

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.

Terms in italics are defined in Section 5.

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:

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

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.

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

- New systems and applications must encrypt covered data elements.
- 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.

Any system use of SSN must be approved in writing by the Vice President for Finance and Chief Financial Officer (formerly, Vice President for Budget and Financial Management).

1.1 An individual use device or mobile devices

Only individuals who have a specific job responsibility to handle one or more of the covered data elements may store such data on an *individual use device* or a *mobile device*. The approval of the relevant data steward and the employee's department head must be obtained first.

An implemented plan for data encryption must be in place whenever any of the covered data elements is stored on an individual-use device or mobile device, or transmitted from an individual-use device or mobile device. The plan must include a method to recover original data, if any.

Additional guidance is available at the sensitive information webpage on the Information Technology Security Office website (www.security.vt.edu/sensitiveinfo.html).

In summary, the following questions should help determine the handling of covered data on an individual use device or mobile device:

1. Do you need the data to successfully complete your job functions?
 - a. YES, proceed to step 2.
 - b. NO, **delete the data file(s) immediately.**
2. Do you have a clear and compelling justification for storing the covered data locally that has been approved in writing by the appropriate data steward and your department head?
 - a. YES, proceed to step 3.
 - b. NO, stop and obtain the necessary written approvals.
3. Do you have a plan for encrypting the data and for recovering original data?
 - a. YES, proceed with your process to secure and store the covered data.
 - b. NO, do not store these covered data elements until you have an encryption plan in place.

Special case: With the written approval of their department head, administrative assistants, fiscal technicians, or employees with similar responsibilities may, at the written request of a colleague, 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.

2. Storing covered PII in third-party systems

2.1 Third-party systems under contract with the university

An exception to storing the covered elements on university-owned devices only occurs if there is a contract to store these elements with a third party. The [Standard for the Procurement of Information Technology Applications](#) requires that any procurement, whether a no-cost application or for money, be reviewed by the Information Technology Security Office and have the approval of the relevant data

steward for any application that collects, stores, displays, or exports personally identifying covered data. Data encryption, both at rest and in transmission, must be required in the contract.

2.2 Third-party systems NOT under contract with the university

The covered data elements may NOT be stored or transmitted to any third-party system that is NOT under contract with the university. University personnel may not make independent decisions to store this information on other sites.

The covered data elements may be transmitted to third party systems when required by federal or state statute or regulation.

4. References

4.1 Required reading

Individuals who are authorized to use covered PII must read these relevant policies and standards.

Policy on Social Security Numbers, University policy 1060 (www.policies.vt.edu/1060.pdf)

Security Standards for Social Security Numbers

(http://www.computing.vt.edu/administrative_systems/banner/security%20standards_5July05.pdf)

Policy for Security Technology Resources and Services, University Policy 7010

(www.policies.vt.edu/7010.pdf)

Administrative Data Management and Access Policy, University Policy 7100

(www.policies.vt.edu/7100.pdf)

Standard for Administrative Data Management

(http://www.it.vt.edu/publications/pdf/Administrative_data_management_standard_2011-March-23.pdf)

Standard for Protecting Sensitive University Information Used in Digital Form

(http://www.it.vt.edu/publications/pdf/StandardforProtectingSensitiveUniversityInformation_October2011_Rev_3.pdf)

Safeguarding Nonpublic Customer Information, University Policy 7025

(<http://www.policies.vt.edu/7025.pdf>)

4.2 Additional references

Board of Visitors' Resolution, June 4, 2007, "Information Technology Security and Authority Resolution" (http://www.bov.vt.edu/minutes/07-06-04minutes/attach_v_070604.pdf)

Sensitive Information Resource Page (www.security.vt.edu/sensitiveinfo.html).

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

(http://www.it.vt.edu/publications/pdf/Security_Standards.pdf)

University Policy 7200, University Information Technology Security Program

(www.policies.vt.edu/7200.pdf)

Family Educational Rights and Privacy Act of 1974

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

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

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

Standard for the Procurement of Information Technology Applications

(www.it.vt.edu/publications/pdf/Procurement_STANDARD_signed_1-19-11.pdf)

5. Definitions

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, passport number).

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.

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. For the purposes of this standard, a one-way hash using a secure algorithm may, where appropriate, be an alternative to encryption.

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.

Individual-use device refers to computer equipment with a storage device or persistent memory that is used primarily 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.

Network is used in this policy to refer to the Internet or other open network such as unprotected wireless connections.

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

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.

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.

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).

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.

6. Approval

Approved and digitally signed by Vice President for Information Technology Earving L. Blythe, July 1, 2008.

7. Revisions

Revision 1

Removed exception request process and incorporated references to the [Standard for the Procurement of Information Technology Applications](#); added “required reading” in references section, and summary of steps to take for individual use and mobile devices. Removed the combination of full date of birth and name in a document from the list of covered data.

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

(Signed) _____