Bucknell
UNIVERSITY

Library and Information Technology
Computer Security Incident Response Policy

Summary

This policy defines the reporting and response to any Computer Security Incident that specifically threatens the security or privacy of Confidential Data. This policy applies to all Users. Computer Security Incidents apply to all computing or network devices owned, leased, or otherwise controlled by Bucknell University.

Confidential Data Security Incidents additionally apply to any computing or network device, regardless of ownership, on which is stored Confidential Data or by which access to Confidential Data might be gained.

Examples include, but aren't limited to:

- A home computer containing Confidential Data.
- A mobile device on which credentials are stored which could be used to access Confidential Data.
- A server housed in an off-site facility.

Objective

This policy defines the steps that staff and users must follow to ensure that Computer Security Incidents are identified, contained, investigated, and remedied.

Requirements

Users must promptly report any suspected or known Computer Security Incident to Library and Information Technology staff. Users will report Computer Security Incidents to Library and Information Technology by any of:

- Calling extension 7-7777, or 570-577-7777 from off campus
- Visiting the Technology Desk
- Contacting a departmental representative

A reported incident suspected, known, or determined to be a Confidential Data Security Incident will be handled according to procedures described herein.

1. If the reported incident is identified by the User to be a Confidential Data Security Incident:
   i. Report the incident to the Assistant Director of Information Security and Networking.

   ii. If the Assistant Director, in collaboration with other appropriate staff, determines that the incident is ***not*** a Confidential Data Security Incident, the incident shall be referred to an appropriate Assistant Director, who shall insure that the incident is handled in accordance with the procedures described herein.

   iii. The Assistant Director of Information Security and Networking shall inform the Director of Technology Infrastructure of the Confidential Data Security Incident. The Director will in turn inform the Chief Information Officer and the Director of Risk Management.

2. Library and Information Technology staff shall determine whether the incident is likely a Confidential Data Security Incident.

3. Library and Information Technology staff shall handle the Computer Security Incident according to established procedures, which lie outside the scope of this policy.

Incident Response Team

Purpose

The purpose of the Incident Response Team is to determine a course of action to appropriately address this incident.

Membership

The Chief Information Officer shall designate the membership of the Incident Response Team. Normally, membership will include appropriate individuals from Library and Information Technology, offices with primary responsibility for the compromised data, and, if necessary, General Counsel's office.

Responsibility

The responsibility of the Incident Response Team is to assess the actual or potential damage to the University caused by the Confidential Data Security Incident, and to develop and execute a plan to mitigate that damage.

Confidentiality

Incident Response Team members will share information regarding the incident outside of the team only on a need-to-know basis and only after consultation with and consensus by the entire team.

Response Priorities

The Incident Response Team should review, assess, and respond to the incident for which it was formed according to the following factors, in decreasing order of priority:

- Safety
  If the system involved in the incident affects human life or safety, responding in an appropriate, rapid fashion is the most important priority.

- Urgent concerns
  Departments and offices may have urgent concerns about the availability or integrity of critical systems or data that must be addressed promptly. Appropriate Library and Information Technology staff shall be available for consultation in such cases.

- Scope
  Work to promptly establish the scope of the incident and to identify the extent of systems and data affected.

- Containment
  After life and safety issues have been resolved, identify and implement actions to mitigate the spread of the incident and its consequences. Such actions might well include requiring that affected systems be disconnected from the network.
- Preservation of evidence
  Promptly develop a plan to identify and implement steps for the preservation of evidence,

consistent with needs to restore availability. The plan might include steps to clone a hard disk, preserve log information, or capture screen information.

Preservation of evidence should be addressed as quickly as possible in order to restore availability of the affected systems as soon as practicable.

- Investigation
  Investigate the causes and circumstances of the incident, and determine future preventative actions.

- Incident-specific risk mitigation
  Identify and recommend strategies to mitigate the risk of harm arising from this incident.

Senior Response Team Formation

If, in the judgment of the Chief Information Officer, the incident might reasonably be expected to cause significant harm to the subjects of the data or to Bucknell University, the Chief Information Officer may recommend to the Provost or to an appropriate Vice President that a Senior Response Team be established. The Senior Response Team shall be comprised of senior-level administrators designated and recommended by the Provost or Vice President.

The Senior Response Team will determine, with assistance and input from General Counsel, whether Bucknell University should make best efforts to notify individuals who's personally identifiable information might have been at risk due to the incident. In making this determination, the following factors shall be considered:

a. Legal duty to notify
b. Length of compromise
c. Human involvement
d. Sensitivity of compromised data
e. Existence of evidence that data were compromised
f. Existence of evidence that affected systems were compromised for reasons other than accessing and acquiring data
g. Additional factors recommended for consideration by members of the Incident Response Team or Senior Response Team

Documentation

a. Log of security incidents
   Library and Information Technology shall maintain a log of all Confidential Data Security Incidents, recording the date, type of Confidential Data affected, number of subjects affected (if applicable), summary of the reason for the breach, and corrective measures taken.

b. Incident report
   Library and Information Technology shall issue a report for every Confidential Data Security Incident describing the incident in detail, the circumstances that led to the incident, and a plan to eliminate the risk of a future occurrence.

c. Annual summary report

Library and Information Technology shall provide annually to the Chief Information Officer a report containing statistics and summary-level information about all known Confidential Data Security Incidents, along with recommendations and plans to mitigate the risks that led to those incidents.

Definitions

Confidential Data includes:

- Sensitive personally-identifiable information
  Information relating to an individual that reasonably identifies the individual and, if compromised, could cause significant harm to that individual or to Bucknell University.

  Examples include, but are not limited to:

  - Social Security Numbers
  - Credit card account numbers
  - Salary information
  - FERPA protected information
  - HIPAA protected information
  - Passwords and other access credentials

- Proprietary information
  Data, information, or intellectual property, in which the University has an exclusive legal interest or ownership right and which, if compromised, could cause significant harm to Bucknell University.

  Examples include, but are not limited to:

  - Financial information
  - Business planning data
  - Data, software, or other material from third parties which the University has agreed to keep confidential

- Any other data, the disclosure of which could cause significant harm to Bucknell University.

User
A Bucknell User is any faculty, staff, student, courtesy account holder, consultant, contractor, or agent of any of the above.

Malware
Any software designed with malicious intent.

Examples include, but aren't limited to:

- Viruses
- Worms
- Trojan horses
- Spyware

Computer Security Incident
A Computer Security Incident is any event that threatens the confidentiality, integrity, or availability of

University systems, applications, data, or networks.

Examples of University systems include, but are not limited to:

- Servers
- Desktop computers
- Laptop computers
- Workstations
- Mobile devices
- Network equipment

Examples of Computer Security Incidents include, but aren't limited to:

- Unauthorized access
- Intentionally targeted but unsuccessful unauthorized access
- Accidental disclosure of Confidential Data
- Infection by malware
- Denial-of-service attack
- Theft or loss of a University system

Confidential Data Security Incident

Any Computer Security Incident that specifically threatens the security or privacy of Confidential Data.