Virginia Tech Risk Classification Standard

1. Purpose and Scope

Virginia Tech is committed to protecting the privacy of its students, alumni, current and former employees, retirees, research participants, and all other internal or external customers as well as protecting other information important to the university's mission. This standard supports university policy no. 7010 - Policy for Securing Technology Resources and Services[1] and establishes the university's data and IT classification scheme for the purpose of determining appropriate controls (safeguards and/or countermeasures) that should be in place for university data and IT assets in order to uphold the information security objectives collectively referred to as the "CIA triad" of computer security[2], [3]:

- **Confidentiality** - Ensuring that only people who are allowed to see certain information can access it, in order to protect personal privacy and sensitive data;
- **Integrity** - Ensuring information is accurate and hasn't been changed by anyone who shouldn't have access, and that its source is trustworthy;
- **Availability** - Ensuring information and systems are available when needed and work reliably.

2. Standard

Risk Classification Labels *These definitions establish the Virginia Tech Risk Classification labels. Risk Classification serves primarily the "Confidentiality" and "Integrity" security objectives of the CIA triad.*
HIGH – RISK
High-Risk data and IT resources include those where the loss of confidentiality, integrity, or availability could result in significant to catastrophic impact on the university's mission, operations, safety, finances, or reputation. This classification includes, but is not limited to: **1. Sensitive Personally Identifiable Information (SSNs, financial account information, driver's license/passport numbers, etc.);** **2. Protected Health Information (PHI) as defined under HIPAA;** **3. Data subject to federal export control regulations (e.g., ITAR, EAR); and** **4. Data for which disclosure or modification could result in significant fines or penalties, regulatory action, or civil or criminal action.**
MODERATE – RISK
Moderate-Risk data and IT resources include those that are not High-Risk and where the loss of confidentiality, integrity, or availability could result in mild to moderate adverse impact on our mission, safety, finances, or reputation. Moderate-Risk data includes data that is not High-Risk but is not generally available to the public.
LOW – RISK
Low-Risk data is data that is intended for public disclosure and where the loss of confidentiality, integrity, or availability would have no adverse impact on the university's mission, operations, safety, finances, or reputation.

2.1 Asset Risk Classification

Use the following tables to determine which Risk Classification is appropriate for a particular type of university data or information asset/technology resource: endpoints, servers, applications, and network infrastructure. When mixed data falls into multiple risk categories, use the highest risk classification across all. Note that these tables do not reflect exhaustive lists of all possible scenarios.

Data Risk Classification *Data are discrete facts/values that convey information related to university business. When mixed data falls into multiple risk categories, use the highest risk classification across all. Note: this is not an exhaustive list of all possible scenarios*			
HIGH	**High-Risk Data Types**		**Justification**
	Student disciplinary records, student financial aid records, student protected health information.		**34 CRF 99 (FERPA)[4]**
	Sensitive Personally Identifiable Information (PII)	**Social Security Numbers (SSN)**	**Va Code §2.2-3808[6], §18.2-186.6[7], §18-2-186.3[8]**
		Credit/debit card numbers	**PCI-DSS[9]; 16 CFR 314 (GLBA) [10]; Va Code §18.2-186.6**
		Financial account numbers	**NACHA[11]; Va Code §18.2-186.6, §18.2-186.3**
		Driver's license, state ID, military ID, passport, visa numbers	**Va. Code §18.2-186.6, §18.2-186.3**
	Medical/mental history, treatment, or diagnoses information; health insurance policy numbers, protected health information (PHI)		**Va. Code §32.1-127.1:05[12]; 45 CFR 160.103[13]**
	Export controlled research data, individually identifiable sensitive research data where disclosure may place an individual at risk of criminal or civil liability, or be damaging to the financial standing, employability, educational advancement, or reputation, or research data with contractual requirements that meet or exceed the VT minimum standard for protection of high-risk data.		**CUI[15], ITAR[16], EAR[17], EINEMR[18], FACR[19], AFAEAR[20], UNCI[21], etc.; 45 CFR 46[22]**
	Engineering, design and/or operational information regarding VT Infrastructure considered "Critical to the University"		**Critical to University**
MODERATE	**Moderate-Risk Data Types**		**Justification**
	Unpublished research data that is not classified as High-Risk		**Competitive and commercial potential; contractual obligation**
	FERPA information that is not otherwise High-Risk data (redacted directory information, class rosters, grade sheets, transcripts)		**34 CFR 99 (FERPA), Va. Code §23.1-405**
	University Employee ID numbers, employment applications and personnel files without PII, as well as non-directory contact information		**Employee privacy**
	Internal communications, email, non-public reports or contracts, intellectual property, and all other information releasable in accordance with the Virginia Freedom of Information Act		**Least privilege and need-to-know**
	Donor contact information and non-public gift information		**Donor Privacy**
LOW	**Low-Risk Data Types**		**Justification**
	VT Directory (Faculty, Staff, Students)		**FERPA, Va Code §23.1-405**
	Unrestricted, non-sensitive research data that is intended for public access and distribution without limitation		**Public use**
	Public VT Websites, University employment advertisements		**Public use**
	Public procedure manuals, public domain information (e.g. campus maps or photography)		**Public use**

Endpoint Risk Classification *Endpoints are desktops, laptops, or mobile devices*	
HIGH	**High-Risk Endpoints**
	Endpoints storing High-Risk data
	Endpoints used by IT administrator(s) to manage or configure other High Risk resources/assets (i.e. Privileged Access Workstation)
MODERATE	**Moderate-Risk Endpoints**
	Endpoints storing Moderate Risk data and no High-Risk data (e.g.: desktop or laptop storing non-public procedures/documentation)
	Student-use endpoints storing Moderate Risk work-related data
LOW	**Low-Risk Endpoints**
	Endpoints storing only Low Risk data (appropriate for public use)
	General use endpoints used as kiosks, where system is restored to known Low-Risk state every day
	Student-use endpoints storing only Low Risk work-related data

Server Risk Classification *Servers are hosts that provide network-accessible services. Server can be physical or virtual machines and may be hosted in-premises or with a cloud service provider (CSP).*		
HIGH	**High-Risk Servers**	
	Servers storing High-Risk data	
	Servers performing High-Risk functions:	Authentication, Authorization, Accounting (AAA) servers
		Domain Name System (DNS) servers
		University Email Servers
		Dynamic Host Configuration Protocol (DHCP) servers
		Hypervisors with multiple hosted VMs are classified as High Risk
		Servers used to manage or configure other university IT resources; servers used to control physical access control systems that could impact human health or safety; “critical infrastructure” servers; or any other “Critical to the University” servers.
MODERATE	**Moderate-Risk Servers**	
	Servers storing Moderate Risk data and no High-Risk data (e.g., file server storing non-public procedures/documents)	
	Hypervisors with VMs classified as Moderate Risk (e.g., file server storing non-public data)	
LOW	**Low-Risk Servers**	
	Servers storing only Low-Risk data (appropriate for public use)	
	Hypervisors where hosted VMs are classified as Low Risk only.	

Application Risk Classification		
Applications are software programs, code, or packages that perform specific functions directly for end users or for other applications. Applications can be "self-contained" or groups of programs and may or may not be network accessible. Applications can be developed and maintained "in-house" by VT units or provided by a 3rd party service provider.		
HIGH	**High-Risk Applications**	
	Applications handling High-Risk data	
	Applications performing High-Risk functions:	**Authentication, Authorization, Accounting (AAA) applications**
		Applications that process electronic payments
		"Critical infrastructure" applications; or any other applications supporting services or processes considered "Critical to the University"
MODERATE	**Moderate-Risk Applications**	
	Applications handling Moderate-Risk data and no High-Risk data	
LOW	**Low-Risk Applications**	
	Applications handling only Low-Risk data (appropriate for public use)	

Network Infrastructure Risk Classification	
Network infrastructure devices transport communications needed for data, devices, applications, services, and multi-media. This includes devices such as routers, switches, load-balancers, wireless access points, firewalls, intrusion detection/prevention systems, and other security or special purpose appliances.	
HIGH	**High-Risk Network Infrastructure**
	Network infrastructure devices deployed in purpose-specific segmented networks or environments with certain regulatory or industry compliance requirements (e.g. PCE-DSS, CUI/export-controlled research, HIPAA, etc.)
MODERATE/LOW	
	Network infrastructure devices that are not High-Risk are classified as Moderate or Low-Risk at the owner's discretion

2.2 Asset Priority Classification

Priority Classification is used in combination with Risk Classification when performing security incident response processes, and also for continuity of operations and disaster recovery planning purposes. Use the following table to determine which Priority Classification is appropriate for your IT resources. Priority Classification serves primarily the *Availability* security objective of the CIA triad.

Asset Priority Classification	
These definitions establish the Virginia Tech Priority Classification labels and classification scenarios. Priority Classification serves primarily the "Availability" objective of the CIA triad. *Note: This is not an exhaustive list of all possible scenarios.*	
CRITICAL	**Critical-Priority Assets** **Assets where the *disruption of access to or use of data* or an IT resource or the *unauthorized destruction of data* could be expected to have a *severe or catastrophic adverse* effect on organizational operations, organizational assets, or individuals. Loss of the asset(s) for even a short period of time could prevent the organization (or university) from maintaining operations essential to achieving its mission; or could pose a risk to human health and safety and/or other university IT resources if compromised or unavailable.** **Critical-Priority assets include technology resources, applications and network infrastructure devices that function as key components of services listed as "Critical Resources" supporting the "Essential Functions" with a recovery time objective (RTO) of less than 12 hours as documented on the University-level or departmental Continuity of Operations Plan (COOP).** **Critical-Priority assets also include technology resources, applications and network infrastructure devices that function as key components of physical access control systems, emergency response services or systems that could impact human health or safety; Industrial Control systems and other "critical infrastructure" devices; and/or any other devices considered "Critical to the University" based upon its Risk Classification (section 2.1).**
ESSENTIAL	**Essential-Priority Assets** **Assets where the *disruption of access to or use of* data or an IT resource or the *unauthorized destruction* of data could be expected to have a *moderate* to *substantial* adverse effect on organizational operations, organizational assets, or individuals. The organization could work around the loss of the assets(s) for several days or perhaps a week , but eventually the assets(s) would have to be restored to a useable status to support essential operations.** **Essential-Priority assets include technology resources, applications and *network infrastructure devices* that function as key components of services listed as "Critical Resources" supporting the "Essential Functions" with an RTO between 12 and 72 hours as documented on the University-level or departmental COOP.**
NON-ESSENTIAL	**Non-Essential-Priority Assets** **Assets where the *disruption of access to or use of data* or an IT resource or the *unauthorized destruction* of data could be expected to have an insignificant to limited *adverse* effect on organizational operations, organization assets, or individuals. The organization can operate without the asset(s) for an extended (though perhaps finite) period, during which some units or individuals may be inconvenienced and/or need to identify alternatives.** **Non-Essential-Priority assets may have an undefined RTO.**

3. Maintenance of Standard

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

4. References

1. Virginia Tech Policy no. 7010: https://policies.vt.edu/assets/7010.pdf
2. NIST SP 500-19: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-19.pdf
3. NIST SP1800-26: https://www.nccoe.nist.gov/publication/1800-26/VolA/index.html
4. Family Educational Rights and Privacy Act (FERPA): https://www.govinfo.gov/content/pkg/USCODE-2021-title20/pdf/USCODE-2021-title20-chap31-subchapIII-part4-sec1232g.pdf https://www.federalregister.gov/documents/2017/01/19/2017-00958/family-educational-rights-and-privacy-act

5. Code of Virginia §23.1-405. Student records and personal information; social media: https://law.lis.virginia.gov/vacode/title23.1/chapter4/section23.1-405/
6. Code of Virginia §2.2-3808. Collection, disclosure, or display of social security number; personal identifying information of donors; penalty: https://law.lis.virginia.gov/vacode/2.2-3808/
7. Code of Virginia §18.2-186.6. Breach of personal information notification: https://law.lis.virginia.gov/vacode/18.2-186.6/
8. Code of Virginia §18.2-186.3. Identity theft; penalty; restitution; victim assistance: https://law.lis.virginia.gov/vacode/18.2-186.3/
9. Payment Card Industry Data Security Standard: https://www.pcisecuritystandards.org/
10. FTC Safeguards Rule implementing sections 501 and 505(b)(2) of the Gramm Leach-Bliley Act: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314
11. NACHA Operating Rules: https://www.nacha.org/rules/operating-rules
12. Code of Virginia §32.1-127.1:05. Breach of medical information notification: https://law.lis.virginia.gov/vacode/title32.1/chapter5/section32.1-127.1:05/
13. HIPAA "Security Rule": https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160
14. VT Privacy and Research Data Protection program: https://www.research.vt.edu/sirc/prdp.html
15. Controlled Unclassified Information (CUI): https://obamawhitehouse.archives.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information
16. International Traffic in Arms Regulations (ITAR); 22 CFR §§120-130: https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M
17. Export Administration Regulations (EAR) 15 CFR §§730-774; https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-730
18. Export and Import of Nuclear Equipment and Material Regulations (EINEMR); 10 CFR §110: https://www.ecfr.gov/current/title-10/chapter-I/part-110
19. Foreign Assets Control Regulations (FACR) 31 CFR §§500-599: https://www.ecfr.gov/current/title-31/subtitle-B/chapter-V
20. Assistance to Foreign Atomic Energy Activities Regulations (AFAEAR) 10 CFR §810: https://www.ecfr.gov/current/title-10/chapter-III/part-810
21. Unclassified Nuclear Controlled Information (UNCI) 42 U.S.C. 2168: https://www.govinfo.gov/app/details/USCODE-2021-title42/USCODE-2021-title42-chap23-divsnA-subchapXI-sec2168
22. Protection of Human Subjects 45 CFR 46: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-46

5. Revisions

Version 1, published July 2017

Version 2, published February 2019

Minor grammatical edits were made on the first page to improve sentence structure.

Version 3, published November 2020

In this version, “medical information” was added as an example of high risk data on page 2

Version 4, published December 2022

In this version, “contact and student directory information not designated by the individual as confidential in MyVT” was deleted as an example of low risk data, because student directory data is suppressed by default.

Version 5, published June 2023

Risk Classification guidance was completely reorganized, and additional examples/scenarios were added. Addition of “priority” classification label definitions and scenarios were also added.

Version 6, published June 2025

Risk Classification Labels modified to remove references to a reporting requirement as part of the definition for high-risk data. Data Risk Classification table modified to move most FERPA protected data to the moderate-risk category.