

SUFFOLK UNIVERSITY
INFORMATION SECURITY POLICY MANUAL

TABLE OF CONTENTS

SUMMARY	2
ACCEPTABLE USE POLICY.....	3
ANTI-VIRUS POLICY	5
ENCRYPTION POLICY	7
INCIDENT RESPONSE POLICY & PROCEDURES.....	10
PASSWORD POLICY.....	14
PORTABLE DEVICE POLICY	16
SYSTEM ADMINISTRATOR ACCOUNT POLICY	19
USER ACCOUNT POLICY	21
VENDOR POLICY	23

SUMMARY

This collection of policies relates to the use of Suffolk University (“the University”) computer and network resources, and other University Information Resources, as well as to University requirements and standards concerning the privacy and security of various designated categories of information maintained by the University. These policies supplement and are incorporated by reference into the Suffolk University Written Information Security Program (the “WISP” or “the Program”). The WISP, together with these policies, describe the administrative, technical and physical safeguards employed to protect the security of information maintained by Suffolk University and to ensure that appropriate information resources are available when needed.

All users of the University’s information and information systems must read and understand their responsibilities under the WISP, including the policies contained in this Policy Manual. Any questions regarding the WISP, or this Policy Manual, should be directed to the Information Security Officer or the Assistant Provost for Information Management.

ACCEPTABLE USE POLICY

I. Objective

The purpose of the Acceptable Use Policy is to establish acceptable and appropriate use of University Information and University Information Resources, which exist to support the educational mission, business and other administrative requirements of Suffolk University.

II. Applicability

The Acceptable Use Policy applies to all University students, 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").

III. Definitions

University Information: any information in any form whether electronic, hardcopy, aural, or otherwise which is created, collected, stored, accessed or used in connection with the operation and/or management of the University, or which is created, collected, stored, accessed or used by a party authorized by the University.

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.

IV. Policy

The Suffolk University community is encouraged to make innovative and creative use of information and technology in support of the University's mission of education, research and public service. University Information and/or University Information Resources are to be used exclusively to advance the University's mission, including but not limited to research, teaching, learning, enrichment, dissemination of scholarly information, and in connection with administrative activities, official University business or other University-approved activities. University Information Resources are limited and should be used carefully with consideration and respect for the needs of others.

The University acknowledges that occasionally, University Users use University Information Resources for personal purposes. Such occasional, personal uses are permitted if they are not excessive, do not interfere with the performance of a faculty, staff, administrator or student's duties, do not interfere with the efficient operation of the University or its Information Resources and are not otherwise prohibited by law or this Policy or any other University policy.

Impermissible Use

University Information and/or University Information Resources may not be used or otherwise accessed for purposes which are unlawful, unethical, dishonest, damaging to the

reputation or resources of the University, in violation of University policy, in violation of the requirements and standards set forth in the Suffolk University Written Information Security Program (WISP), inconsistent with the University’s mission or likely to subject the University to liability.

Examples of impermissible use include, but are not limited to:

- Adversely affecting University Information Resources such as bandwidth, security, and/or performance
- Using University Information and/or University Information Resources to engage in activities that may harass, threaten or abuse others
- Using excessive amounts of storage
- Sending mass messages, junk mail, spam or other broadcast messages
- Sharing passwords to University systems
- Accessing University Information Resources for the purpose of viewing pornography or engaging in abusive conduct in a chat room or social media channel
- Tampering or degrading systems performance
- Sending, copying, storing or displaying copyrighted material, including illegally downloading or sharing music, movies, software or other files
- Introducing viruses, worms, Trojan Horses, spy ware, malware or other rogue programs or physically damaging systems
- Downloading, installing or running security programs or utilities that reveal or exploit weakness in the security of a system such as password cracking programs, packet sniffers, port scanners, unless authorized by the Information Security Officer or Chief Information Officer.

V. 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.

VI. Revision History

Date	Responsible University Office	Approved By
9/14/10	Information Technology Services	Provost Barry Brown

ANTI-VIRUS POLICY

I. Objective

The purpose of the Anti-Virus Policy is to establish the requirements for addressing Malware infection, prevention, detection and cleanup.

II. Applicability

The Anti-Virus Policy applies to all University students, 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”).

III. Definitions

Malware: includes Virus, Trojan Horse and Worm.

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.

IV. Policy

- All University Information Resources, whether connected to the Suffolk University network, or standalone, must use the Information Technology Services (ITS) management-issued virus protection software and configuration.
- All other non-University Information Resources must use ITS management-approved virus protection software and configuration, prior to any connection to a University Information Resource. For example, if a user is connecting to the University network through a personal computer, the user’s personal computer must use ITS management-approved virus protection software and configuration.
- The virus protection software must not be disabled or bypassed.
- The settings for the virus protection software must not be altered in a manner that will reduce the effectiveness of the software.
- The automatic update frequency of the virus protection software must not be altered to reduce the frequency of updates.
- Each E-mail gateway must utilize Suffolk University ITS management approved email virus protection software and must adhere to the Suffolk University rules for the setup and use of this software, which includes but is not limited to scanning of all inbound and outbound emails.
- Every Malware that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported. A user may become aware that a virus has not been automatically cleaned upon receipt of a pop-up message from the virus protection software.

In the event a user suspects that any University Information Resource may be infected by a virus, please contact the University's ITS Helpdesk immediately at 617-557-2000.

V. 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.

VI. Revision History

Date	Responsible University Office	Approved By
9/14/10	Information Technology Services	Provost Barry Brown

ENCRYPTION POLICY

I. Objective

The purpose of the Encryption Policy is to provide technical guidance to the University community on the use of Encryption technologies. More information regarding the specific types of information that must be encrypted can be found in the University's Written Information Security Program.

II. Applicability

Where technically feasible, the Encryption Policy applies to all 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.

III. Definitions

AES: Advanced Encryption Standard is cryptographic cipher that uses a block length of 128 bits and key lengths of 128, 192 or 256 bits to protect data.

Asymmetric Key: is a form of encryption where keys come in pairs. What one key encrypts, only the other can decrypt. This is used in digital signatures and also in public-key cryptography such as PGP where you share your public key with anyone. The data is encrypted with your unshared private key and can be decrypted with your public key that you have shared. The public-key cannot encrypt any data it can only decrypt a message already encrypted with the paired private key.

Elliptical Curve Key: is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.

Encryption: The process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

Encryption Key: a sequence of numbers used to encrypt or decrypt data.

Encryption Key Management: In Encryption it is the creation, distribution and maintenance of a secret key. It determines how secret keys are generated and made available to both parties.

Kerberos: is a secure method for authenticating a request for a service from a computer by providing an encrypted master ticket, which is created on initial user logon to a Kerberos system.

PGP: Pretty Good Privacy (PGP) is a computer program that provides cryptographic privacy and authentication. PGP is often used for signing, encrypting and decrypting e-mails to increase the security of e-mail communications. It is also used to provide disk and file encryption.

RSA: is an algorithm for public-key cryptography and is used for signing as well as encryption.

Secure Socket Layer (SSL): is a security protocol used to validate the identity of a Web site and to create an encrypted connection for sending sensitive data.

SSH: secure shell is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

Symmetric Key: An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message (example DES).

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.

IV. Policy

All Encryption must meet the following minimum requirements:

- Symmetric key lengths of at least 128 bit
- Asymmetric key lengths of at least 3072
- Elliptic Curve key lengths of at least 256 bit
- AES key lengths of at least 128 bit
- RSA key lengths of at least 3072
- Web server certificates SSLv3/TLSv1 (example secure web sites HTTPS)
- SSH version 2 (example network device administration)
- Kerberos (example windows server and connecting device)
- PGP – AES 128 bit (example whole disk, file, USB and email encryption)
- PGP – Public Keys RSA 3072 (example digital signatures and encrypted email).

The Information Security Officer must approve all Encryption technologies used on University Information Resources. Approved Encryption will be based on publicly proven algorithms and technologies. No other Encryption technology may be used.

Digital Certificates

- Public facing Secure Socket Layer (SSL) services must use digital certificates issued by a trusted authority approved by the Information Security Officer or Chief Information Officer.
- Non-public facing SSL services may use self-signed digital certificates when used for management purposes.

Encryption Key Management

- Encryption Key Management procedures must ensure that authorized users can access and decrypt all encrypted data and comply with data retention requirements. (see Retention Records Policy)
- Encryption keys must have at least 2 approved authorized users who can access and decrypt the applicable encrypted information.

- All Encryption keys must be treated as Confidential Information and must be stored securely. (See Data Classification Policy)

Some data is subject to encryption standards by law. To the extent that such legal requirements are different or more specific than required under this Policy, the applicable legal requirements shall be followed. For example, any use of credit cardholder data must follow PCI-DSS encryption requirements (see PCI-DSS standards <https://www.pcisecuritystandards.org>).

V. 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.

VI. Revision History

Date	Responsible University Office	Approved By
9/14/10	Information Technology Services	Provost Barry Brown

INCIDENT RESPONSE POLICY & PROCEDURES

I. Objective

The purpose of the University Incident Response Policy is to establish the responsibilities for reporting, investigating and responding to Security Incidents.

II. Applicability

The Incident Response Policy applies to all University students, 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”).

III. Definitions

Confidential Information: This information consists of University Information which falls into one of the following categories:

(a) Massachusetts Personal Information (as defined herein)

(b) Financial Customer Information (as defined herein)

(c) Records and information the University, or any of its employees or units, is required by law to keep confidential, including but not limited to the following:

(i) Personally identifiable information about students of the University, other than “directory information,” contained in “Education Records,” i.e. records “directly related to a student”, to the extent protected by the federal law known as the Family Educational Rights and Privacy Act or “FERPA”

(ii) Records pertaining to individuals receiving health care related services from any Massachusetts licensed clinic operated by the University, to the extent they are considered confidential under Massachusetts law.

(iii) Information considered privileged under Massachusetts law, including but not limited to information consisting of or relating to communications between an individual and an employee of the University acting in their professional capacity as a licensed psychotherapist, psychologist, mental health counselor, or sexual assault counselors.

(d) Information the University is required by contract, or by University policy, to keep confidential

(e) Other highly sensitive personal information about an individual the disclosure of which could foreseeably result in identity theft, financial fraud, damage to reputation, or acute embarrassment, or other significant harm to the individual. Examples of such

information include: information about a person's medical condition or physical or mental health; or personnel or employee payroll records.

(f) Other University Information that is proprietary to the University and that the University has a strong financial, strategic, or competitive interest in keeping confidential, or that the University is expected to keep confidential under applicable ethical norms. Examples of such information include: trade secret information, proprietary information relating to inventions or patents, research data, or personal information about volunteer research subjects collected in the course of human subject research.

Security Incident: any event that is known or suspected to cause Confidential Information to be accessed or used by an unauthorized person, and shall include any incident in which the University is required to make a notification under applicable law.

University Information: any information in any form whether electronic, hardcopy, aural, or otherwise which is created, collected, stored, accessed or used in connection with the operation and/or management of the University, or which is created, collected, stored, accessed or used by a party authorized by the University.

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.

IV. Policy

- All University Users are responsible for reporting known or suspected Security Incidents promptly, such as theft, loss of equipment or documents, or unauthorized access or unauthorized acquisition of Confidential Information to the Information Security Officer (ISO) by either telephone or by emailing: securityincident@suffolk.edu.
 - By way of illustration only, Security Incidents may include:
 - The theft or physical loss of computer equipment containing or suspected to contain Confidential Information
 - An unencrypted list of student names and social security numbers e-mailed to an unauthorized recipient
 - A firewall is accessed by an unauthorized entity
 - Printed copies of student loan applications are discovered in a publicly accessible dumpster.
- The University has established procedures to coordinate response to and resolution of Security Incidents (see Incident Response Procedures). The Assistant Provost for Information Management will document all responsive actions taken in connection with any Security Incident and will work with the Suffolk Incident Response Team (SIRT) to conduct a mandatory post-incident review of events and actions taken, if any, to ensure that the University undertakes any change in business practices relating to the protection of Confidential Information.
- Whenever necessary (e.g. in the event of a "Security Breach" as defined by M.G.L.c. 93H, s 1), external notification (e.g notification to affected individuals, government

agencies and/or the media) shall be made as required by law, and appropriate remedial or preventative action shall be taken to protect individuals potentially affected by the Security Incident. Decisions concerning the University's responsibilities with respect to external notification, and any appropriate remedial or preventative actions, shall be made by the Provost in consultation with SIRT.

V. Procedures

In the event of an actual or suspected Security Incident, procedures for responding will include the following steps:

- a. Discovery & Internal Reporting
Any University User who identifies an actual or potential Security Incident should report it promptly to the Information Security Officer (ISO) or by emailing securityincident@suffolk.edu. The user must secure the Confidential Information if he or she still has access to it.
- b. Assessment
The ISO and the Assistant Provost for Information Management will determine the likelihood that an actual Security Incident has occurred. If a Security Incident has occurred, the Assistant Provost for Information Management will notify SIRT, which includes the Provost's Office, Information Technology Services (ITS), Public Affairs, the General Counsel's Office, and any other applicable department as determined by the Provost's Office.
- c. Containment
SIRT will work with the applicable department to contain the Security Incident as soon as possible.
- d. Investigation
SIRT will work with the applicable department to investigate the Security Incident and document all findings.
- e. Resolution and Review
SIRT shall conduct a post Security Incident review of events and determine if changes should be made to mitigate risks and help prevent similar incidents.
- f. External Notification & Remedial and Preventative Actions
Whenever necessary (e.g. in the event of a "Security Breach" as defined by M.G.L.c. 93H, s 1), external notification (e.g notification to affected individuals, government agencies and/or the media) shall be made as required by law, and appropriate remedial or preventative action shall be taken to protect individuals potentially affected by the Security Incident. Decisions concerning the University's responsibilities with respect to external notification, and any appropriate remedial or preventative actions, shall be made by the Provost in consultation with the SIRT.
- g. Documentation

The ISO will document all Security Incidents, as well as any and all subsequent actions taken to assess, notify, contain, investigate and resolve the Security Incident (as applicable).

Documentation should include:

- How the incident was detected
- Relevant dates (including the suspected date of compromise, date the compromise was detected, date the incident was contained, date the incident was resolved)
- Names (including individuals added to the Suffolk Incident Response Team (SIRT), party responsible for compromising the University Information Resource, if known)
- Investigation and scope (including cause of the compromise, impact of the Security Incident, severity of the Security Incident, nature of the resolution)
- Proposed improvements to ensure future Security Incidents may be avoided or minimized.

VI. 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.

VII. Revision History

Date	Responsible University Office	Approved By
9/14/10	Information Technology Services	Provost Barry Brown

PASSWORD POLICY

I. Objective

The purpose of the Password Policy is to establish parameters for secure authentication when accessing University Information Resources. Access to University Information Resources by an unauthorized party may cause loss of information, a breach of confidentiality and/or integrity, and may compromise availability.

II. Applicability

The Password Policy applies to students, 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").

III. Definitions

University Information: any information in any form whether electronic, hardcopy, audial, or otherwise which is created, collected, stored, accessed or used in connection with the operation and/or management of the University, or which is created, collected, stored, accessed or used by a party authorized by the University.

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.

IV. Policy

- Any and all passwords, including initial passwords, must meet the following requirements when technically feasible:
 - must be changed at least every 120 days
 - must not be anything that can be easily tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc
 - must have a minimum length of 8 alphanumeric characters
 - must contain a mixture of both upper and lower case characters
 - must include at least two (2) numbers and one (1) special character, such as: # \$ % ^ * () _ + | ~ - = \ : ; < > ? , . / @
 - must lock a User Account after ten (10) invalid login attempts, and will require an authorized administrator to unlock the account
 - must be forced to be changed upon first use
 - must keep history for at least two (2) previous passwords
 - must be encrypted during transmission and storage
- A screen-saver or a power timeout shall be configured after a period of 15 minutes (staff) and 30 minutes (faculty) of idle activity to the extent technically feasible, and such timeout shall require password re-entry

- Default passwords must be changed prior to system use.
- Stored passwords must be encrypted when feasible.
- User account passwords must not be shared with anyone. Suffolk University Information Technology Services (ITS) and ITS third-party service providers will not ask for University User account passwords.
- University Users must not circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software, except for University User email which is password secured by the overlaying operating system on University User workstations or personal digital assistants (PDA).
- Computing devices must not be left unattended without enabling a password-protected screensaver or logging off of the device.

If a University User suspects or has reason to know that the security of a password may be compromised, the password must be changed immediately. Under such circumstances, University Users should immediately report the discovery to the Suffolk University ITS Help Desk (617) 557-2000.

Users should contact the ITS Helpdesk to change a password. When a user seeks a password change, ITS must undertake the following procedures:

- authenticate the User's identify before changing the password
- change to a strong password
- require the User to change the password at first login.

V. 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.

VI. Revision History

Date	Responsible University Office	Approved By
9/14/10	Information Technology Services	Provost Barry Brown

PORTABLE DEVICE POLICY

I. Objective

The purpose of the Suffolk University Portable Device Policy is to safeguard University Portable Devices and University Information on Portable Devices, including but not limited to laptops, flash drives, personal digital assistants (PDA), or hand held computers, which may be susceptible to theft or loss.

II. Applicability

The Portable Device Policy applies to 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.

III. Definitions

Confidential Information: This information consists of University Information which falls into one of the following categories:

(a) Massachusetts Personal Information (as defined herein)

(b) Financial Customer Information (as defined herein)

(c) Records and information the University, or any of its employees or units, is required by law to keep confidential, including but not limited to the following:

(i) Personally identifiable information about students of the University, other than "directory information," contained in "Education Records," i.e. records "directly related to a student", to the extent protected by the federal law known as the Family Educational Rights and Privacy Act or "FERPA"

(ii) Records pertaining to individuals receiving health care related services from any Massachusetts licensed clinic operated by the University

(iii) Information considered privileged under Massachusetts law, including but not limited to information consisting of or relating to communications between an individual and an employee of the University acting in their professional capacity as a licensed psychotherapist, psychologist, mental health counselor, or sexual assault counselors

(d) Information the University is required by contract, or by University policy, to keep confidential

(e) Other highly sensitive personal information about an individual the disclosure of which could foreseeably result in identity theft, financial fraud, damage to reputation, or acute embarrassment, or other significant harm to the individual. Examples of such

information include: information about a person's medical condition or physical or mental health; or personnel or employee payroll records

(f) Other University Information that is proprietary to the University and that the University has a strong financial, strategic, or competitive interest in keeping confidential, or that the University is expected to keep confidential under applicable ethical norms. Examples of such information include: trade secret information, proprietary information relating to inventions or patents, research data, or personal information about volunteer research subjects collected in the course of human subject research

Portable Devices: Any device that is easily carried or moved and capable of storing, sending and/or receiving data. These include, but are not limited to, laptops, PDAs, USB drives and cell phones.

Remote Wipe: The deletion of the contents of a Portable Device through a remote command or action by a University IT system administrator

University Information: any information in any form whether electronic, hardcopy, audial, or otherwise which is created, collected, stored, accessed or used in connection with the operation and/or management of the University, or which is created, collected, stored, accessed or used by a party authorized by the University

IV. Policy

Portable Devices present unique security concerns because they are easily carried or moved and susceptible to theft, electronic invasion or unintentional exposure of data. Any use, access or storage of University Information on any Portable Devices, whether provided by the University or not, must be protected and monitored as follows to ensure appropriate security, availability and integrity:

- Portable Devices must be physically locked or otherwise appropriately secured by its user/custodian when left unattended
- University Information stored on Portable Devices should be backed up to University servers to avoid losing or compromising information
- University issued laptops and PDAs must be capable of Remote Wiping
- University issued laptops and PDAs must be configured to timeout after a period of inactivity in accordance with the Password Policy
- All University issued laptops that access Confidential Information are required to be encrypted using University encryption software in accordance with the Encryption Policy
- Confidential Information must not be stored on unencrypted removable media (such as CDs, flash drives, USB drives, external hard disks, etc.)

Contact the Information Security Officer infosecurity@suffolk.edu for questions relating to this policy and for assistance with enabling appropriate security measures for laptops and other portable devices.

Reporting Loss or Theft of a Portable Device

In the event that any University issued Portable Device is lost or stolen, the University User shall report the incident immediately to the Information Security Officer and the University Police Department.

V. 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.

VI. Revision History

Date	Responsible University Office	Approved By
9/14/10	Information Technology Services	Provost Barry Brown

SYSTEM ADMINISTRATOR ACCOUNT POLICY

I. 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.

II. 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.

III. 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.

IV. 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"

V. 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.

VI. Revision History

Date	Responsible University Office	Approved By
9/14/10	Information Technology Services	Provost Barry Brown

USER ACCOUNT POLICY

I. 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.

II. 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”)

III. 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

IV. 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

V. 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.

VI. Revision History

Date	Responsible University Office	Approved By
9/14/10	Information Technology Services	Provost Barry Brown

VENDOR POLICY

I. Objective

The purpose of the University Vendor Policy is to establish requirements for the selection and approval of third-party service providers.

II. Applicability

The Suffolk University Vendor Policy applies to any third-party service provider that creates, uses or otherwise accesses or interacts with any University Information and/or University Information Resources.

III. Definitions

Confidential Information: This information consists of University Information which falls into one of the following categories:

(a) Massachusetts Personal Information (as defined herein)

(b) Financial Customer Information (as defined herein)

(c) Records and information the University, or any of its employees or units, is required by law to keep confidential, including but not limited to the following:

(i) Personally identifiable information about students of the University, other than "directory information," contained in "Education Records," i.e. records "directly related to a student", to the extent protected by the federal law known as the Family Educational Rights and Privacy Act or "FERPA"

(ii) Records pertaining to individuals receiving health care related services from any Massachusetts licensed clinic operated by the University

(iii) Information considered privileged under Massachusetts law, including but not limited to information consisting of or relating to communications between an individual and an employee of the University acting in their professional capacity as a licensed psychotherapist, psychologist, mental health counselor, or sexual assault counselors.

(d) Information the University is required by contract, or by University policy, to keep confidential

(e) Other highly sensitive personal information about an individual the disclosure of which could foreseeably result in identity theft, financial fraud, damage to reputation, or acute embarrassment, or other significant harm to the individual. Examples of such information include: information about a person's medical condition or physical or mental health; or personnel or employee payroll records

(f) Other University Information that is proprietary to the University and that the University has a strong financial, strategic, or competitive interest in keeping confidential,

or that the University is expected to keep confidential under applicable ethical norms. Examples of such information include: trade secret information, proprietary information relating to inventions or patents, research data, or personal information about volunteer research subjects collected in the course of human subject research

Security Incident: any event that is known or suspected to cause Confidential Information to be accessed or used by an unauthorized person, and shall include any incident in which the University is required to make a notification under applicable law.

IV. Policy

- Any Suffolk University faculty or staff member seeking to engage a third-party service provider who will access, handle or otherwise interact with Confidential Information must first contact the Assistant Provost for Information Management, who will (in consultation with the Office of General Counsel as appropriate) review the third-party's ability to implement and maintain security measures consistent with University policy and applicable law
- All third-party service providers must comply with the WISP and all other applicable University policies
- All third-party service providers that will access, handle or otherwise interact with Confidential Information must be required by contract to implement and maintain security measures consistent with University policy and applicable law to safeguard Confidential Information
- Upon termination of contract or at the request of University, the third-party service provider must surrender all University identification badges, access cards, equipment and supplies immediately
- All third-party service providers must report any actual or suspected Security Incidents directly to their University point of contact and Information Security Officer (infosecurity@suffolk.edu)

V. 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.

VI. Revision History

Date	Responsible University Office	Approved By
9/14/10	Information Technology Services	Provost Barry Brown