

Information Technology – Incident Response Procedure	Procedure Number	8.6.4P
	Effective Date	October 05, 2026

1.0 PURPOSE

This Incident Response Plan (IRP) outlines the procedures and responsibilities for responding to cybersecurity incidents at The College. The goal is to ensure a swift, effective, and coordinated response to minimize the impact of incidents on The College's operations, data, and reputation. Upon determining the level of the severity of the incident, a breach notification procedure outlined below will be activated.

2.0 REVISION HISTORY

Adopted on: 10/05/26

3.0 DEFINITIONS

- A. *College Data* – College data are assets of The College in any form or location that meets one or more of the following criteria:
 - a. Data that The College has a legal obligation to responsibly manage.
 - b. Data that is relevant to the operations, planning, management, control, reporting, auditing, and administration of The College.
 - c. Data that is created, received, maintained, or transmitted as a result of the function of The College.
 - d. Data that is included in an official College report.
 - e. Data that is used to derive any data element that meets the above criteria.
- B. *Cybersecurity Playbook* – A document internal to ITS that provides guidance on how to respond to specific types of cybersecurity incidents.
- C. *Data* – stored collection of information that may include symbols, words, sounds or images.
- D. *Data Breach* – Any unauthorized disclosure, misuse, alteration, destruction, or other compromise of information, such as unauthorized access.
- E. *Event* – Any observable occurrence in a system or network.
- F. *Family Educational Rights and Privacy Act (FERPA)* – A federal law enacted in 1974 that protects the privacy of student education records.
- G. *Gramm-Leach-Bliley Act (GLBA)* – A 1999 federal law in the United States designed to regulate how financial institutions handle, disclose, and protect consumers' private financial information.
- H. *Health Insurance Portability and Accountability Act (HIPAA)* – A United States federal law designed to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.
- I. *Incident* – A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
- J. *Incident Intake Checklist* – A document used to aid in taking a report of a cybersecurity incident to ensure necessary information is collected and investigation is not unnecessarily delayed.
- K. *Personally Identifiable Information (PII)* – nonpublic information relating to an individual that

reasonably identifies the individual and, if compromised, could cause significant harm to that individual or to The College. Examples may include, but are not limited to, social security numbers, credit card numbers, bank account information, student grades or disciplinary information, salary or employee performance information, donations, patient health information, information that The College has agreed to keep confidential and account passwords or encryption keys used to protect access to confidential College data.

- L. *Regulated Data* – Refers to information that is protected by federal, state, or industry regulations due to its sensitive nature. The handling, storage, and transmission of such data are subject to specific legal and compliance requirements. In the event of a security incident involving regulated data, additional notification, documentation, and remediation steps may be required.
- M. *Sensitive Information* – any information whose disclosure could cause harm to The College or its constituents including PII and proprietary information.

4.0 PROCEDURES

- A. Roles & Responsibilities – Incident Response Team (IRT)
 - a. **IT Cybersecurity Lead:** Incident Response Coordinator, responsible for managing the technical response.
 - b. **CIO:** Responsible for communication during the incident. Will share printouts and other resources needed with the rest of the team.
 - c. **IT Infrastructure Lead:** Provides technical support for containment and recovery.
 - d. **Legal Counsel:** Advises legal implications and compliance.
 - e. **Marketing & Communications:** Manages public communication and media relations.
 - f. **President’s Cabinet:** Provides strategic oversight and decision-making.
 - g. **FERPA Compliance Officer:** Provides guidance and oversight on FERPA related data.
 - h. **HIPAA Compliance Officer:** Provides guidance and oversight on HIPAA related data.
 - i. **Director of Risk Management:** Coordinates communication with our cyber insurance provider.
 - j. **Other Individuals Identified:** as needed.

- B. Incident Classification

Incidents at The College are classified into four severity levels:

- a. **Low:** Minor incidents such as spam emails or low-risk phishing attempts.
 - i. Handled by IT Cybersecurity Lead or Help Desk.
 - ii. No immediate escalation.
 - iii. Documented in ticketing system.
 - iv. No formal notification is required.
- b. **Moderate:** Malware detected and contained, unauthorized access attempts.
 - i. IT Cybersecurity Lead investigates and mitigates.
 - ii. Notify Infrastructure Engineer if system-level changes are needed.
 - iii. CIO is informed.
 - iv. Incident logged and reviewed post-resolution.

- c. **High:** Data exposure, system compromise, ransomware infection.
 - i. Immediate action by IT Cybersecurity Lead and Infrastructure Engineer.
 - ii. CIO is actively involved.
 - iii. Legal Counsel and Marketing & Communications are notified.
 - iv. Incident Response Team (IRT) convenes.
 - v. Begin documentation for potential regulatory reporting.
- d. **Critical:** Widespread system outage confirmed data breach involving sensitive information.
 - i. Full IRT activation.
 - ii. CIO leads communication efforts.
 - iii. Legal Counsel and Marketing & Communications coordinate external messaging.
 - iv. Relevant regulatory agencies are notified
 - v. Consider law enforcement or third-party forensics.
 - vi. The President's Cabinet is briefed.
 - vii. Post-incident reviews are mandatory.
- C. Regulated data must be retained and disposed of in accordance with applicable laws and The College's data retention policies. Secure deletion methods must be used when disposing of sensitive information.
 - a. This means either physical destruction of disks to be discarded or NIST approved sanitization methods for disks to be repurposed internally.
- D. Communication and Reporting Procedures
 - a. User Incident Reporting

Suspected incidents can be reported through multiple channels: email, support desk ticketing system, phone call, or Microsoft Teams. Regardless of the method, consistent questions should be asked and essential data collected using the Incident Intake Checklist.

 - i. Incident Intake Checklist
 1. Reporter's Name and Contact Info
 2. Date and Time of Report
 3. Method of Report
 4. Description of the Incident
 5. Systems or Services Affected
 6. Any Suspicious Activity Observed
 7. Screenshots, Emails, or Logs (if available)
 8. Has the Incident Been Contained or Is It Ongoing?
 9. Other Individuals or Departments Involved
 10. Initial Severity Assessment (if possible)
 - b. Notification
 - i. Internal Notifications

Depending on the severity, the following individuals are notified:

 1. CIO

2. Infrastructure Engineer
 3. Legal Counsel
 4. Marketing & Communications
 5. Executive Leadership
 6. Risk Management
 7. HIPAA\FERPA Compliance Officer(s)
- ii. External Notifications
- In certain cases, external parties may also be notified including, but limited to:
1. U.S. Department of Education (GLBA compliance)
 2. The Department of Health and Human Services (HIPAA compliance)
 3. Cyber Insurance Provider
 4. Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3)
 5. Federal Bureau of Investigation (FBI) Denver Field Office
 6. Cybersecurity and Infrastructure Security Agency (CISA)
 7. Wyoming CARE Team
- iii. A contact list is maintained within ITS internal documentation and will be provided to members of the IRT to ensure quick access to the right people when time is critical.
- iv. Marketing and Communications will handle communications
- E. ITS Incident Response Flow
- a. The ITS workflow outlined here is followed once an incident has been reported. This is a general guideline, and some of these steps may take place in a different order, multiple times, or not at all, depending on the situation.
 - i. Reporting
Incidents are reported through email, help desk ticketing system, phone call, Microsoft Teams, or in person to a member of ITS. Relevant information from the Incident Intake Checklist is gathered as quickly as possible to try to get information while it's still fresh.
 - ii. Detection and Classification
The IT Cybersecurity Lead assesses the incident and classifies it into one of four severity levels.
 - iii. Containment
Immediate actions are taken to isolate affected systems and prevent the spread of the incident.
 - iv. Eradication
The threat is removed, and affected systems are cleaned and secured.
 - v. Recovery
Systems are restored, and their integrity is verified.
 - vi. Communication
The CIO leads communication efforts, providing updates to leadership, stakeholders, and external parties as needed.

vii. **Post-Incident Review**

Depending on the assessed severity level, a review is conducted to identify lessons learned and improve future response efforts.

b. **Guidance on Using the Cybersecurity Playbook**

- i. For detailed procedures on containment, eradication, and recovery, refer to the Cybersecurity Playbook. The playbook provides step-by-step guidance for responding to different types of incidents, ensuring consistent and effective actions.

F. **Appendix**

a. **Examples of Regulated Data at The College**

The following categories of data commonly fall under regulatory oversight and may be present within The College systems:

i. **Personally Identifiable Information (PII)**

Includes names, Social Security numbers, dates of birth, addresses, and other data that can be used to identify an individual.

ii. **Financial Information**

Includes bank account numbers, credit card numbers, and financial aid records. Subject to regulations such as the Gramm-Leach-Bliley Act (GLBA).

iii. **Educational Records**

Includes student grades, transcripts, class schedules, and disciplinary records. Protected under the Family Educational Rights and Privacy Act (FERPA).

iv. **Health Information**

Includes medical records, disability documentation, and counseling notes. May be subject to the Health Insurance Portability and Accountability Act (HIPAA) if handled by covered entities.

v. **Authentication Credentials**

Includes usernames, passwords, security questions, and multi-factor authentication tokens.

vi. **Payment Card Information (PCI)**

Includes credit/debit card data processed through campus systems. Subject to PCI-DSS compliance requirements.

Note: This list is intended to provide examples and is not exhaustive. When in doubt, report the incident as a suspected exposure or breach in accordance with Section 5(A) of this procedure.