| | |
|---|---|
| **Policy Title:** | Cybersecurity Incident Response and Business Continuity Policy |
| **Policy Owner:** | Information Technology Services |
| **Effective Date:** | 01/02/2025 |
| **Last Updated:** | 01/02/2025 |
| **Scheduled Review** | 01/02/2027 |
| **Related Policies:** | Acceptable Use of Computing Resources |
| **Related Forms:** | N/A |

## I. POLICY STATEMENT

It is of paramount importance that Seattle University maintains and/or quickly restores all critical functions of its information technology systems during and after a Cybersecurity Incident. Having a readily accessible plan to address such emergencies is critical to minimizing any disruption to the teaching, research, and other work central to the University's mission. Accordingly, this Cybersecurity Incident and Business Continuity Policy ("Policy") establishes the University's requirements for reporting a Cybersecurity Incident, identifies who at the University will receive reports of Cybersecurity Incidents, and identifies who at the University is responsible for developing, maintaining, and carrying out a Cybersecurity Incident Response Plan.

## II. PURPOSE & BACKGROUND

The purpose of this Policy is to describe the University's policy for ensuring that mission-critical services and processes are maintained or restored in the event of a Cybersecurity Incident.

## III. APPLICABILITY/RESPONSIBILITY

This Policy applies to all University personnel, contractors, and students.

## IV. DEFINITIONS

***Contractor:*** A third party, including an individual, sole proprietor, and/or business entity, or an agent, employee, or representative of the same, that supplies goods or services to the University through a contractual relationship (whether oral or written). The definition of contractor includes suppliers and vendors.

***Cybersecurity Incident:*** An actual or suspected event that jeopardizes the confidentiality, integrity, or availability of the University's information systems, networks, or data. This includes, but is not limited to, unauthorized access to systems or data, data breaches, malware infections, ransomware attacks, denial of service attacks, and any other activities that compromise or threaten the security of the University's information technology or digital assets.

***Key University Personnel/Key Personnel:*** Individuals within the University who hold a critical role or responsibility essential for the continuity and recovery of business operations during or after a Cybersecurity Incident, or during or after any component of a Cybersecurity Incident response. Key Personnel includes, but is not limited to, the University's President, Provost, the Vice President and University Counsel, the Chief Information Officer and Vice President for Information Technology, the Chief Financial Officer and Vice President for Finance and Business Affairs, and the Associate

Vice President of Information Technology and Information Security Officer.

***Personal Information:*** "Personally identifiable information," as defined in the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g, *et seq.*, as well as any information that relates to an identified or identifiable individual. This includes, but is not limited to names, address, social security numbers, dates of birth, driver's license numbers, passport numbers, and other government-issued identifiers; credit card numbers and bank account details; medical information and health insurance details; biometric data, such as fingerprints, facial recognition data, DNA, and other biological data; and any data that can be used to distinguish or trace an individual's identity, either directly or indirectly, through combinations of other information.

***Personnel:*** A combined reference to all non-student University community members, including faculty, staff, fellows, employees, and others. The term does not include contractors, suppliers, or vendors.

## V. POLICY REQUIREMENTS

**1.** **Report:** As soon as any individual becomes aware of an actual or suspected Cybersecurity Incident, they shall notify the Vice President and University Counsel ("VP & UC"), the Vice President for Information Technology ("VP for IT"), and the Associate Vice President and Information Security Officer ("AVP & ISO") using the following contact information:

Vice President and University Counsel

Jordan Talge
Vice President & University Counsel
talgej@seattleu.edu
(206) 296-2043

Vice President for Information Technology

Travis Nation
Chief Information Officer
Vice President for Information Technology
cio@seattleu.edu
nationt@seattleu.edu
(206) 296-2002

Associate Vice President and Information Security Officer

Jerry Vergeront
Associate Vice President
Information Security Officer
vergeront@seattleu.edu
(206) 296-5607

**2.** **Receipt of Report.** Upon receiving a report of an actual or suspected Cybersecurity Incident, the VP & UC, VP for IT, and AVP & ISO shall initiate the Cybersecurity Incident Response Plan.

**3.** **Cybersecurity Incident Response Plan.** The Cybersecurity Incident Response Plan ("Plan") shall be maintained by the AVP & ISO, who shall be responsible for developing, maintaining, and updating the Plan from time to time, on an as-needed basis. The Plan shall be kept confidential and disclosed only to those University trustees, officers, or employees who have a "need to know" in order to protect the best interests of the University.

### 4. Training and Awareness.

The AVP & ISO is responsible for ensuring that all community members are aware of this Policy.

The AVP & ISO will provide regular training sessions and resources to educate faculty, staff, students and other employees on identifying and reporting actual, potential, or suspected cybersecurity threats.

The AVP & ISO will ensure that those who have a need to know, based on the best interests of the University, are aware of and understand the University's Cybersecurity Incident Response Plan, and will provide regular training sessions and resources to educate those who have responsibilities under the Cybersecurity Incident Response Plan on how to carry out those responsibilities.

## VI. VIOLATIONS

Any violation of this Policy, including a failure to report an actual or suspected Cybersecurity Incident, and regardless of whether such actual or suspected Cybersecurity Incident causes injury to the University, may result in disciplinary action by the University in accordance with University policy, including the Faculty Handbook, Human Resources Policies, Code of Student Conduct, or applicable law, up to and including termination.

## VII. RELATED INFORMATION

| Item | Description |
|---|---|
| **University Links** | Seattle University Policy on the Acceptable Use of Computing Resources |
| **Forms** | N/A |
| **Related Links** | Information Technology Services<br>Office of University Counsel |
| **Procedures** | Cybersecurity Incident Response Plan |