Information Technology Services
Juniata College

814.641.3619
help@juniata.edu

https://www.juniata.edu/offices/information-technology-services/index.php

Incident Management Plan

10/29/23 AMW

Incident Reporting

Juniata employees are expected to immediately report any actual or suspected security incident that involves:

- **unauthorized access** to the College's cloud or on-premise technology systems;
- unauthorized **disclosure or modification** of sensitive information;
- malicious **alteration or destruction** of data, information, or communications;
- unauthorized **interception or monitoring** of communications;
- loss of College-owned devices or media; and
- any unauthorized **destruction or damage** of IT resources.

Reports should be made to:

a. The Information Technology Help Desk at (814)641-3619;
b. the individual's supervisor; and
c. other individuals as required by the circumstances.

Incidents will be treated as confidential unless there is a need to release specific information.

Incident Response Procedures

1. This incident, if necessary, will be passed to the Incident Response Team. The CIO or designee leads the response process with the IT Security Team and includes other relevant parties as necessary. This may include working closely with 3rd party vendors in the event the incident has occurred in their systems.
    a. This constitutes the Incident Response Team. After initial notification, updates and communications are provided as appropriate throughout the incident response process, to both internal and external constituents.
    b. External support through 3rd parties is acquired if needed throughout the process.
2. The Incident Response Team:
    a. Creates a shared log of actions taken and maintains this log consistently throughout the response process.
    b. Secures the affected area(s) and identifies potential evidence, both physical and electronic, and determines if perishable evidence exists.
    c. Assesses the need for forensic analysis which can aid in understanding the nature and scope of the incident and provide evidence for any potential criminal investigation. During this process, the

potential value of forensic analysis vs. the immediate need to protect and restore College resources and services are considered. The decision process is documented.

d. Collects and saves any forensic information identified in the previous two steps. This may include video records, access logs, system logs, network traces, IP addresses, MAC addresses, data backups, system images, or affected computer hardware.
e. Regains control of the compromised system. This may include network disconnection, process termination, or other action as indicated to prevent further compromise of protected information.
f. Analyzes the intrusion. Documents the nature of the intrusion and its impact on information and process integrity. Determines if unauthorized individuals may have acquired protected information. Attempts to determine the identity of those whose data may have been acquired. Estimates the potential cost (time, money, and resources) of the intrusion to the College. If a breach (*any unauthorized disclosure, misuse, alteration, destruction or other compromise of protected information)* is detected, report as necessary.
g. Corrects any identifiable system or application vulnerabilities that allowed the intrusion to occur.
h. Verifies system and data integrity.
i. Restores service.

3. An incident report with relevant information is provided to necessary parties and includes:
4. Date and time the incident occurred;
    a. description of incident;
    b. detailed list of system(s) and data which were compromised;
    c. identifiable risks to other systems or information;
    d. corrective actions taken to prevent future occurrences;
    e. estimated costs of incident and any corrective actions; and
    f. identity of those responsible for the incident (if available).
5. Communications with the media and public is to be restricted to College employees designated to speak to the public on college related matters. College employees involved in the incident or the incident's response and investigation should refer all media and other public inquiries to the designated individual(s).

Human Resources, along with General Counsel as necessary, with input from the Incident Response Team and other appropriate individuals, determines if disciplinary action should be taken, criminal charges filed against those involved, and which individuals and regulatory bodies should be notified.

Juniata College will act in accordance with the Pennsylvania data breach notification law, P.L. 474, No. 94.