time stamps for audit records that meets the organizational defined granularity of time measurement based on the sensitivity of the system and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.

NSU-AU-7 PROTECTION OF AUDIT INFORMATION

Control:

1. Protect audit information and audit logging tools from unauthorized access, modification, and deletion;
2. Alert the Chief Information Security Officer upon detection of unauthorized access, modification, or deletion of audit information;
3. Store audit records at least once every 24 hours in a repository that is part of a physically different system or system component than the system or component being audited; and
4. Authorize access to management of audit functionality to only authorized administrators and security personnel.

NSU-AU-8 AUDIT RECORD RETENTION

Control: Retain audit records for the retention schedule identified in the University's records retention policy to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.

NSU-AU-9 MONITORING FOR INFORMATION DISCLOSURE

Control:

a. Monitor organization-defined open source information and/or information sites at the appropriate organization-defined frequency for evidence of unauthorized disclosure of organizational information; and

b. If an information disclosure is discovered, notify the Chief Information Security Officer.

EDUCATION AND COMPLIANCE

This standard shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

- Communicate the standard in writing, electronic or otherwise, to the University community within 30 days of approval.
- Post the standard on the appropriate Website.
- Educate and train all stakeholders and appropriate audiences on the standard's content, as necessary. Failure to meet the publication requirements does not invalidate this standard.

The Chief Information Security Officer (or designee) is responsible for official interpretation of this standard. Questions regarding the application of this standard should be directed to the Office of Information Technology. The Chief Information Security Officer reserves the right to revise or eliminate this standard.

Violations of this standard, including without limitation any misuse of data or IT resources may result in the limitation or revocation of access to University IT resources. In addition, failure to comply with requirements of this standard may result in disciplinary action up to and including termination or expulsion in accordance with relevant University policies, and may violate federal, state, or local laws.

EXCEPTIONS

Exceptions to this standard must be documented in writing and approved by the Vice President for Operations and Chief Strategist, the Chief Information Officer, and the Chief Information Security Officer.

REVIEW SCHEDULE

- Next Scheduled Review: **05/28/2025**
- Approval by, date: OIT Standards Development Group, **05/28/2024**
- Revision History: N/A
- Supersedes: SEC530 AU Controls

RELATED DOCUMENTS

32-01 - Acceptable Use of Technological Resources
https://www.nsu.edu/policy/admin-32-01.aspx
32-02 - Data Classification Policy
https://www.nsu.edu/policy/admin-32-02.aspx
38-10 - Information Security Policy