Policy Title: Access Control Policy and Procedures

Policy Type: Administrative


Approval Date: August 10, 2018

Responsible Office: Information Technology Services

Responsible Executive: CIO

Applies to: Information Technology Services

POLICY STATEMENT

Access Enforcement addresses the implementation of access measures established by Information Technology Services in order to authorize and control user access to the University’s Information System. The purpose of this policy is to describe the standard for the effective implementation of selected access control measures.

Table of Contents

CONTACT(S) ..................................................................................................................... 1
STAKEHOLDER(S) ............................................................................................................. 2
POLICY STATEMENT ........................................................................................................ 2
DEFINITIONS .................................................................................................................... 2
POLICY .............................................................................................................................. 3
REQUIREMENTS ............................................................................................................. 3
USER RESPONSIBILITIES ............................................................................................ 5
VIOLATIONS .................................................................................................................... 5
INTERPRETATION ......................................................................................................... 5
PUBLICATION .................................................................................................................. 5
REVIEW SCHEDULE ....................................................................................................... 5

CONTACT(S)

Information Technology Services – (757) 823-2916
STAKEHOLDER(S)
University Faculty & Staff
Information Technology Services

DEFINITIONS

Administrative Safeguards – consists of policies and administrative procedures that manage the selection, development, implementation, and maintenance of security measures that protect the university’s electronic information and information systems.

Application – a computer program that processes, transmits, or stores University information and which supports decision-making and other organizational functions. It typically presents as a series of records or transactions. These records and transactions are generally accessible by more than one user.

Availability – the expectation that information is accessible NSU user community when needed.

Business Unit – the term applies to multiple levels of the university, such as a revenue generating unit or a functional unit (e.g., Compliance, Human Resources, Legal, and Finance). It may also be comprised of several departments.

Confidential Information – the most sensitive information, which requires the strongest safeguards to reduce the risk of unauthorized access or loss. Unauthorized disclosure or access may 1) subject NSU to legal risk, 2) adversely affect its reputation, 3) jeopardize its mission, and 4) present liabilities to individuals (for example, HIPAA penalties).

Confidentiality – the expectation that only authorized individuals, processes, and systems will have access to NSU’s information.

Guest Account – accounts provisioned to individuals not employed by NSU, but who have a justifiable business reason to access University resources.

Information System – consists of one or more components (e.g., application, database, network, or web) that is hosted in a University campus facility, and which may provide network services, storage services, decision support services, or transaction services to one or more business units.

Least Privilege – giving every user, task, and process the minimal set of privileges and access required to fulfill their role or function. This includes access to information systems and facilities.

Physical Safeguards – physical measures to protect the facilities that house the University’s electronic information and information systems.
Administrative Policy # 32 – 8 – 103 (2018) Access Enforcement

Private Information – sensitive information that is restricted to authorized personnel and requires safeguards, but which does not require the same level of safeguards as confidential information. Unauthorized disclosure or access may present legal and reputational risks to the University.

Access Enforcement Policy

Access to the University’s electronic information and information systems, and the facilities where they are housed, is a privilege that may be monitored and revoked without notification. Additionally, all access is governed by law, other University policies, and the NSU Code of Ethics.

Persons or entities with access to the University’s electronic information and information systems are accountable for all activity associated with their user credentials. They are responsible to protect the confidentiality, integrity, and availability of information collected, processed, transmitted, stored, or transmitted by the University, irrespective of the medium on which the information resides.

Access must be granted on the basis of least privilege - only to resources required by the current role and responsibilities of the person. In addition to the administrative, physical, and technical safeguards presented in this policy.

Requirements

Access controls to the University’s information systems must be enforced to ensure the confidentiality, integrity, and availability of the data accessible via those systems.

1. Registration of Access; With respect to registration of access to the University’s information systems:
   a. There must be a formal authorization process documented for access requests.
   b. The requester’s identity must be confirmed and authenticated.
   c. User activity must be logged and tied to the user ID provisioned to the user.
   d. User IDs must be unique and require a password.
   e. Requests for access must be approved by the requester’s manager

2. Registration of Access for Non-NSU Personnel
   a. Individuals who are not members of the Norfolk State community and who have a justifiable business reason to gain access to NSU information services must go through the guest account registration process.
   b. Cancellation of access to all University information systems, facilities, and information services (e.g., remote access) must be done in accordance with the procedures listed in applicable University policy when access is no longer needed.
3. Information System Identity Access Management

4. Information systems must, at minimum, require a user ID and password.
   a. Requests for a deviation from this requirement are limited to clinical systems which
      have been identified by the school or unit as requiring a different access method in
      order to provide patient care.
   b. Deviations must be reviewed and approved by the Chief Information Officer.
   c. User ID Naming Conventions
   d. Passwords
   e. User IDs must have an associated password.

5. Service Accounts
   a. Service accounts are subject to the requirements in this policy.
   b. Service accounts can only be created by a member of NSU’s Active Directory
      or Domain Administrators team to facilitate an identified operational need.
   c. Service accounts do not expire.

6. System Default Service Accounts
   a. Whenever possible, system default service accounts should be renamed or disabled
      as long as it doesn’t adversely impact the operations of the application
   b. System default Service Accounts do not expire.

7. Access Entitlement Review
   a. Access to information systems with information classified as Confidential or
      Private, or otherwise considered sensitive must be, at minimum, reviewed quarterly.
   b. Access to information systems with non-sensitive information must be reviewed
      semi-annually.
   c. Access to the University’s data centers must be reviewed semi-annually.

8. Information Owners (Data Stewards) must
   a. Establish access authorization procedures to their electronic information and
      information systems.
   b. Perform and comply with the policy requirements relevant to their information
      systems.
   c. Review access entitlements to their information systems as stipulated in this policy
      or when requested by the Information Security Office, and/or Internal Audit.
ADMINISTRATIVE POLICY # 32 – 8 – 103 (2018) Access Enforcement

USER RESPONSIBILITIES

Users of NSU Information Systems will be held accountable for following the University's practices in safeguarding their personal authentication information.

VIOLATIONS

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 32-01 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee.

INTERPRETATION

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to Information technology Services. The Information Security Officer reserves the right to revise or eliminate this policy.

PUBLICATION

This policy 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:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;
2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;
3. Post the policy on the appropriate Website;
4. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 08/10/2019
- Approval by, date: Information Technology Services, 08/10/2018
- Revision History:
  Supersedes policy #32-8-103 (2014) Dated 5/28/2015 Revised; Access Enforcement