

<b>Document Name</b>	<b>Third Party Vendor Management Policy</b>
<b>Document Creation Date</b>	<b>12/09/2023</b>
<b>Document Created By</b>	<b>CISO</b>
<b>Version Control History</b>	<b>1.0</b>
<b>Document Reviewed Date</b>	<b>05/12/2024</b>
<b>Document Reviewed By</b>	<b>CISO-CSE &amp; CRO-CSE</b>
<b>Document Approved By</b>	<b>Standing Committee on Technology</b>

## CSE Third Party Vendor Management Policy

### I. Purpose

The Third-Party Vendor Security Management program, governed by the Information Security Team is an initiative to reduce the risk to Exchange Data and computing resources from Third-Party Providers. Information Security collaborates with the Legal Affairs Department, Procurement Department and Exchange Department to protect Information Technology Resources and digital intellectual property at the Exchange.

The purpose of this policy is to ensure that all vendors have appropriate controls to minimize risks that could adversely impact Confidentiality, Availability, and/or Integrity of the service or product.

### II. Scope and Applicability

- A. This Policy applies to all Exchange operations involving Exchange Information or its Information Technology Resources.
- B. This Policy applies to all Exchange Employees as well as adjunct faculty, Third-Party Providers to include contractors, consultants, temporary employees, and other third parties performing duties on behalf of the Exchange.

### III. Definitions

Capitalized terms shall have the meaning ascribed to them herein, and shall have the same meaning when used in the singular or plural form or any appropriate tense.

Availability: The principle of ensuring timely and reliable access to and use of Information based upon the concept of Least Privilege.

Confidentiality: The principle of preserving authorized restrictions on Information access and disclosure, including means for protecting personal privacy and proprietary information.

Contractor: A person or a company that undertakes a contract to provide materials or labour to perform a service.

Data: Data is element(s) of information in the form of facts, such as numbers, words, names, or descriptions of things from which "understandable information" can be derived.

Employee: Exchange staff and faculty, including non-exempt, exempt, and overseas staff and collegiate faculty.

Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual.

Information Technology Resource(s): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by CSE directly or by a third party under a contract with CSE which requires the use of such equipment. The term includes computers, mobile devices, software, firmware, services (including support services), and CSE's network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network.

Information System: Inter-related components of Information Resources working together for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Integrity: Ensuring records and the Information contained therein are accurate and Authentic by guarding against improper modification or destruction.

Third-Party Provider: Third party as an external entity, including, but not limited to, service providers, vendors, supply-side partners, demand-side partners, alliances, consortiums and investors, with or without a contractual relationship to the Exchange.

#### IV. **Third-Party Management**

##### A. Initial Screening

1. All Exchange departments engaging third-party IT products or services are required to undergo a security risk review of the requested product or service.
2. Based on the security review performed, the CSE Information Security Team will determine if a comprehensive security assessment will be required prior to entering into any agreement with the vendor.

**B. Comprehensive Security Assessment**

1. The Third-Party Provider should complete a security questionnaire like any security audit report of the vendor is present or not and present it before CSE IT authority.
2. For commonly and widely used off the shelf products this type of audited certification is not required.
3. The Information Security Team will review the security assessment and determine whether the Third-Party Provider complies with the Exchange security requirements. If the Third-Party Provider is non-compliant, compensating controls will need to be implemented and reassessed.

**C. Contracting Agreements**

1. Third-Party Providers that will store, process or transmit Data must:
  - a. Sign a Data Processing Agreement (DPA) if applicable.
  - b. Permit inclusion of CSE standard security clauses and language in all relevant contracts, which addresses compliance with CSE security policies, right to audit, right to access, right to monitor and compliance with applicable regulations where feasible.

**D. Subsequent Reviews**

1. Security reviews for third-party providers will cover a single use case and are required upon a new solution acquisition, changes in scope or use cases for current solutions, changes in system design or controls, business transfer, merger, or acquisition, and upon the renewal of current solutions.
2. Periodic review of a Third-Party Provider security posture and continued compliance will be conducted as needed, based upon changes in system use, design or controls, contract renewal or business transfer, merger, or acquisition.

**V. Exceptions**

Exceptions to this policy should be submitted to the CFO/CTO/Head of Information Security for review and approval. If an exception is requested a compensating control or safeguard should be documented and approved.

**VI. Enforcement**

- A. Any Employee, Contractor, or Third-Party Provider performing duties on behalf of the Exchange with knowledge of an alleged violation of this Policy shall notify the VP of Information Security as soon as practicable.
  
- B. Any Employee, Contractor, or other Third-Party Provider performing duties on behalf of the Exchange who violates this Policy may be denied access to Information Resources and may be subject to disciplinary action, up to and including termination of employment or contract or pursuit of legal action.

**Version Control History**

**Version Change Date:**

**Version Number:**

**Changes:**