SOUTHWESTERN OREGON COMMUNITY COLLEGE

AP 11000 Cyber Security Incident Response

Southwestern Oregon Community College's ("The College") intentions for publishing a Cyber Security Incident Response Procedure is to focus significant attention on data security and data security breaches and how Southwestern Oregon Community College's established culture of openness, trust and integrity should respond to such activity. Southwestern Oregon Community College Information Technology Services is committed to protecting Southwestern Oregon Community College's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

This procedure mandates that any individual who suspects that a theft, breach, or exposure of Southwestern Oregon Community College protected data or Southwestern Oregon Community College sensitive data has occurred must immediately provide a description of what occurred to Integrated Technology Services via e-mail to cyberincidentreporting@socc.edu, or by calling the Executive Director of Technology Services/CIO.

This procedure applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle protected or sensitive information of Southwestern Oregon Community College members. Any agreements with vendors will contain language similar that protects the College.

As soon as a theft, data breach, or exposure containing Southwestern Oregon Community College protected data or sensitive data is identified, the process of removing all access to that resource will begin. Once the Executive Director of Integrated Technology Services/CIO is informed of the theft, breach or exposure, the Executive Director of Integrated Technology Services/CIO will convene and chair an incident response team meeting. The team may include; but is not limited to, staff members from the following areas:

- ITS Response Team
- Administrative Services Risk Management
- Finance
- Communications
- Human Resources
- Student Services
- Additional individuals/departments may be included based on the data type involved as deemed necessary by the Executive Director of Integrated Technology Services/CIO.

Work with Forensic Investigators
As provided by the college cyber insurance, the insurer will provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a Communication Plan
Executive Director of Integrated Technology Services/CIO will work with the College's Emergency Management Team within their Incident Command Structure regarding communications with internal employees, the public, and those directly affected.

Enforcement
Any College staff or student found in violation of this procedure may be subject to disciplinary action. The College reserves the right to deactivate any user's access rights when necessary to preserve the integrity of ITS Resources.

The College reserves the right to report security violations or compromises to the appropriate authorities. This may include reporting violations of Federal, State, and local laws and regulations governing computer and network use, or required accreditation reporting. Anyone who violates this procedure may be held liable for damages to the college assets, including but not limited to the loss of information, computer software, and hardware, lost revenue due to disruption of normal business activities or system down time, and fines and judgments imposed as a direct result of the violation.

Adopted: December 2, 2020