User Account Policy

- Objective
- Applicability
- Definitions
- Policy
- Violation of Policy
- Revision History

Objective

The purpose of the User Account Management Policy is to ensure that access to all Suffolk systems and applications are properly approved and monitored.

Applicability

The User Account Policy applies to any student, any faculty or staff members, whether full- time or part-time, paid or unpaid, temporary or permanent, as well as all agents and representatives of the University, including any third party service provider providing services to the University who create, use or otherwise access or interact with any University

Information or University Information Resource ("University Users")..

Definitions

User Account: A combination of a unique user name and password that provides access to a University Information Resource.

University Information Resource: any tool, device, equipment, or system used to create, collect, record, process, store, retrieve, display and transmit University Information, including but not limited to email, mainframes, servers, computers, laptops, personal digital assistants (PDA), telecommunication resources, fax machines, printers, file cabinets, software and embedded technology.

Policy

Establishing User Accounts

- All User Accounts must have an associated request and approval that is appropriate for the system or service.
- All User Accounts created will have permissions only to University Information Resources that are necessary for an individual to perform his/her duties.
- All User Accounts must be uniquely identifiable and assigned to an individual.
- All User Accounts must have a password in accordance with the "Password Policy."

User Account Maintenance

- All access must be promptly removed when access is no longer needed or upon notification from authorized University personnel
- All account owners are accountable and responsible for the security and protection of their account and its use
- System Administrators or other designated University Staff:
  - are responsible for removing the User Accounts of individuals that change roles within the University or are no longer affiliated with the University
  - must establish a procedure for modifying a User Account
  - must periodically reviewing existing accounts

Violation of Policy

The University reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with this Policy. Violations of this Policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this Policy may result in dismissal from the University.

Revision History

Version	Date	Responsible University Office	Approved By

1.0	09/14/10	Provost Office	Provost Barry Brown