Office of Information Technology

Procedure #: 00001-A
Procedure Title: Procedure for responding to a possible exposure of sensitive University data
Version Number: 2.0
Posting Date: February 2, 2012
Revision Date: May 21, 2024
Responsible Executive: CISO
Contact: OIT Service Desk

Purpose

The purpose of this procedure is to provide appropriate steps to follow if sensitive University data is exposed to unauthorized individuals. This response to any potential data breach situation will fulfill the University's legal and contractual obligations and will minimize the risk to any people who may be affected by the potential data exposure as well as minimize the risk to the University.

If you believe your computer, communications device or storage medium has been lost, stolen, or tampered with, please call the OIT Service Desk at 609-258-HELP for immediate assistance.

Data exposure possibilities

The steps in this procedure relate to the following situations in which sensitive University data might possibly become exposed to unauthorized individuals:

- A computer, mobile device, or removable storage media (like a thumb drive or external drive) is lost or stolen.
- Sensitive information is discovered to be accessible to unauthorized individuals, whether inside or outside the University.
- It was discovered that sensitive information was distributed to unauthorized individuals.
- A University device or a University administrative or academic system may have been compromised.

Reporting potential data exposure

Members of the Princeton University community:

- If you experience a possible data breach, contact the OIT Service Desk by calling (609) 258-HELP to report the incident. If you are faculty or staff, you also may choose to ask a member of your department's technology support team (e.g., SCAD/DCS or your OIT support person) to report the incident on your behalf.

- If your computer, mobile device, or removable media was stolen or lost, contact the OIT Service Desk by calling (609) 258-HELP to report the theft. Also contact the University's Department of Public Safety by calling (609) 258-1000. If the device was stolen or lost off-campus, also file a report with local law enforcement or security authorities. Princeton Public Safety will want a copy of their report.

Office of Information Technology

Procedure #: 00001-A
Procedure Title: Procedure for responding to a possible exposure of sensitive University data
Version Number: 2.0
Posting Date: February 2, 2012
Revision Date: May 21, 2024
Responsible Executive: CISO
Contact: OIT Service Desk

Individuals unaffiliated with the University:

- Individuals unaffiliated with the University community who recover a lost computer, mobile device, or removable storage media belonging to the University, who detect suspicious behavior from a University computer, or who discover University information exposed on the Internet that is sensitive in nature, are encouraged to notify the University's Computer Incident Response Team by sending an email message to abuse@princeton.edu or by phoning the Service Desk at (609) 258-HELP.

For technical support staff: Reporting potential data exposure for an individual you support

- If you are contacted by an individual reporting a possible data exposure situation, and you are the individual's IT support person (e.g., SCAD/DCS, OIT support), a member of the University's Computer Incident Response Team (CIRT), or a member of the Department of Public Safety, notify the OIT Service Desk about the incident. The OIT Service Desk is responsible for ensuring that the appropriate computer support person and CIRT team member are aware of the possibility that a data breach may have occurred. If the breach involves a stolen University device, be sure Public Safety is advised of the matter.

Responding to reports of possible compromised computers

- In cases where it is suspected that a computer has been compromised, the appropriate computer support person should make a forensic copy of the computer's hard drive(s) and determine whether the attack was capable of exposing data on the system or was a well-known attack capable only of service disruption. If the attack was capable only of service disruption, the computer support person should reimage the system and notify the OIT Service Desk that the incident can be closed.

- If the case remains open, the OIT Service Desk will notify the member of the University's Computer Incident Response Team on call, who will serve as the Process Manager (PM) throughout the execution of the breach procedure.

Once OIT is notified of the incident

The OIT Service Desk will contact a member of the Data Breach Investigation and Response Team. The team member will initiate the University's procedure for handling a potential data breach.

During the process, one or more members of the data breach response team will contact the user of the lost, stolen, or compromised device and/or the IT support person associated with the device for information, clarification, and to discuss remedial actions.

Office of Information Technology

Procedure #: 00001-A
Procedure Title: Procedure for responding to a possible exposure of sensitive University data
Version Number: 2.0
Posting Date: February 2, 2012
Revision Date: May 21, 2024
Responsible Executive: CISO
Contact: OIT Service Desk

Appendix A --- Key Definitions

- **Sensitive Information** requires a higher level of protection because:
    - It is confidential in nature (i.e., disclosure to unauthorized individuals would violate existing laws or University contracts, or could incur financial or reputational loss for the University and/or its constituents),
    - Significant impact would be incurred if its integrity were compromised, and/or
    - It is necessary to have the information available on demand.

The following are examples of specific types of sensitive information that, if exposed to unauthorized individuals, could pose serious consequences for the University:

Personally Identifiable Information (PII) is any information about a person that, if it were exposed to unauthorized individuals, could result in identity theft. This type of data includes name associated with social security number, driver's license number, credit card numbers or bank account numbers with or without associated PIN.

Legislatively Protected Information is information that is subject to government regulatory oversight.

- The Family Educational Rights and Privacy Act (FERPA) – protection of student records
- Gramm-Leach-Bliley Act (GLBA) – protection of financial records
- The Health Insurance Portability and Accountability Act (HIPAA) – protection of health care records
- State privacy legislation

Contractually Protected Information is information for which specific data protection obligations have been defined within the University's contract with another individual or organization. Contractually Protected Information includes credit and debit card information that is protected by our contracts with our merchant bank and the Payment Card Industry (PCI).

Other Sensitive Information is information for which unauthorized disclosure could lead to a business, financial and/or reputational loss. These data include business related data, such as payroll information, benefit information, work history and other personnel information, alumni contributions, budget information, research findings, tools, and methods.

Data Breach – A condition that occurs when sensitive information is available to be viewed or obtained by an unauthorized individual.

Affected Individual – An individual or household whose personal information has been exposed to unauthorized viewing or access.