Policy Number	707.000
Policy Title	Data Breach Policy
Responsible Officer	Vice President of Information Technology
Responsible Office	Office of Information Technology
Summary	The purpose of this policy is to provide parameters and a process to report suspected thefts involving data, data breaches or exposures (including unauthorized access, use, or disclosure) to the appropriate Information Technology staff and other parties; and to outline the response to a confirmed theft, data breach or exposure.
Approving Body	12.08.2023 (Acad C); 11.15.2023 (Admin C)
Approval Date	12.08.2023
Re-evaluation Date	Fall 2026
Departmental Impact	All departments that use CIU data and information, including access to corporate email and reports.

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

Policy Statement

This policy covers parameters that need to be adhered to in the event of data breach on computer systems, network devices, email accounts (CIU or BLS), and/or any additional systems and outputs containing or transmitting protected or confidential data from corporate databases or applications.

Rationale

Institutional data is essential for business and academic operation. Such mission critical data must be managed securely and protected from improper use or unauthorized access.

Policy Procedures

Reporting Suspected Thefts, Data Breaches

Any individual who suspects that a theft, breach, or exposure of CIU protected or confidential data has occurred must immediately contact and provide a description of what occurred (i) via email to **cybersecurity@ciu.edu** and (ii) by calling 803-807-5199.

Upon notification of a suspected breach, the Information Security staff will investigate all reported data thefts, data breaches and exposures to confirm if a theft, breach, or exposure has occurred. The response to the suspected data breach will be done in accordance with internal IT incident response plans and procedures.

If the incident involves a suspected theft of technology equipment (computer, printer, phone, etc.), the individual must also notify the Department of Campus Safety in addition to the Office of Information Technology. The Department of Campus Safety will determine whether a local law enforcement agency should be contacted based on the location and details of the incident. Technology thefts or breaches that involve both physical and data resources may require a joint response from the Department of Campus Safety and the Information Security staff in accordance with local and national data breach response requirements. Although not required, employees who suspect a data incident are encouraged to notify the respective Data Owner or Manager as well. For a list of data owners and managers, click here.

Confirmed Theft, Data Breach or Exposure of CIU Protected or Confidential Data

As soon as a theft, data breach or exposure containing CIU protected or confidential data is identified in the Data Governance Policy, the process of removing all access to that resource will begin as soon as possible. If the information is available on a site outside of CIU, that site will be contacted to have the information removed as soon as possible. The IT Risk Subcommittee Chair will lead the command center response team to handle breaches or exposure. A roster of the command center response team will be maintained by the IT Risk Subcommittee Lead. The roster will be made up of Data Owners (or their delegates) and other key stakeholders across the organization.

The Marketing and Communications Department will handle all communications about the breach or exposure. The Information Security staff will work with the appropriate parties to remediate the root cause of the breach or exposure.

Third-Party Breaches or Exposures that Impact the Organization

As soon as a theft, data breach or exposure containing CIU protected or confidential data is identified being involved with a Third-Party Vendor, the process of removing all vendor access to that resource will begin as soon as possible. If the information is available on a site outside of CIU, that site will be contacted to have the information removed as soon as possible.

Inclusion Rules for Breach Types

For any data breaches, exposures, or thefts the IT Risk Subcommittee Lead will be responsible for using an established Breach Incident Inclusion Checklist to ensure all parties are communicated about the incident.

IT Risk Subcommittee Responsibility

In the event of a suspected data breach, the IT Risk Subcommittee will activate a command center to coordinate incident response activities to support the response to the breach and post recovery efforts. The IT Risk Subcommittee is also responsible for preparation activities (training, tabletop exercises, etc.) to ensure stakeholders are aware of risks and their responsibilities in the event of suspected data breaches. The IT Risk Subcommittee's Command Center will work with respective internal stakeholders and departmental representatives, in addition to local and national law enforcement agencies in the response effort. A Breach Response Checklist will guide the IT Risk Subcommittee's Command Center in the response effort.

Breach Response Checklist

For any data breaches, exposures, or thefts the Risk Subcommittee Lead will communicate a Breach Response Checklist to all those listed in the Breach Incident Inclusion Table to ensure all pre-identified risk response actions are being addressed.

Questions about this Policy

If you have questions about this policy, please contact the Information Security team at **cybersecurity@ciu.edu**.

Policy Adherence

Failure to follow this policy could result in disciplinary action as provided in the CIU Employee Handbook and/or CIU Student Handbook. Disciplinary action for not following this policy may include termination, as provided in the

applicable handbook.

Hyperlinks/References

www.ciu.edu/policy

Information Technology Security Management Policy

Revision Table