Standard for Protecting Sensitive University Information Used in Digital Form

The purpose of this standard is to list responsibilities of university employees to avoid inappropriate release of *sensitive university information.* The focus of this standard is on sensitive university information that exists in a *digital form*, whether *stored* in a database, used in an application, *transmitted* over a network, or used in a report. *University information* must be protected from any inappropriate sharing, releasing, or use.

Understanding the risks involved in handling information in digital form includes an appreciation of the greatly increased vulnerability made possible by technological conveniences that offer portability, easy copying, and wide—potentially global—distribution.

Terms in italics are defined in Section 3.

1. Standard

Employees, including faculty, staff, graduate assistants and student wage employees, and volunteers, must read, understand, and continually meet the responsibilities listed below. Additional guidance is available at the Sensitive Information Resource website (www.security.vt.edu/sensitiveinfo.html).

- **Know what information is available to you**

Identify what university information is stored under your control, and to which you have access. Identify the university information you can enter, and the information you are authorized to view.

- **Know where the information is stored**

Understand what university information is stored in all devices under your control, including routine workstations, portable devices and portable storage media, and local servers.

Use security tools to locate Social Security numbers and credit card numbers (www.security.vt.edu). The Standard for Storing and Transmitting Personally Identifying Information outlines mandatory steps for Social Security numbers, financial account numbers, and related information. (http://www.it.vt.edu/publications/pdf/PII_October2011_Rev_1.pdf)

- **Understand the sensitivity of university information**

Clarify with supervisors the nature of university information that you handle or access and its level of sensitivity. Ask:

a. Does the information fall under the privacy protections of federal or state statutes or regulations? Examples of such information include data subject to the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and related regulations and policies, including university policies.

b. Is the information subject to privacy or confidentiality protections of private agreements? Examples may include non-disclosure agreements and other contractual agreements.

c. Does the information require confidentiality through professional ethics or through procedural requirements? Examples may include unpublished research findings, the identity of research subjects, and examination questions.

d. Does access to the information require approval? Examples include Banner access, access to confidential files, and access granted to and required by computer system administrators. Information classified as "limited access" data according to Policy 7100 is sensitive.

e. Could the personal information potentially cause harm to a person or persons? For example, one might handle information about large numbers of individuals, such as applicants for admission to a university program or individuals who have purchased items from a department. One might also handle information about one or two people. For example, someone who makes travel plans for others might have another person's personal credit card number to make hotel reservations.

- **Destroy information that is not needed**

Information may need to be retained for a specific time. Often, however, individuals keep information—whether in file cabinets, on storage media, or on a computer—for an unnecessarily long time. Be sure to comply with the Records Management retention requirements that can be found on their web site:

www.facilities.vt.edu/tcs/records/

Offices will often have "copies" that may be destroyed if the original or source document has been preserved.

Digital devices and storage media to be surplused must be handled properly to ensure information is destroyed. Procedures can be found at the following site:

www.computing.vt.edu/security_and_viruses/surplusprocedure.pdf

- **Mitigate risks of exposure of sensitive information**

Departments and workgroups must evaluate the risks of exposure of sensitive data, and implement mitigating or compensating controls for those risks. This process must include reviewing the sensitivity of the information, methods of storage and transmission of data, the physical security of systems, and the infrastructure and systems security in place.

To mitigate the risks of exposure, you must:

- Comply with the Standard for Storing and Transmitting Personally Identifying Information (http://www.it.vt.edu/publications/pdf/PII_October2011_Rev_1.pdf). These covered data elements are the following six items:
  - Social Security number
  - Credit card number
  - Debit card number
  - Bank account number

- *Driver's license number*
- Passport number

- Select appropriate methods to safeguard all other sensitive data. See the guidelines on www.security.vt.edu/sensitiveinfo.html for specific considerations and possible methods of mitigation.

2. References

University Policy 7105, Policy for Protecting University Information in Digital Form (www.policies.vt.edu/7105.pdf)
Information Technology Standard for Storing and Transmitting Personally Identifying Information (http://www.it.vt.edu/publications/pdf/PII_October2011_Rev_1.pdf)
Board of Visitors' Resolution, June 4, 2007, "Information Technology Security and Authority Resolution" (www.minutes.bov.vt.edu/minutes/07-06-04minutes/07-06-04AttachmentV.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 7010, Policy for Securing Technology Resources and Services (www.policies.vt.edu/7010.pdf)
University Policy 7100, Administrative Data Management and Access Policy (www.policies.vt.edu/7100.pdf)
University Policy 7200, University Information Technology Security Program (www.policies.vt.edu/7200.pdf)
University Policy 1060, Policy on Social Security Numbers (www.policies.vt.edu/1060.pdf)
Security Standards for Social Security Numbers (www.computing.vt.edu/administrative_systems/banner/security%20standards_5July05.pdf)
University Policy 7025, Safeguarding Nonpublic Customer Information (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)
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)

3. Definitions

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 elements classified as *limited-access* are sensitive information.

Employees include all persons directly employed by Virginia Tech in their capacity as employees. The policy also covers anyone to whom the electronic communications and computing resources of employees have been extended. These include (but are not limited to) recently terminated employees whose communications and computing resources have not yet been terminated, deleted, or transferred, consultants that may be hired, and individuals whose electronic communications and computing resources continue between periods of employment. This also includes student workers, volunteers, and other individuals who are using state-owned equipment and carrying out university work.

Digital form refers to the technology of computers and data communications, and includes products of those systems, including printed reports.

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.

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

Storage refers to data at rest, a term that refers to all data 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 that temporarily reside in computer memory to be read or updated.

1. **Approval**

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

1. **Revisions**

Revision 1

Updated hyperlinks

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

Date _February 18, 2009_____

Revision 2

Clarified sensitive data definition and risk mitigation steps. Previous steps to review applications prior to implementation and to secure individual computing devices were eliminated since they are already required in other policies and standards.

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

(Signed)

Revision 3

Changed list of personally identifying information covered date elements to conform to the Standard for Storing and Transmitting Personally Identifying Information

Updated links

Signed Earving L Blythe

Digitally signed by Earving L Blythe
DN: dc=edu, dc=vt, c=US, o=Virginia Polytechnic Institute and State University, cn=Earving L Blythe, 0.9.2342.19200300.100.1.1=809628, serialNumber=1231
Date: 2011.10.10 15:24:01 -04'00'