Office of the Chancellor
Pennsylvania State System of Higher Education

Information Technology Security Guidelines Number 2010-04
Guidelines on Breach Notification

Approved by: CITO

History: Issued 4/16/2010

Revised --

Additional History

Related Policies:

Additional References:

I. Introduction

The purpose of these guidelines is to establish a PASSHE approach to lost or stolen Information Technology (IT) devices or PASSHE data and the steps to take for notification.

II. Guidelines:

1) If an IT device or PASSHE data, regardless of where it is stored (paper, personal device, or PASSHE provided device) is lost or stolen, or if confidential data is accessed by an unauthorized user, contact PASSHE Legal Counsel immediately, as well as university and OOC IT. They will assist in performing an assessment as to whether confidential or sensitive information is on the device (as defined by the OOC Guidelines on Data Classification). Refer to Attachment A: Security Breach Checklist.
2) The legal division, University IT and OOC IT will provide information on notification guidelines in the event that confidential or sensitive information may have been compromised. Title 73, Breach of Personal Information Notification Act will be used as the model for notification.

ATTACHMENT A: SECURITY BREACH CHECKLIST

Step 1 – Make a Preliminary Assessment of the Incident

- ☐ When and where did the security breach occur?
- ☐ What devices or data were lost, stolen or breached?
- ☐ If devices were stolen, were they immediately reported to law enforcement?
- ☐ What potential data might be involved? (Refer to Data Classification Guidelines)
- ☐ Can the data be used for fraudulent or other purposes?
- ☐ Have the security or access issues been resolved to prevent additional data loss?
- ☐ Is there other information at risk?
- ☐ How many individuals were affected by the security breach?

Step 2 – Notify Appropriate People within the System & University

- ☐ Make the following contacts:
    a. Information Technology
    b. PASSHE Legal Counsel
    c. Executive responsible for the business area
    d. External Affairs
    e. Depending upon severity, notify university and/or OOC executive staff

Step 3 – Further Evaluate the Scope of the Incident

- ☐ Does there appear to be evidence of suspicious behavior or negligence by an employee?
- ☐ Was there criminal intent by an employee? If so, is an external investigation warranted?
- ☐ Does a backup of the system/data exist?
- ☐ Is there a similar functioning device that can be analyzed to help determine the risk?
- ☐ Does Human Resources need to be involved?
- ☐ If there was physical damage to a building, consider additional security improvements?
- ☐ Do the access codes or locks for the building need to be updated?
- ☐ Were users' ID and passwords disabled that might have been associated with the stolen or lost devices?
- ☐ Should employees be briefed on the situation?
- ☐ Has a key person within the organization been identified to monitor the progress and communicate the actions to the appropriate people identified in Step 2 of this checklist?

Step 4 – Determine Need to Notify Public

- ☐ Do Office of the Chancellor employees need to be informed of the incident?
- ☐ Should the public be notified of the incident? If so, consider the following:
    a. Develop talking points
        i. Key Message
        ii. Next steps
    b. Press Release
    c. Press Conference
    d. Any National Associations that could assist in communicating the information to the public
- ☐ If law enforcement was involved, did the organization consult with them to determine the timing of what and when details of the security breach could be released to the public?
- ☐ Has an individual been designated as the contact person for releasing information?
- ☐ Have the communication messages regarding the security breach been coordinated between the employees, universities, and the public?
- ☐ Does the organization need to notify affected citizens?

Step 5 – Communication to the Public

- ☐ How are affected individuals going to be notified of the potential identity theft?
- ☐ Has a notification letter been prepared announcing the incident to the affected individuals?
- ☐ Should a fact sheet be created with the following key elements?
    a. Outline the incident
    b. Explain the actions currently being taken by the organization
    c. Include the contact information (e.g. the toll free number and web site)
    d. Any other pertinent information
- ☐ Does a toll free number need to be established to address questions from the individuals?
- ☐ Does a call center need to be established to handle the calls?
- ☐ Should questions and answers be developed and shared with the individual(s)?
- ☐ Would a web site be beneficial to share information with the individual on the incident and next steps?
- ☐ What types of services need to be arranged for affected individuals in order to mitigate the data breach?
    a. Does a contract need to be setup with one of the credit bureaus (e.g. Equifax, Experian or TransUnion) to provide free credit monitoring for affected individuals?

b. How often should the credit bureau track statistics and report any identity thefts to your agency?

c. If a contract is established with one of the credit bureaus, how will the information be communicated to the individuals?

d. Does a reminder letter on the credit services need to be sent to the citizens?

e. When the credit bureau is unable to locate a credit file for an individual, should a notification be sent?

Step 6 – Analyze Need to Address Data Security Weaknesses

- ☐ Did the organization have full disk encryption on the hardware devices?
- ☐ Was the security software up-to-date?
- ☐ Did the organization employ other local security measures outside of encryption (i.e. password protected files, multiple factor authentication, etc.)?
- ☐ Did the organization have security policies in place? If so, were the policies followed? If not, do guidelines need to be implemented?
- ☐ Does the organization need to conduct a security assessment?
- ☐ Should this type of data be stored in the current location?
- ☐ Does the access to the data need to be restricted?
- ☐ Was the data being saved to the network and not to the local hard drives?
- ☐ If the data should be stored in that particular location, is there a way to truncate the information?
- ☐ Are policies in need of modifications?
- ☐ Identify opportunities for user education.