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 Control addresses the measures implemented by Information Technology Services in order to authorize and manage user access to the University’s Information System.

Table of Contents

CONTACT(S)..................................................................................................................... 1
STAKEHOLDER(S)........................................................................................................ 2
PURPOSE................................................................................................................... 2
DEFINITIONS............................................................................................................. 2
REQUIREMENTS....................................................................................................... 2
USER ACCESS CONTROL....................................................................................... 3
SYSTEM AND APPLICATION ACCESS CONTROL............................................. 3
USER RESPONSIBILITIES ...................................................................................... 4
VIOLATIONS ............................................................................................................. 4
Publication.................................................................................................................. 4
REVIEW SCHEDULE............................................................................................... 4

CONTACT(S)

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

PURPOSE
The purpose of this standard is to establish the guidelines on the issuance of access to authorized users and to define the requirements necessary to restrict access to IT systems.

DEFINITIONS

Access Control Policy - outlines the controls to a computer system and software in order to limit access to computer networks and data. It provides details including access control standards, user access, network access controls, operating system software controls, passwords, access to files and documents and specialized system access, controls for remote user access and other access as required.

Data Owners – Individuals at any level who oversee data management functions related to the capture, maintenance, and dissemination of data for a particular operational area. They are responsible for decisions about the usage of University data under their management and control.

Information Technology Resources are defined as computers, telecommunication equipment, networks, automated data processing, databases, the Internet, printing, management information systems, and related information, equipment, goods, and services.

IT Facilities – locations or facilities, fixed or mobile that contain Norfolk State University information technology equipment, systems, services, and personnel.

Sensitive System is a classification given to any IT system in which the loss to confidentiality, integrity, and/or availability of the system or data could have a material adverse effect on University interests or the privacy of individuals.

Private Information is 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.

REQUIREMENTS

1. An access control policy will be established, documented and reviewed and implemented based on business and information security requirements.

2. The policy will be reviewed and updated by data owners at regular intervals.
USER ACCESS CONTROL

Access to data will be controlled through a formal management process. A defined process for granting access will be implemented to assign or revoke access rights for all user types to all systems and services.

Access to sensitive IT systems, data and the facilities housing these items will be granted based on the principle of least privilege. Users will only be provided with access to the network and networks services that they have been specifically authorized to use.

Access to and use of privileged rights will be restricted and controlled.

Data Owners will review users' access rights at regular intervals.

The Department of Human Resources will conduct a background check for fulltime staff employees at the initial recruitment.

Physical and logical access rights will be removed upon personnel transfer or termination, or when requirements for access no longer exist.

Non-disclosure and security agreements for access to IT systems and data will be required, based on sensitivity and risk.

Separation of duties will be established to protect sensitive IT systems and data, or specific controls will be used when constraints or limitations of NSU processes preclude a separation of duties.

SYSTEM AND APPLICATION ACCESS CONTROL

Access to information and application system functions will be managed in accordance with the access control policy.

Where required, access to systems and applications will be controlled by a secure log-on procedure.

Based on the defined IT role, users, managers, officers and owners are responsible for ensuring that access control standards are followed for their respective IT resource.

Password management systems will be interactive and will ensure quality passwords.

The use of utility programs that might be capable of overriding system and application controls will be restricted and tightly controlled.

Access to program source code will be restricted.

Visitor access to IT facilities that house sensitive systems or data will be controlled.
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.

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 SharePoint Site and/or 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: