

## Standard for Storing and Transmitting Personally Identifying Information

All *university information* must be handled with appropriate security and access controls, and with attention to safeguarding confidentiality. No information should be *exposed inappropriately*. Many data elements and other types of information are protected by federal or state statute or regulation. Information that is not protected by law or regulation should nonetheless be protected against inappropriate exposure.

These responsibilities are defined in university policies, and in state and federal law and regulations. (See Reference section.)

Terms in italics are defined in Section 3.

In light of the threat to individuals from identity theft, this standard singles out a subset of *sensitive university information* that is *personally identifying* to individuals affiliated with Virginia Tech. Exposure of these data elements may cause personal or financial harm to those individuals. This standard addresses electronic *storage* and *transmission* of this information, and is intended to restrict the use of these data elements to essential uses only, and to protect these elements when they are used. *Covered data* includes the following six individual data elements, and the combination of name and date of birth listed below:

### Covered data

These individual data elements are included in the personally identifying information covered by this standard:

- Social Security number
- Credit card number
- Debit card number
- Bank account number
- *Driver's license number*
- Passport number

In addition, the following combination is covered when it occurs in *documents*:

- Name (first name or first initial with last name) with *date of birth* (month, day, and year)

### 1. Standard for storing and transmitting covered data

When required for business purposes, these covered data elements must be stored only on university-owned devices that are neither an *individual-use device* nor a *mobile device*.

Covered data elements must be *encrypted* when they are stored or transmitted over a network.

- New systems and applications must encrypt covered data elements.

June 13, 2008

- Existing systems and applications must migrate to encryption of covered data elements in a timely manner, and the migration progress must be reported to the Vice President for Information Technology.

The covered combination must be encrypted when stored in a document and when transmitted over a network.

Additional guidance is available at the Sensitive Information Security website ([www.security.vt.edu/sensitiveinfo.html](http://www.security.vt.edu/sensitiveinfo.html)).

## **2. Exceptions: permission to store data elements in individual-use devices, mobile devices, or third party systems**

Rare exceptions may be granted for storing covered data on individual-use devices, on mobile devices, or on third-party systems. If granted, an exception requires that the covered data elements/combination be encrypted when stored or transmitted. For requests to be considered, there must be:

- A clear and compelling justification, and
- A plan for encrypting the data and for recovering original data.

The approval process begins by requesting review from the appropriate data steward, the requestor's management hierarchy through the Vice President, and arranging for a security review. Final review and approval decisions are made by the Vice President for Information Technology. Requests for exceptions must use the appropriate form, for either (a) *individual-use or mobile devices* or (b) *third-party systems*.

### **Special circumstance: Individual-use device**

Storage on an individual-use device is permitted through an expedited approval process in a specific circumstance only. Administrative assistants, fiscal technicians, or employees with similar responsibilities may, at the written request of the colleague and (if a different person) with the written permission of the department head, retain a credit or debit card number or passport number of that colleague for the purposes of assisting the colleague in travel arrangements or similar logistical support. When kept electronically, these data elements must be encrypted. Further, these data elements must be deleted when no longer needed for business purposes.

## **3. References**

Policy for protecting university information in digital form [New!] ([www.policies.vt.edu](http://www.policies.vt.edu))  
Board of Visitors' Resolution, June 4, 2007, "Information Technology Security and Authority Resolution" [www.bov.vt.edu/minutes/07-06-04minutes/documents/AttachmentV\\_000.pdf](http://www.bov.vt.edu/minutes/07-06-04minutes/documents/AttachmentV_000.pdf)  
Sensitive Information Resource Page ([www.security.vt.edu/sensitiveinfo.html](http://www.security.vt.edu/sensitiveinfo.html)).

June 13, 2008

HB 1469 Identity theft; notice of database breach, approved by Governor to amend Chapter 801, effective 7/1/08 (<http://leg1.state.va.us/cgi-bin/legp504.exe?081+ful+CHAP0801>)

Information Technology Security Standard ([www.it.vt.edu/Security%20Standards.pdf](http://www.it.vt.edu/Security%20Standards.pdf))

University Policy 7010, Policy for Securing Technology Resources and Services ([www.policies.vt.edu/7010.pdf](http://www.policies.vt.edu/7010.pdf))

University Policy 7100, Administrative Data Management and Access Policy ([www.policies.vt.edu/7100.pdf](http://www.policies.vt.edu/7100.pdf))

University Policy 7200, University Information Technology Security Program ([www.policies.vt.edu/7200.pdf](http://www.policies.vt.edu/7200.pdf))

University Policy 1060, Policy on Social Security Numbers ([www.policies.vt.edu/1060.pdf](http://www.policies.vt.edu/1060.pdf))  
Security Standards for Social Security Numbers

([www.computing.vt.edu/administrative\\_systems/banner/security%20standards\\_5July05.pdf](http://www.computing.vt.edu/administrative_systems/banner/security%20standards_5July05.pdf))

University Policy 7025, Safeguarding Nonpublic Customer Information ([www.policies.vt.edu/7025.pdf](http://www.policies.vt.edu/7025.pdf))

Family Educational Rights and Privacy Act of 1974

Gramm-Leach-Bliley Act ([www.ftc.gov/privacy/glbact/glbsub1.htm](http://www.ftc.gov/privacy/glbact/glbsub1.htm))

Health Insurance Portability and Accountability Act (<http://aspe.hhs.gov/admnsimp/pl104191.htm>)

Virginia Tech student privacy/FERPA ([www.registrar.vt.edu/records/ferpa.php](http://www.registrar.vt.edu/records/ferpa.php))

### 3. Definitions

**Personally identifying information** is any data or information that can uniquely identify a person.

**Storage** refers to data at rest, a term that refers to information stored on computing devices, excluding data that is traversing a network or that is temporarily residing in computer memory to be read or updated. Data at rest include both archived data as well as data that are subject to regular but not constant change. Examples include files stored on the hard drive of an employee's desktop computer, files on an external backup medium, and files on the servers of a storage device.

**Transmission** refers to data traversing a network, including the university network and the Internet. Transmission includes using the network to send data across an office or building as well as across the globe. Transmission excludes data at rest and excludes data that temporarily reside in computer memory to be read or updated.

**University information** includes information collected by or used by university personnel in the conduct of their university responsibilities. It includes information collected and used for learning, discovery, engagement, support, and administration. University information in digital form may exist in a variety of formats, ranging from highly structured elements in a database to unstructured, narrative information. University information includes information within the control of university personnel in the conduct of their job responsibilities, whether the information resides in university-owned digital systems or elsewhere. Further, university information may be gathered or used at the direction of the university but residing in applications hosted by vendors or other third parties.

**Sensitive university information** includes all university information that could cause physical, financial, or reputational harm to the university or to members of the university community if released inappropriately. Under Policy 7100, data classified as university-internal or as limited-access may be sensitive information.

June 13, 2008

**Inappropriate exposure** refers to the disclosure or presentation to the view of others caused by carelessness, negligence, or inattention to the precautions for dealing with university information.

**Covered data** refers to six covered data elements—those university nonpublic data elements specified in this standard (Social Security number, credit card number, debit card number, bank account number, driver’s license number, or passport number)—and the covered combination, the occurrence of name and date of birth carried together in a document.

**Driver’s license number**, as a covered data element, includes any identification card number issued by a state in lieu of a driver’s license number.

**Date of birth** is the complete reference to the specific date an individual was born, including all of (a) the birth month, (b) the specific day within the month, and (c) the birth year. “Date of birth” is distinguished from “birthday,” or anniversary of the date of birth, in that “birthday” does NOT include the year.

**Individual-use electronic device** refers to computer equipment with a storage device or persistent memory that is used by one person at a time, and any individually assigned file space on a shared system or server. Typically, desktop computers, laptop and tablet computers, personal digital assistants, and smart phones are such devices.

A **mobile device** is any computing or digital storage device designed to be carried with a person, including, but not limited to, laptop computers, tablet computers, personal digital assistants, handheld computers, CDs, DVDs, USB drives (“flash drive,” “jump drive,” “memory stick,” “thumb drive”), and other mobile external drives and storage devices.

**Encryption** refers to the algorithmic transformation of data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key.

**Documents** include many types of files that contain data. In unencrypted form, documents can be read by humans, and are typically capable of being printed. Examples include word-processing files, spreadsheets, PDF files, various image formats. Usage in this policy includes other file formats that communicate data to other human senses, including data in audio files.

**Third party systems** refer to hosted systems and vendor-provided services running on servers external to Virginia Tech, regardless of whether the system is purchased, leased, or donated. The definition does NOT include partners that receive transmissions of university data under requirements of law or regulation (for example, the Internal Review Service or the State Council of Higher Education for Virginia).

#### 4. Approval

Approved, Vice President for Information Technology, Earving L. Blythe

(Signed)

\_\_\_\_\_

Date

July 1, 2008

June 13, 2008

## **5. Revisions**