Incident Response Policy

Objective

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

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").

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, 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.

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 Cheif Information Security Officer (CISO) 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 Chief Information Officer with the Chief Information Security Officer 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 President in consultation with SIRT.

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 CISO and the Chief Information Officer (CIO) will determine the likelihood that an actual Security Incident has occurred. If a Security Incident has occurred, the CIO or CISO will notify SIRT, which includes the President, Information Technology Services (ITS), Public Affairs, the General Counsel's Office, and any other applicable department.

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 remedical or preventative actions, shall be made by the President 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.

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
1.1	02/12/13	Senior VP of Finance and Administration and Treasurer Office	Senior VP Danielle Manning
1.2	01/04/24	Information Security Office Revision: Title changes	CISO Paul Guarino