Policy Number	703 001
Policy Title	Security Management Policy
Responsible Officers	Vice President, Information Technology
Responsible Offices	Information Technology Services
Summary	Columbia International University (CIU) is committed to safeguarding the integrity and confidentiality of our academic, financial, student and personnel data while providing guarded standards of availability to internal and external constituents. The purpose of this policy is to outline the basic data security protocol for all corporate information systems of CIU. It is essential that faculty, staff, and students familiarize themselves with this protocol to effectively maintain CIU data integrity and confidentiality.
Definitions	*Computer Resources*-Hardware and software components associated with the CIU network infrastructure to include telephones, PCs, printers, faxes, scanners, servers, switches, routers, cabling, fiber, etc. *Data/Information Breach* -Unauthorized disclosure of information that compromises the security, confidentiality, or integrity of the CIU system network, infrastructure, or data. *Information Data Stewards* -Individuals responsible for the management of specific information systems (usually a department head). *Information System*-Any systematic collection of students, personnel, academic or financial data that is stored on the CIU network and used to conduct CIU business. Information may be housed on a server(s) or on individual machines. *Ransomware* - A type of malicious software designed to block access to a company's data or computer system until a sum of money is paid.
Approving Body	Information Security Review Committee Academic Council; Administrative Council
Approval Date	September 1, 2010 Aca C (07.18.2022); Admin C (06.13.2022)
Last Revision	April 12, 2022
Re-evaluation Date	April 12, 2023
Departmental Impact	All CIU, Ben Lippen, and Pineview Employees and Students

Failure to follow the following policy may result in disciplinary action, including termination of employment.

Policy

It is the responsibility of CIU to protect our infrastructure and constituent data from potential corruption, loss, or malicious tampering and/or dissemination. It is also our responsibility to ensure CIU is operating within the spirit and letter of existing local, state, and federal legal and regulatory requirements that govern the use of computers, software, communications networks, and online material. As such CIU is committed to the following standards.

CIU will maintain an Information Security Review Committee consisting of information system stewards appointed by and responsible to the VP for Information Technology. The committee will meet at a minimum once a year and is responsible for:

- conducting an annual review of the information security policies.
- classifying and defining user restrictions and access to all CIU data and information systems.
- recommending business processes or control changes necessary for compliance with best practices.
- implementing policy changes and/or additions as approved by the VP for Information Technology.
- conducting or delegating annual risk assessments of all CIU information systems.
- inviting ad hoc agents to committee meetings for compliance input, definition, and clarification when necessary for specific policy reviews.

All computer resources, whether hardware or software, provided by CIU are:

- intended for use in conducting CIU business only.
- approved and registered with the IT Department.
- to be used by authorized employees, students, and volunteers.

IT will monitor network and computer related activity and files at its discretion in order to:

- protect the security and integrity of computing resources.
- protect CIU from legal liabilities.
- analyze usage patterns or investigate unusual or excessive activity.
- investigate apparent violations of the law.
- investigate apparent violations of CIU policy or standards; comply with legal requirements.
- respond to exigent circumstances.

CIU will comply with all legal requirements regarding copyright and licensing per government regulating agencies as noted in the CIU Copyright policy.

CIU will develop and maintain an information security education plan that will provide formal and informal training for all students, faculty, staff, and volunteers that will:

- raise awareness as to risks, threats, and potential damage.
- raise awareness of best practices.
- inform students, faculty, and staff as to their personal contribution in the use of sound security practices.

Encryption

All employees should adhere to the guidelines under the Encryption Guidelines on IT Policies page. Good security management requires that users adhere to acceptable limits of encryption to those algorithms that have received substantial public reviews and have been proven to work effectively.

Enforcement

CIU will convene a committee comprised of representatives from Human Resources (HR), the CFO, Security, Physical Plant, and Information Technology, to be chaired by the VP for Information Technology for the purpose of reviewing known or suspected violations per the enclosed policies. This committee may recommend disciplinary action in accordance with CIU standards as outlined in the employee handbook, student handbook, and technology handbook.

The committee is also responsible for determining the appropriate action and associated responsible parties in the event of mediation between external legal agents or public media.

Violations are to be reported to Information Technology or the appropriate Data Owner. Notification of a violation is considered sensitive information and will be handled with discretion. IT support will respond within 24 hours to the notification per the following:

- Document and record the violation in a password protected folder entitled Security Violations on the IT secure drive. Storage of the folder's password will be in the Password Safe in the event the VP for Information Technology is unavailable and access by authorized personnel is necessary.
- Inform the VP for Information Technology
- Take immediate action to contain any damage or potential damage to information and/or information systems (e.g., lock down account; terminate individual access; change password)

IT support will investigate the nature and damage of the violation and make recommendations to the VP for Information Technology as to the severity, course of action, and future prevention. The VP for Information Technology will communicate with the Information Security Enforcement Committee and at his/her discretion convene a meeting to determine necessary disciplinary action up to and including potential dismissal.

Hyperlinks

www.ciu.edu/policy