Policy Title: Personal Information Security Breach Policy

Policy Type: Technology **New/revised:** Revised

Old Policy #: Personal Information Security Breach Policy

Approval level: ☐ Board of Trustees
☒ President
☐ Vice President
☐ Other (specify here)

Purpose: Tennessee State Code § 39-14-150 defines the rights of victims of identity theft. The University Personal Information Security Breach Notification Policy governs how ETSU will respond to incidents involving theft of sensitive data.

Policy:

1.0 Definitions

"Personal Information" is defined to mean any of the following items:

- Name, Social Security number, date of birth, official state or government issued driver license or identification number, alien registration number, passport number, employer or taxpayer identification number;
- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- 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;
- Telecommunication identifying information or access device; or
- 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" is defined to mean: an incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach.

Good faith acquisition of personal information by an employee or agent of the University for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the University and is not subject to further unauthorized disclosure.

2.0 Procedures in the Event of a Security Breach

2.1. Containment, Classification, and Report of a Breach

2.1.1. Containment:

The first priority after a security breach is discovered is to contain the breach and notify supervisory personnel as quickly as possible. For any category of breach, the data must be secured, and the reasonable integrity, security, and confidentiality of the data or data system must be restored.

2.1.2. Classification:

The next step is to determine the exact nature of the breach in terms of its extent and seriousness. Is personal information easily accessible?

2.1.3. Internal Reporting of a Breach:

As soon as a breach has been identified, the employee who discovered it must take immediate steps to report the breach to his or her supervisor. The supervisor must take immediate action to determine the extent and category of the breach and to take such further action as is necessary to contain the breach or recover the missing data. Assistance from Information Technology Services, Public Safety or other office with relevant expertise should be requested as soon as possible. If the potential or actual breach involves loss or theft of University-owned equipment or other criminal activity, notify the Public Safety. In all cases of a breach, University Counsel's Office must be notified as soon as practicable.

The supervisor must document the breach, noting the category involved, the scope of the breach, steps taken to contain the breach, and the names or categories of persons whose personal information was, or may have been, acquired by an unauthorized person. A copy of that documentation must be sent to University Counsel.

2.2 Notification to Victims

2.2.1. Time for Providing Notification

The University shall notify affected individuals without unreasonable delay. However, notification shall be delayed if law enforcement informs the University that disclosure of the breach would impede a criminal investigation or jeopardize national or homeland security.

2.2.2. Responsibility for Providing Notification

The responsibility for providing notification shall lie with the Head of the Division that has primary authority for the data. The University Counsel will review the proposed notification before it is sent and will assist in drafting as required. A copy of the notification will also be provided to the Director of University Relations prior to the time it is posted or sent to affected individuals.

2.3. Contents of the Notification

Notification shall be clear and conspicuous and include a description of the following:

- The incident in general terms.
- The type of personal information that was subject to the unauthorized access and acquisition.
- The actions taken by the University to protect the personal information from further unauthorized access. However, the description of those actions may be general so as not to further increase the risk or severity of the breach.
- A telephone number that the person may call for further information and assistance.
- Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

2.4. Method of Notification

Notification to affected persons must be provided by one of the following methods unless substitute notification is permitted:

- Written notification, or
- Electronic notification, for those persons for whom the University has a valid e-mail address

3.0 Supplemental Information:

Link to Tennessee State Code Annotated 39-14-150

Link to Tennessee State Code Annotated 47-18-2107

Notes:

Approved: Information Technology Governance Council
Reviewed: February 2017
Active since: August 10, 2010

3/24/2017 – approved by the Board of Trustees.