Policy IT029: Breach/Data Leak Notification Policy

Recommended for Approval by: Fawn Petrosky, Vice President for Finance

Approved by: Dr. Dale-Elizabeth Pehrsson, President

Effective Date: 2/24/2023

A. Intent

The purpose of this Policy is to establish a consistent approach to the handling of lost or stolen Pennsylvania Western University (PennWest) Information Technology (IT) devices or data. It will also define the steps to take for notification when necessary.

B. Definition(s)

Not applicable.

C. Policy

All policies of the University will be in conformity with all applicable Federal and Pennsylvania statutes and regulations. All policies need to be consistent with Board of Governors policies and Pennsylvania State System of Higher Education collective bargaining agreements.

D. Procedure(s)

1. If a University-owned IT device or PennWest data, regardless of where it is stored (paper, personal device, or University provided device) is lost or stolen, or if confidential data is accessed by an unauthorized user, contact University Technology Services immediately.
2. Information Technology Services, upon being notified will contact PASSHE Legal Counsel. They will assist in performing an assessment as to whether confidential or sensitive information is on the device (as defined by Data Classification Policy). Campus Police will be notified of stolen devices.
3. PASSHE Legal Counsel and University IT will follow the Pennsylvania Breach of Personal Information Notification Act if personal information is deemed to be possibly breached or stolen.

- The Breach of Personal Information Notification Act defines “Personal information” as:
    - An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted:

      1. Social Security number.

      2. Driver's license number or a State identification card number issued in lieu of a driver's license.

      3. Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

      4. Medical Information – Any individually identifiable information contained in the individual's current or historical record of medical history or medical treatment or diagnosis created by a health care professional.

      5. Health Insurance information - An individual's health insurance policy number or subscriber identification number in combination with access code or other medical information that permits misuse of an individual's health insurance benefits.

      6. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

4. Notification - May be provided by any of the following methods of notification:
    - Written notice to the last known home address for the individual.
    - Telephone notice, if the customer can be reasonably expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.
    - E-mail notice will be provided if the person is a current PennWest Faculty/Staff/Student. Otherwise written or telephone notice will be provided.
    - Substitute notice, if the entity demonstrates one of the following:
        - The cost of providing notice would exceed $100,000.
        - The affected class of subject persons to be notified exceeds 175,000.
        - The entity does not have sufficient contact information.
        - Substitute notice shall consist of all of the following:

          1. E-mail notice when the entity has an e-mail address for the subject persons.

          2. Conspicuous posting of the notice on the entity's Internet website if the entity maintains one.

          3. Notification to major statewide media.

        - Notification shall be made as soon as possible upon detection of breach but

in no event more than 60 days following discovery of the breach.

- Public Relations will be responsible for notification of affected individuals.

5. General rule – PennWest shall provide notice of any breach of the security of electronic systems/data following discovery of the breach of the security of the system to any person who's unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person.

6. Encrypted information – PennWest must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

7. Vendor notification - A vendor that maintains, stores or manages computerized data on behalf of PennWest shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data.

8. When PennWest provides notification under this act to more than 1,000 persons at one time, they shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in section 603 of the Fair Credit Reporting Act (Public Law 91-508, 15 U.S.C. § 1681a), of the timing, distribution and number of notices.

9. PennWest will offer free credit monitoring to those whose information may have been affected by a data breach.

Forms

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:
  - Information Technology (Individual contacts UTech who then handles the other contacts.)
  - PASSHE Legal Counsel
  - Executive responsible for the business area

- Public Relations
- Campus Police for devices

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

- Should the public be notified of the incident? If so, consider the following:
  - Develop talking points
    - Key Message
    - Next steps
  - Press Release
  - 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?
    - Outline the incident
    - Explain the actions currently being taken by the organization
    - Include the contact information (e.g. the toll free number and web site)
    - 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?
    - 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?
    - How often should the credit bureau track statistics and report any identity thefts to your agency?
    - If a contract is established with one of the credit bureaus, how will the information be communicated to the individuals?
    - Does a reminder letter on the credit services need to be sent to the citizens?
    - 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.

E. Related policies

Data Classification Policy.

F. Contact Information

Information Technology Services

G. Policy Review Schedule

All policies will be reviewed every two years or on an as needed basis if a change in BOG, PASSHE or Pennsylvania law would create the need for an immediate change.