

Standard for High Risk Digital Data Protection v. 5

Purpose

All university data, regardless of risk classification, must be protected with the minimum qualifications set forth by policy 7010, Policy for Securing Technology Resources and Services and [the Virginia Tech Risk Classifications](#). Digital high risk data pertains to data where protection of the data is required by law or regulation and Virginia Tech is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed. The unauthorized release of this data could result in a significant adverse impact on the university's mission, safety, finances, or reputation. Therefore, additional security precautions must be taken when storing, transmitting, and/or processing such data.

Scope

All users of high risk digital data must successfully complete online security awareness training offered or recommended by the University IT Security Office at least annually. See References, below, for training resources.

Standard

The following table highlights the university's high risk data elements/types, associated university policies and standards, associated laws and regulations, and the protections required by the university for that data element/type. The first six elements (Social Security number, credit and debit card number, bank account number, driver's license number, and passport number) are defined by the university as personally identifiable information (PII).

Data element	VT policies and standards	Laws and regulations	VT protections
<i>Social Security number</i>	Policy 1060, Policy on Social Security Numbers www.policies.vt.edu/1060.pdf	Code of Virginia: Collection, exposure, or display of social security number. http://law.lis.virginia.gov/vacode/2.2-3808/ Code of Virginia, Breach of personal information notification. http://law.lis.virginia.gov/vacode/18.2-186.6/ Code of Virginia, identity theft; penalty; restitution; victim assistance. http://law.lis.virginia.gov/vacode/18.2-186.3/	<ul style="list-style-type: none"> ▪ Usage and collection must be approved by data trustee, Vice President for Finance and Chief Financial Officer ▪ Encrypt the data file/database element in storage and in transmission using cryptographic methods approved by NIST ▪ No third-party storage or transmission without prior ITSO review and university contract ▪ No use as an identifier
Debit and credit card numbers	Accepting and Handling Payment Card Transactions http://www.policies.vt.edu/3610.pdf	Payment Card Industry Data Security Standard https://www.pcisecuritystandards.org/ Standards for Safeguarding Customer	<ul style="list-style-type: none"> ▪ Encrypt the data file/database element in storage and in transmission using cryptographic methods approved by NIST ▪ Obtain prior written approval of department head after written request of coworker for storing debit/credit card numbers for assisting with travel arrangements. ▪ No third-party storage or transmission without prior ITSO review, Bursar approval,

	<p>Safeguarding Nonpublic Customer Information, Policy 7025</p> <p>www.policies.vt.edu/7025.pdf</p>	<p>Information, 16 CFR Part 314, implementing sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act</p> <p>https://www.ecfr.gov/current/title-16/part-314</p> <p>Code of Virginia, Breach of personal information notification.</p> <p>http://law.lis.virginia.gov/vacode/18.2-186.6/</p>	<p>and university contract</p> <ul style="list-style-type: none"> ▪ Acceptance of credit card payments and methods must be approved by the University Bursar ▪ Must not be requested, received, or transmitted through an unsecure medium. ▪ Processing payments cards received by email, text, or instant messaging (encrypted or unencrypted) is prohibited
Bank account numbers	<p>Safeguarding Nonpublic Customer Information, Policy 7025</p> <p>www.policies.vt.edu/7025.pdf</p>	<p>NACHA Operating Rules and Guidelines</p> <p>Code of Virginia, Breach of personal information notification.</p> <p>http://law.lis.virginia.gov/vacode/18.2-186.6/</p> <p>Code of Virginia, identity theft; penalty; restitution; victim assistance.</p> <p>http://law.lis.virginia.gov/vacode/18.2-186.3/</p>	<ul style="list-style-type: none"> ▪ Encrypt the data file/database element in storage and in transmission using cryptographic methods approved by NIST ▪ No third-party storage or transmission without prior ITSO review and university contract
<i>Driver's license numbers, military id numbers, and passport numbers</i>		<p>Code of Virginia, Breach of personal information notification.</p> <p>http://law.lis.virginia.gov/vacode/18.2-186.6/</p> <p>Code of Virginia, identity theft; penalty; restitution; victim assistance.</p> <p>http://law.lis.virginia.gov/vacode/18.2-186.3/</p>	<ul style="list-style-type: none"> ▪ Encrypt the data file/database element in storage and in transmission using cryptographic methods approved by NIST ▪ Obtain prior written approval of department head after written request of coworker for storing passport numbers for assisting with travel arrangements ▪ No third-party storage or transmission without prior ITSO review and university contract
Medical or mental history; Medical treatment or diagnoses information; health insurance policy numbers		<p>Code of Virginia, Breach of personal information notification.</p> <p>https://law.lis.virginia.gov/vacode/title32.1/chapter5/section32.1-127.1:05/</p>	<ul style="list-style-type: none"> ▪ Encrypt the data file/database element in storage and in transmission using cryptographic methods approved by NIST ▪ No third-party storage or transmission without prior ITSO review and university contract

<p>Student data (nondirectory or items marked confidential)</p>	<p>Student Privacy/FERPA https://www.registrar.vt.edu/FERPA.html</p> <p>Maintaining Student's Privacy https://www.registrar.vt.edu/FERPA.html</p>	<p>The Family Educational Rights and Privacy Act (FERPA) http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title34/34cfr99_main_02.tpl</p>	<ul style="list-style-type: none"> ▪ Departments must not include personally identifiable FERPA data in totality in an email: e.g. no full name in combination with full student ID number. ▪ Departments must not list student name and ID number in the subject line ▪ Departments may communicate using either the student ID with the full initials of the student [999999999 (ANW)] or use the full name with the last four of the ID [Alice N. Wonderland (1234)] ▪ Departments must not attach spreadsheets or scanned documents with full identifiers or nondirectory information via email. Departments may communicate spreadsheets or scanned documents via a secure link or shared electronic files requiring user authentication ▪ Do not store FERPA data on a flash drive. ▪ If forwarding items with personally identifiable FERPA data, use a cover sheet directing the recipient to contact you if it is misdirected.
<p>Export controlled research data</p>	<p>Virginia Tech Technology Control Plan https://www.research.vt.edu/oesrc/ResearchSecurity/technology-control-plan.html</p> <p>VT Export and Sanctions Compliance Policy http://www.policies.vt.edu/13045.pdf</p> <p>OSP Procedure 29-05: Management of Restricted Research Agreements https://osp.vt.edu/content/dam/osp</p>	<p>Executive Order 13556 Controlled Unclassified Information https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information</p> <p>Controlled Unclassified Information 32 CFR §2002 https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information</p> <p>Export Administration Regulations (EAR) 15 CFR §§730-774</p>	<p>Virginia Tech Technology Control Plan guidelines https://www.research.vt.edu/oesrc/ResearchSecurity/technology-control-plan.html</p> <p>Department of Defense Instruction 8582.01 https://irp.fas.org/doddir/dod/i8582_01.pdf</p> <p>(As applicable) Federal Acquisition Regulation 52.204-21 Basic Safeguarding of Covered Contractor Information Systems https://www.acquisition.gov/far/52.204-21-0</p> <p>(As applicable) NIST 800-171 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf</p> <p>(As applicable) NIST 800-53 https://doi.org/10.6028/NIST.SP.800-53r5</p>

	<p>vt edu/policies/vt_osp export control policy osp-29-05.pdf</p> <p>VT Policy 12115: Accepting and Reporting Gifts-in-Kind</p> <p>http://www.policies.vt.edu/12115.pdf</p>	<p>http://www.ecfr.gov/cgi-bin/text-idx?SID=a010f4662b853e201c87b56dab273b42&mc=true&tpl=/ecfrbrowse/Title15/15CVIsubchapC.tpl</p> <p>International Traffic in Arms Regulations (ITAR) 22 CFR §§120-130</p> <p>http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title22/22cfr120_main_02.tpl</p> <p>Importation of Arms, Ammunition and Implements of War 27 CFR §447</p> <p>https://regulations.atf.gov/447</p> <p>Export and Import of Nuclear Equipment and Material Regulations (EINEMR) 10 CFR §110</p> <p>https://www.nrc.gov/reading-rm/doc-collections/cfr/part110/full-text.html</p> <p>Assistance to Foreign Atomic Energy Activities Regulations (AFAEAR) 10 CFR §810</p> <p>http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title10/10cfr810_main_02.tpl</p> <p>Unclassified Nuclear Controlled Information (UNCI) 42 U.S.C. 2168</p>	
--	--	--	--

		https://www.gpo.gov/fdsys/granule/USCODE-2010-title42/USCODE-2010-title42-chap23-divsnA-subchapXI-sec2168 Foreign Assets Control Regulations (FACR) 31 CFR §§500-599 http://www.ecfr.gov/cgi-bin/text-idx?SID=2b44158b17abd90e0056f2cf97d5a257&mc=true&tpl=/ecfrbrowse/Title31/31cfrv3_02.tpl#0 Secrecy of Certain Inventions and Licenses to Export (PTO) 37 CFR §5 https://www.gpo.gov/fdsys/granule/CFR-2002-title37-vol1/CFR-2002-title37-vol1-part5	
--	--	---	--

Unauthorized Exposure of PII

Upon confirmation by the ITSO that personally identifiable information may have been exposed, the department in which the exposure occurred shall be responsible for notifying the individuals whose personally identifiable information was exposed, as well as offering credit monitoring as arranged through the university's Procurement Department. If the unauthorized data exposure consisted of information that was not related to university business, the department shall have no obligation to offer credit monitoring and the matter may also be referred to human resources for review in compliance with the acceptable use policy.

Definitions

Driver's License Number: also includes any identification card number issued by a state in lieu of a driver's license number.

Social Security number (SSN): include those issued to persons by the United States Social Security Administration, and also those issued to individuals by the United States government in lieu of an SSN. SSNs also include nation-based identification numbers issued to individuals by other countries. SSNs also include railroad numbers. SSNs do not include tax IDs issued to corporations.

References

NIST Cryptographic Toolkit: <http://csrc.nist.gov/groups/ST/toolkit/index.html>

Dealing with Data Exposures: https://security.vt.edu/incident/dealing_with_data_exposure.html

Protecting Sensitive Data: <http://security.vt.edu/resources/sensitiveinfo.html>

Policy for Securing Technology Resources and Services: <https://policies.vt.edu/assets/7010.pdf>

Virginia Tech Risk Classifications: https://it.vt.edu/content/dam/it_vt_edu/policies/Virginia-Tech-Risk-Classifications.pdf

Social Security Numbers for Retired Railroad Employees: <https://secure.ssa.gov/poms.nsf/lnx/0110225045>

IT Security Training Resources: <https://security.vt.edu/resources.html>

Dept Head training: [DEPT HEAD TRAINING - IT Security \(google.com\)](#)

Maintenance of Standard

The IT Security Office is responsible for this IT Standard. Questions may be directed to security@vt.edu.

Approval and Revisions

This standard supersedes and replaces Security Standards for Social Security Numbers; Standard for Protecting Sensitive University Information Used in Digital Form; and Standard for Storing and Transmitting Personally Identifying Information.

Version 1, published July 2017

Version 2, published November 2020 added military id and health data

Version 3, published September 2021 added training resource urls

Version 4, November 2021 updated links to references

Version 5, published February 2022 updated links, references and formatting