UVM Data Classification Matrix

The University of Vermont 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 it against unauthorized access.

Special note to UVM researchers: Except for regulated data such as Protected Health Information (PHI) as defined under HIPAA, Social Security Numbers (SSNs), financial account numbers, and data covered under explicit Data Use Agreements (DUAs), non-sensitive research data and systems will most often fall into the **Low Risk** classification. However, even **low risk data** can have intellectual property concerns. Researchers should be aware of any intellectual property rights on research data and classify it accordingly. Review the classification definitions and examples below to determine the appropriate risk level to apply. For more information security practices and guidelines specific to research computing systems, see:

- UVM policy: Controlled Unclassified Information
- UVM Research Protections Office
- UVM Office of Research Integrity
- UVM Enterprise Technology Services

Low Risk	**Moderate Risk**	**High Risk**	**Restricted**
Data and systems are classified as **Low Risk** if they are not considered to be **Moderate Risk, High Risk**, or **Restricted**, and	Data and systems are classified as **Moderate Risk** if they are not considered to be **High Risk** or **Restricted**, and:	Data and systems are classified as **High Risk** if they are not considered to be **Restricted**, and:	Data and systems are classified as **Restricted** if:
1. The data is intended for public disclosure, is generally available to the public, or	1. The data is not generally available to the public, or	1. Disclosure of the data to the public is prohibited, or	1. General protection and handling of the data is prescriptively required by law/regulation/ contract and
2. If the data were lost, inappropriately accessed, used, or disclosed, or there was a loss of confidentiality, integrity, or availability of the data or system, there would be no adverse impact on, or harm to, UVM's mission, safety, finances, or reputation, or	2. The loss of confidentiality, integrity, or availability of the data or system could have an adverse impact on our mission, safety, finances, or reputation, or	2. UVM is required to self-report to the government/law enforcement or provide notice to the impacted individuals if the data is inappropriately accessed, used, or disclosed, or	2. UVM is required to self-report to the government/law enforcement or provide notice to the impacted individuals if the data is inappropriately accessed, used, or disclosed, or
3. The data is **not** personally identifiable, cannot be used in whole or in part to identify an individual or, when combined with other data elements or information, cannot identify an individual.	3. The data is **not** personally identifiable, cannot be used in whole or in part to identify an individual or, when combined with other data elements or information, cannot identify an individual.	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, or	3. The loss of confidentiality, integrity, or availability of the data or system could threaten national security as well as have a significant adverse impact on UVM's mission, safety, finances, or reputation, or
		4. The data **is** personally identifiable, can be used in whole or in part to identify an individual or, when combined with other data elements or information, can identify an individual.	4. The data is personally identifiable, can be used in whole or in part to identify an individual or, when combined with other data elements or information, can identify an individual,

			and disclosure will likely negatively impact the individual.

Data Risk Classification Examples

Use the examples below to determine which risk classification is appropriate for a particular type of data. This is not an exhaustive list. If you are ever in doubt, always ask the data steward listed beginning on page 10 of UVM's Information Security Procedures or contact the Office of Compliance and Privacy Services. Always defer to the most stringent risk category classification - when mixed data falls into multiple risk categories, use the highest risk classification for all data.

Low Risk	Moderate Risk	High Risk	Restricted
• Non-sensitive Research data (at data stewards discretion based on approved data management plan) • UVM Net ID usernames • Information authorized to be available on or through UVM's website without campus credentials (UVM or LCOM Net ID authentication) • Policy and procedure manuals designated by the owner as public • Job postings • University contact information not designated by the individual as private • Information in the public domain • Publicly available campus maps	• Unpublished research data (at data steward's discretion) • Student records and admission applications • Faculty/staff employment applications, personnel files, benefits, salary, birth date, personal contact information • Non-public University policies and policy manuals • Non-public contracts • University internal memos and email, non-public reports, budgets, plans, financial info • University and employee ID numbers • Project/Task/Award (PTA) numbers	• Health Insurance policy ID numbers • Social Security Numbers • Financial account numbers • Police Records/Individual Criminal Records • Driver's license or non-driver state identification card numbers • Individual taxpayer identification numbers • Passport and visa numbers • Military identification card numbers • Other identification numbers that originate from a government identification document that is commonly used to verify identity • Passwords, Personal Identification Numbers (PINs) • Donor contact information and non-public gift information • Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs • Trade union membership • Genetic data, biometric data • Data concerning a person's sex life or sexual orientation • Engineering, design, and operational information regarding university infrastructure.	• Health Information (physical and mental), including Protected Health Information (PHI) • Cardholder Data (CHD) per PCI DSS • Export controlled information • Controlled Unclassified Information (CUI) • Special Category Data (GDPR)

Data Compliance Classification Examples

The following examples are not an exhaustive list. If you are ever in doubt, always ask the data steward listed under the Data Steward Designations section of UVM's Information Security Procedures or contact the Office of Compliance and Privacy Services.

Low Risk	Moderate Risk	High Risk	Restricted
• **Anonymized data** - Data that has gone through an anonymizing process by which it removes information from data that would otherwise allow recognition of particular individuals. • **Deidentified data without a reidentification code** – Data in which identifiers have been removed according to the regulation that covers the data and that do not have a reidentification code. For example, health information is deemed deidentified if it meets HIPAA requirements. Student record data has been deemed deidentified if it meets the definition under FERPA. If no regulation exists, UVM uses HIPAA's deidentification process as a guide. • Data otherwise not protected or regulated by policy or regulation • Aggregate data	• **Deidentified data with a reidentification code** – the same definition as listed in the Low Risk column except that the data has a reidentification code that allows authorized individuals to re-identify the data. • Non-Health (physical and mental), non-financial FERPA data • Data Use Agreements with general data protections called out • GDPR	• Health-related (physical and mental) FERPA data • GLBA • Student Financial Aid Data • GDPR non-special category data	• HIPAA • PCI DSS • Export controlled data • FISMA • CUI • GDPR special category data • Data Use agreements with explicit compliance requirements

Server Risk Classification Examples

A server is defined as a host that provides a network accessible service.

NOTE: servers are the responsibility of official IT units sanctioned by the CIO and **should not be run** by individuals or individual groups unless a formal approval and documentation process has occurred. If you believe data is being run on local servers and not going through Enterprise Technology Services, contact the Information Security Office for further guidance.

Low Risk	Moderate Risk	High Risk	Restricted
• Servers used for research computing purposes without involving **Moderate Risk**, **High Risk**, **or Restricted** Data • File server used to store published public data • Database server if the only identifiers contained are UVM Net IDs. • The server does not require user authentication and **only** contains low risk data	• Servers handling **Moderate Risk** Data • Database of non-public University contracts • File server containing non-public procedures/ documentation • Server storing non-health related student records • Server requiring NetID or LCOM username authentication	• Servers handling **High Risk** Data • Servers managing access to **High Risk** systems • Core campus infrastructure • Server storing employee or student health records • Server requiring privileged account and/or group access or special network controls	• Servers handling **Restricted** Data • All hosts enclosed in a special-purpose enclave due to regulatory requirements • Server requiring privileged account and/or group access or special network controls • CIO approved multi-factor authentication

Application Risk Classification Examples

An application is defined as software running on a university sanctioned server that is network accessible. If you are unsure whether the server you are running is university sanctioned, contact the Information Security Office for further guidance.

Low Risk	Moderate Risk	High Risk	Restricted
• Applications handling **Low Risk Data** • Online maps • University online catalog displaying academic course descriptions • Bus schedules • Publicly available salary information	• Applications handling **Moderate Risk Data** • Mechanisms for salary distribution • Directory containing phone numbers, email addresses, and titles • University application that distributes information in the event of a campus emergency • Online application for student admissions	• Applications handling **High Risk Data** • Human Resources application that stores employee SSNs • Application that stores campus topology information • Applications that store student/family and employee financial information • Employee salary information from sources outside of UVM and salary data that is not otherwise public • Application collecting personal information of donor, alumnus, or other individual • Application that processes credit card payments	• Applications handling **Restricted Data** • Research computing dealing with CUI • Application accepting CHD for payments • HR, Student Health Service, and provider applications that store health information • Research computing under a DUA or other agreement with strict security requirements(?)

Approved Services – Non-Research

This table indicates which classifications of data are allowed on a selection of commonly used UVM IT services. This is not a comprehensive list. Please verify with the appropriate data steward for the service allowed for your data type. For a list of current data steward designations, see page 10 of UVM's Information Security Procedures. If you are ever unsure, contact the Chief Privacy Officer for further guidance.

Low Risk	Medium Risk	High Risk	Restricted
• www.uvm.edu • www.med.uvm.edu	• BrightSpace • PlanOn • Email • OneDrive • COMET, VIC and related applications • PeopleAdmin • SharePoint Services • Axiom	• PeopleSoft • Banner • SEDRC	• PointNClick • ASPN • HIPAA/PHI enclave(s) • CMMC enclave(s)

Approved Services for Research

Researchers should consult with Enterprise Technology Services/LCOM Information Security at iso@uvm.edu whenever collecting, using, or storing restricted data. The following is not an exhaustive list. Should you ever have any questions please reach out to one of the following:

- Sponsored Project Administration
- Vice President for Research
- Chief Information Officer
- Information Security Officer

Low Risk	Medium Risk	High Risk	Restricted
• Public data • Read Only/View access	• Coded data with no additional requirements (no BAA or DUA requirements where the key is kept separately and securely)	• Identifiable Data (human subject research) • Required Protections covered under Data Use agreement	• CUI • Export Controlled Data • PHI • Required protections under BAA
• www.uvm.edu • VACC • Zoo files • LCOM file servers • OneDrive • Local computer hard drives • Removable media	• OneDrive • Restricted access institutional file servers • LCOM secured L: drive • Qualtrics • REDCap	• LCOM SEDRC • REDCap	• CMMC enclave(s)