# Vendor Policy



## Objective

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

## 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.

## 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

- Any Suffolk University faculty or staff member seeking to engage a third-party service provider who will access, handle or otherwise interact with Suffolk University Information, to the extent necessary will be required to follow IT Governance and be reviewed for accessibility, data security and privacy, contract language by the appropriate department. Also, the review of third-party's ability to comply, implement and maintain measures and standards consistent with University policy, industry standards, 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 withConfidential Information must be required by contract to implement and maintain data security and data privacy measures consistent with University policy, industry standards, 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 Information, 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)

## 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 | 06/05/23 | Information Security Office<br>Revision: Updated required review of vendor third-party ability to meet university standards, governance process, and return of information | CISO Paul Guarino |