Access Control Procedures and Supplemental Guidance

Objective

Access Control document provides procedures and supplemental guidance in direct support of the WISP, Acceptable Use Policy, System Administrator Policy, User Account Policy, and Vendor Policy. Access controls are designed to minimize potential exposure to the University resulting from unauthorized use of resources and to preserve and protect the confidentiality, integrity, and availability of the University networks, systems, and applications.

Scope

Applies to Suffolk University faculty, staff, students, contractors, and vendors that connect to servers, applications, or network devices that contain or transmit Suffolk data, per Data Classification.

Access Control Procedures and Supplemental Guidance

In support of the Acceptable Use Policy, System Administrator Policy, User Account Policy, and Vendor Policy the following provisions are required to be followed.

Segregation of Duties

Access to any University system will only be provided to users based on an academic requirement, business requirement, job function, responsibilities, or need-to-know. All additions, changes, and deletions to individual system access must be approved by the appropriate supervisor and system owner, with a valid academic or business justification. Account creation, deletion, and modification as well as access to protected data and network resources is completed by the ITS resource system administrator with appropriate and authorized approval.

The System Administrator and or Application Administrator will audit all user and administrative access to the respective system. Discrepancies in access will be reported to the ISO and appropriate supervisor in the unit responsible and remediated accordingly. Documentation of review will be retained and submitted to ISO upon request.

User Access

All users of university systems will abide by the following set of rules:

- Users will not log in using generic, shared, or service accounts.
- Users with access to Confidential systems where possible will use Multi Factor Authentication or a unique account that is different from their normal University account. This account will conform to the Password Policy and User Account Policy.
- Authorized third parties with University remote access must use a unique authentication credential (such as a password/phrase) for each authorized individual.

VPN Access

Users may only gain access to the VPN environment if:

- Access required to perform a University approved business requirement.
- A Suffolk employee.
- A Suffolk-sponsored vendor.
- Suffolk Supervisor must approve user access.
- Users will abide by access control guidelines Acceptable Use Policy, User Account Policy, and any applicable policy specific to the Data Classification of the system (Confidential, Internal Use, Public).

Administrative Access

- Administrators will abide by the privileged access and user access guidelines in support of the System Admin Policy.
- Administrators will immediately revoke a user’s access when a change in employment status, job function, or responsibilities dictate the user no longer requires such access.
- All service accounts must be limited in use to accomplish a specific repeatable required function. Service accounts should not be used for more than one service, application, or system.
- Administrators must not extend a user group’s permissions in such a way that it provides inappropriate access to any user in that group.
- All servers, applications, and network devices, when feasible, shall contain a login banner that displays authorized use and adherence to university policies.

Minimum recommended banner information:

“Suffolk University Authorized Use Only. All university policies apply.”

Standard recommended banner information:

“Suffolk University Authorized Use Only. This system is restricted to authorized users for official use only and shall be in accordance with Suffolk University policies. Use of this system is subject to monitoring and audit. Unauthorized use is prohibited, and violations will be enforced.”

- The server System Administrator and or Application Administrator will be responsible for enabling/disabling accounts and monitoring access for the systems they administer. See System Administrator Policy

Remote Access

All users and administrators accessing University Systems must abide by the following rules:
• No unauthorized technology is allowed on any Suffolk network. This includes remote access technology, remote access applications (i.e., LogMeIn, TeamViewer, vendor monitoring tools), modems, wireless access points, or other unapproved remote access technology.

• All remote access must be authenticated and encrypted through the University’s VPN or an approved secure connection approved by the Information Security Officer.
• All directly connected remote access to University on campus resources will be accomplished using two-factor authentication; a username and password, and a second method not based on user credentials, such as hardware, certificate, or token, provisioned to the user.
• Any machine used for direct remote access must have approved antivirus software installed, up-to-date, running, and enabled. This requirement is enforced by a host checker component of the University’s VPN software.
• Any third party, a non-Suffolk affiliate that requires remote access to University Systems for support, maintenance, or administrative reasons must have
  ○ Suffolk sponsor designated to be the Point of Contact (POC)
  ○ Active contract with the University
  ○ Third-party user must be an individual user maintaining a valid official vendor email address specific to the vendor (i.e., not a shared email system like, yahoo.com, live.com, gmail.com).
  ○ All third-party access must be approved by the Information Security Officer or their designee.
  ○ Third parties may access only the systems that they support or maintain.
  ○ All third-party accounts on University Systems will be disabled and inactive unless needed for support or maintenance.
  ○ Third-party accounts must be immediately disabled after support or maintenance is complete.
• All third parties with access to University Systems must adhere to all University Policies, laws, regulations, and standards associated with that data.
• Confidential Data must not be copied from University systems to a user’s non-Suffolk issued machine. See Portable Device Policy, Acceptable Use Policy, Encryption Policy, Document and Data Storage Guidance, and WISP.
• Remote Access will be disconnected automatically after a specified time (10 hours).
• Users will abide by the above user access guidelines and supporting University Policies.

**Physical Access**

All ITS data centers will abide by the following physical security requirements:

• Video surveillance will be installed to monitor access into and out of ITS data centers.
• Access to ITS data centers will be accomplished through the use of electronic badge systems, biometrics, and or physical key management.
• Only the Facilities Department, ITS Infrastructure, and the Network Services Team will have physical key access.
• Physical access to ITS data centers is limited to ITS personnel, designated approved Suffolk University employees or contractors whose job function or responsibilities require such physical access.
• Visitors accessing ITS data centers will be accompanied by authorized ITS personnel, and all access will be documented. Documentation will be kept for at least a period of three months.
• Modification, additions, or deletions of physical access to ITS data centers will be accomplished by utilizing the ITS proxy and biometrics system.
• All terminated Suffolk personnel will have their access revoked immediately.
• Physical access requires the approval of the ITS Infrastructure Director and or the Network Services Director.
• The ITS Infrastructure Director or their designee will audit physical access to ITS data centers

Access to secured network rooms and or closets will be authorized by the ITS Infrastructure Director and or the Network Services Director through physical key management.

Rev 1.2

09/23/21 ITS Information Security Officer