Data Breach Notification

Policy Effective Date: 3/24/2017 • **Policy Revised:** Insert
Procedures Effective Date: 3/24/2017 • **Procedures Revised:** Insert

Policy Name: Data Breach Notification

Policy Purpose

This policy describes the process for documentation and appropriate internal and external reporting of information Security Breaches.

Applicability

This policy is applicable to students, employees, visitors, third-party vendors, and contractors.

Responsible Official, Office, and Interpretation

The Office of Information Technology Services and Information Technology Council are responsible for the review and revision of this policy. For questions about this policy, please contact Information Technology Services. The Chief Information Officer, in consultation with the Office of University Counsel, has the final authority to interpret this policy.

Defined Terms

A defined term has a specific meaning within the context of this policy.

Personal Identifying Information (PII)

Any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including (1) Name, social security number, date of birth, official state or government issued drive license or identification number, alien registration number, passport number, employer or taxpayer identification number; (2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (3) Unique electronic identification number, address, routing code or other personal identifying data which enables an individual to obtain merchandise or service or to otherwise financially encumber the legitimate possessor of the identifying data; (4) Telecommunication identifying information or access device; or (5) Any name, number, information, medical prescribing pad, electronic message, or form used by a physician, nurse practitioner, or other health care provider for prescribing a controlled substance.

Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or

listed, and does not include information made lawfully available to the general public from federal, state, or local government records.

Security Breach

Any incident involving the unauthorized access to and acquisition of unencrypted and unredacted records or data containing Personal Identifying Information, where the illegal use of that information has occurred, is reasonably likely to occur, or creates a material risk of harm to the individual. A Security Breach also includes any unauthorized access to and acquisition of encrypted records or data if the encryption key or confidential process that renders the data secure is also accessed or acquired.

The good faith acquisition of Personal Identifying Information by a university employee or agent for a legitimate business purpose does not constitute a Security Breach, provided that the information is not used for any purpose other than the lawful operations of the University and is not subject to further unauthorized disclosure.

Policy Name: Data Breach Notification

Policy

ETSU will investigate and provide Notification of Security Breaches to affected individuals and/or federal and state agencies in accordance with applicable federal and state requirements.

1. Containment and Classification.

In the event of a data Security Breach, the first priority is to contain the breach and immediately notify supervisory personnel. All reasonable steps must be taken to secure the data and restore the integrity, security, and confidentiality of the affected data or systems.

An employee who suspects a breach has occurred must report it without delay to their immediate supervisor. The supervisor is responsible for immediately notifying Information Technology Services (ITS). ITS will assist with determination of the magnitude and classification of the data breach. Any affected data should be classified according to the University Records Classification Guide.

ITS, the ETSU Police Department, the system or data owner, and other relevant departments will be contacted by the supervisor as soon as possible for assistance. In cases involving the loss or theft of university-owned equipment, or where criminal activity is suspected, the ETSU Police Department must be notified immediately. If ITS suspects that the breach-related incident may lead to an insurance claim, the CIO or designee within ITS will make an initial notification to the Tennessee Comptroller of the Treasury within no more than ten (10) hours of identification of the incident; should it subsequently be determined that an insurance claim is unnecessary, the Comptroller will should be updated.

In all cases, the Office of University Counsel must be notified as soon as practicable. The supervisor is responsible for documenting the breach, including the type and scope of the breach, actions taken, and the identities or categories of individuals whose Personal Identifying Information (PII) may have been exposed. A copy of this documentation must be submitted to the Office of University Counsel for official recordkeeping and further action, if necessary.

2. Notification to Victims.

2.1. Notification Responsibility.

The responsibility for issuing breach notifications to those affected by the breach rests with the data owner who holds primary authority over the affected data or system. The Office of University Council will review the proposed notification prior to distribution and will assist with drafting any communication as needed. A copy of the final notification must be provided to the Vice President of Marketing and Communications for their review before it is sent to or made available to affected individuals.

2.2. Notification Communication.

The written notification must be clear and conspicuous, and include the following information: (1) The incident in general terms; (2) The type of PII involved in the unauthorized access or acquisition; (3) A summary of the actions taken by the University to prevent further unauthorized access; this description may be general in nature to avoid increasing the risk or severity of the breach; (4) A telephone number that affected individuals may contact for additional information and assistance; and (6) Guidance advising individuals to remain vigilant by reviewing account statements and monitoring their credit reports, which are available at no cost.

2.3. Notification Method.

Notification to affected individuals must be provided by either (1) Written notification; or (2) Electronic notification for individuals for whom the University has a valid email address, unless substitute notification is permitted.

2.4. Notification Timing.

The university shall notify affected individuals of a data breach without unreasonable delay, not to exceed forty-five (45) days from identification of the breach. Notification may be postponed at the request of law enforcement if such disclosure may impede a criminal investigation or compromise national or homeland security. ITS will obtain and retain documentation of any such request by law enforcement. If delayed, notification must be made no later than forty-five (45) days after the law enforcement agency determines that notification will not compromise the investigation.

Policy Name: Data Breach Notification

Procedures

N/A

Applicable Forms and Websites

N/A

Authority and Revisions

Authority: Tenn. Code Ann. § 47-18-2107; Tenn. Code Ann. § 39-14-150

Previous Policy: Personal Information Security Breach

The ETSU Board of Trustees is charged with policy making pursuant to TCA § 49-8-203, et seq. On March 24, 2017, the Board delegated its authority to ETSU's President to establish certain policies and procedures for educational program and other operations of the University, including this policy. The delegation of authority and required process for revision to this policy can be found on the Policy Development and Rule Making Policy webpage.

To suggest a revision to this policy, please contact the responsible official indicated in this policy. Before a substantive change to the policy section may take effect, the requested changes must be: (1) approved by the responsible office; (2) reviewed by the Office of University Counsel for legal sufficiency; (3) posted for public comment; (4) approved by either Academic Council or University Council; and (5) approved by ETSU's President.