Virginia Tech Risk Classifications

Virginia Tech is committed to protecting the privacy of its students, alumni, current and former employees, and retirees as well as protecting the confidentiality, integrity, and availability of information important to the university's mission.

Virginia Tech has classified its information assets into risk-based categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect against unauthorized access.

As of July 2017, a new set of classifications has been established and is now in effect for Virginia Tech data and systems: **Low Risk**, **Moderate Risk**, and **High Risk**. The former framework — public, university-internal, and limited-access — will be phased out by January 2018.

Low Risk

Data and systems are classified as low risk if they are not considered to be moderate or high risk, and:

1. The data is intended for public disclosure, or
2. The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our mission, safety, finances, or reputation.

Moderate Risk

Data and systems are classified as moderate risk if they are not considered to be high risk and:

1. The data is not generally available to the public, or
2. The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on our mission, safety, finances, or reputation.

High Risk

Data and systems are classified as high risk if:

1. Protection of the data is required by law/regulation,
2. Virginia Tech is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed, or
3. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

Data Risk Classification Examples

Use the examples below to determine which risk classification is appropriate for a particular type of data. *When mixed data falls into multiple risk categories, use the highest risk classification across all.* Note: This is not an exhaustive list of examples.

Low Risk

- Research data (at data owner's discretion)
- Information authorized to be available on or through Virginia Tech's website without PID/Hokies authentication
- Procedure manuals designated by the owner as public
- Job postings
- University contact and student directory information not designated by the individual as "confidential" in MyVT
- Information in the public domain
- Publicly available campus maps

Moderate Risk

- Unpublished research data (at data owner's discretion)
- Properly de-identified research data
- Employment applications and personnel files without PII, as well as non-directory contact information
- Internal memos and email, nonpublic reports, intellectual property, and all other information releasable in accordance with the Virginia Freedom of Information Act.
- Donor contact information and non-public gift information

High Risk

- Social Security Numbers
- Credit and debit card numbers
- Financial account numbers
- Export controlled information under U.S. laws
- Driver's license numbers
- Passport and visa numbers
- Student records
- Engineering, design, and operational information regarding VT infrastructure

Server Risk Classification Examples

A server is defined as a technology resource that provides a network accessible service whether the hardware is on-campus or hosted remotely.

Low Risk

- Servers storing low risk data
- Servers used for research computing purposes without involving moderate or high risk data
- File server used to store published public data

Moderate Risk

- Servers handling moderate risk data
- File server containing nonpublic procedures/documentation

High Risk

- Servers handling high risk data
- Server storing student records
- Servers managing access to other systems
- University IT and departmental email systems
- Active Directory and Enterprise Directory
- DNS
- DHCP

Application Risk Classification Examples

An application is defined as software running on a server that is network accessible.

Low Risk

- Applications handling low risk data
- Online maps
- University online catalog displaying academic course descriptions
- Directory containing phone numbers, email addresses, and titles

Moderate Risk

- Applications handling moderate risk data
- Human Resources application that stores personnel information

High Risk

- Applications handling high risk data
- Human Resources application that stores PII
- Application that stores campus network node information
- Application that processes credit card payments
- Application collecting financial information of donor, alumnus, or other individual
- Online application for student admissions
- University application that distributes information in the event of a campus emergency

Version 1, published July 2017