

Reporting A Suspected Information Security Breach Or Violation & Incident Response Procedures

This policy describes procedures employees must follow when an *information security breach* is suspected. This policy also outlines the roles and responsibilities for incident response when an actual breach has occurred. This policy applies to all university employees and all individuals having access to information for which the university has a duty to protect.

1. **Information Security Breach Defined**

For purposes of this policy, a suspected *information security breach* has occurred when any employee has reason to believe a university-owned and managed information system has been accessed by unauthorized individuals, or when an employee has reason to believe confidential information has been disclosed to a person not authorized to receive it. Examples of information security breach which require immediate reporting include:

- A. Loss or theft of computers (such as laptops), PDAs, or any storage device (such as backup tapes or flash drives) which may have contained confidential, sensitive or personal information.
- B. Suspected access or use of confidential information inconsistent with university responsibilities, such as an employee who uses an assigned account to access student records for personal or unapproved reasons.
- C. Evidence of suspected attacks against university information systems such as website defacements, account lockouts due to excessive password guessing, sudden appearance of inappropriate or unexpected files indicating possible inappropriate system access, the appearance of accounts within file servers which are unaccounted for, system log files indicating a high number of failed access attempts or unexplained successful access attempts, or the sudden disappearance of log files from servers.
- D. Possible virus or other malware infections not instantly resolved by properly installed and configured anti-virus software.
- E. Loss or theft of paper records containing confidential information.

2. **Reporting of Suspected Information Security Breaches**

Persons who have reason to believe a theft, breach, or exposure of Ball State University protected information may have has occurred must *immediately*:

- A. **Notify the BSU Computer Security Incident Response Team (CSIRT):** Report the suspected incident to the CSIRT immediately. *Under no circumstances may reporting be delayed to try to determine if a breach or exposure has occurred.* The BSU CSIRT can be reached by calling the UCS Helpdesk (765-285-1517) or computer operations support (765-285-1549) any time of day or night and asking to report a suspected information security breach. In certain situations, a recording at the above numbers may give instructions to call an after-hours emergency cell phone to reach the CSIRT directly.

When reporting an incident it is helpful to have the following information ready, however do not delay reporting to attempt to gather these details:

- i. **Reporting person's contact information.**
(do not wait for a supervisor; report the incident immediately).
- ii. **Description of incident.**
(try to be concise, explain what is known and avoid speculation).
- iii. **If the breach may have involved confidential information.**
(and if so, what type of records may have been involved).
- iv. **Date and time the incident was discovered.**
- v. **Make and model of the affected device.**
- vi. **If the system is still powered on and connected to the network.**
- vii. **If confidential information on the device or media was encrypted.**

B. Disconnect And Isolate Involved Computers: Never attempt to “fix” a computer or server which may have been breached. If possible, disconnect the network cable, however do not shut down or power off the equipment unless instructed to do so.

C. Confidentiality: Do not discuss a suspected breach with anyone other than the CSIRT team, the *Office of University Compliance*, or *University Police* unless directed to do so. Refer any media inquiries to *University Marketing and Communications* as that office will have the most complete and accurate information concerning the incident.

3. Incident Response

The CSIRT team responds to significant information security incidents 24 hours a day, 365 days a year and coordinates response efforts of all parties. The CSIRT will investigate reported data breaches and exposures to confirm if an incident has occurred.

4. Suspected Information Security Breach Incident Response Procedures

Depending on the nature of the incident, the CSIRT may immediately disconnect (or require others to disconnect) information systems which the CSIRT believes may present a significant risk. Disconnected computers may not be brought back on-line until the CSIRT determines the threat has been mitigated. In the event CSIRT disconnects systems or equipment, reasonable efforts will be made to notify the local administrator. The CSIRT will also notify the *UCS Helpdesk* and *UCS Operations Support* if warranted so they are aware of any services interruption.

5. Confirmed Information Security Breach Incident Response Procedures

As soon as a significant theft, data breach or exposure containing Ball State University confidential information is identified, the *Office of Information Security Services* will:

- A. Convene The CSIRT:** The CSIRT has responsibility for coordinating the university's response to information security breach or exposure incidents. The team may include members from:
- i. Information Technology
 - ii. University Police
 - iii. University Marketing and Communications (UMC)
 - iv. The Office of University Compliance
 - v. The department hosting the involved system which may have been breached

vi. Additional individuals as deemed necessary by the team

- B. Isolate Involved Computers:** All access to the involved server or computer will be suspended. If the breach involves an external vendor, the vendor will be contacted by the CSIRT to direct access be restricted.
- C. Contact University Police:** University Police will be notified when theft of physical property or criminal activity is suspected to have occurred.
- D. Contact University Marketing And Communications (UMC):** UMC will have all responsibility for media communications; no person is authorized to speak to the media without prior approval from UMC.
- E. Report Incident Response Status To University Administration:** The CSIRT will make ongoing and periodic updates to the *Vice President For Information Technology* concerning the status of the suspected breach and associated incident response. The CSIRT will also work with the appropriate parties to remediate the root cause of the breach or exposure, and upon incident resolution will make a final report of its findings to the *Vice President For Information Technology*, who will advise the *President* and the *President's cabinet*.

6. Policy Adherence

Refer questions about this policy to the *Office of Information Security Services* by e-mail to the Office of Information Security Services at security@bsu.edu.