System Administrator Account Policy

Objective

The purpose of the System Administrator Account Policy is to ensure that access to all Suffolk systems and/or applications are properly approved and monitored.

Applicability

The Suffolk University System Administrator Account Policy applies to any University System Administrator and any individual that receives temporary System Administrator access to University systems and/or applications.

Definitions

Root System Administrator Account: root is the user name or account that by default has access to all commands and files on a system.

System Administrator: Individual responsible for the effective operation and maintenance of University systems and/or applications.

System Administrator Account: An account that has all access permissions, rights, or privileges to a University system and/or application.

Temporary account: An account on an as need basis that has rights or privileges to a University Information Resource, such as an account for a vendor to do; maintenance, software development, software installation – this account could be an Administrative account.

Policy

- All departments must submit to the Information Security Officer or Chief Information Officer a list of System Administrators for any University systems and/or applications. The list shall include the name of the System Administrator(s), Telephone Extension, Email Address, Operating System, System Name, IP Address and system's function.
- All System Administrator account users must not abuse their access privilege.
- All System Administrator Accounts must comply with the "Password Policy".
- The password for a Root System Administrator Account must change when an individual with the password is no longer affiliated with the University.
- University systems and applications with a single System Administrator must establish a password escrow procedure in the event the System Administrator is unavailable.
- Additionally Temporary System Administrator Accounts must be created with a specific expiration date or be removed when work is completed.
- Each System Administrator Account must also comply with the "User Account Policy".

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