DATA CLASSIFICATION MATRIX

Special note to UVM researchers: If you are working with human subjects data, visit https://www.uvm.edu/rpo/research-data-management-human-participant-protocols or click on the link below. This matrix does not address research data management for human participant protocols. If you are working with non-human subjects data, follow these charts below. As it relates to non-human subject research data, it is important to note that even low risk data can have intellectual property concerns. Researchers working with non-human subjects data should be aware of any intellectual property rights on this 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

Researchers working with human subjects data, visit:
Research Data Management for Human Participant Protocols

Instructions: All data in use at UVM will fall into one of these categories. If you have a combination of levels, always pick the highest. For example, if your data set contains mostly information that is intended for public disclosure but one data element that is classified as "high-risk" then your data set should be handled as high-risk.

IMPORTANT NOTE: This matrix is a guide. You may have additional information that puts data in a different category than what is listed. If you ever have any questions or want to discuss a discrepancy, contact the Information Security Office at iso@uvm.edu or the Office of Compliance and Privacy Services at privacy@uvm.edu and someone can help you work through the classification.

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 **MODERATE RISK** if they are not considered to be **HIGH RISK**, or **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

LOW RISK	MODERATE RISK	HIGH RISK	RESTRICTED
• Non-sensitive Research data (at data stewards discretion based on approved data management plan)	• Unpublished research data (at data steward's discretion)	• Health Insurance policy ID numbers	• Health Information (physical and mental), including Protected Health Information (PHI)
• UVM Net ID usernames	• Student records and admissions applications	• Social Security Numbers	• Cardholder Data (CHD) per PCI DSS
• Information authorized to be available on or through UVM's website without campus credentials (UVM or LCOM Net ID authentication)	• • Faculty/staff employment applications, personnel files, benefits, salary, birth date, personal contact information	• Financial account numbers	• Export controlled information
• Policy and procedure manuals designated by the owner as public	• Non-public University policies and policy manuals	• Police Records/Individual Criminal Records	• Controlled Unclassified Information (CUI)
• Job postings	• Non-public contracts	• Driver's license or non-driver state identification card numbers	• State-Specific Data defined under state law (VCDPA, PIPA, CPA, and others)
• University contact information not designated by the individual as private information not designated by the individual as private	• University internal memos and email, non-public reports, budgets, plans, financial info	• Individual taxpayer identification numbers	• Special Category Data (GDPR, PIPL, LGPD, other international privacy laws)
• Information in the public domain • Publicly available campus maps	• University and employee ID numbers • Project/Task/Award (PTA) number	• 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	

DATA COMPLIANCE CLASSIFICATION EXAMPLES

The following examples are not an exhaustive list. If you are ever in doubt, always ask the data steward for your department, college, or unit or contact the Office of Compliance &

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 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.	• Health-related (physical and mental) FERPA data	• HIPAA • PCI DSS • Export Controlled Data • FISMA • CUI
• 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.	• Non-Health (physical and mental), non-financial FERPA data	• Non-special category data specified in State and International Privacy Laws (VCDPA, PIPA, CPA, GDPR, PIPL, LGPD, and others)	• Non-special category data specified in State and International Privacy Laws (VCDPA, PIPA, CPA, GDPR, PIPL, LGPD, and others)
• Data otherwise not protected or regulated by policy or regulation • Aggregate data	• Data Use Agreements with general data protections called out	• GLBA • Student Financial Aid Data	• Data Use Agreements (DUAs) with explicit compliance requirements

SERVER RISK CLASSIFICATION EXAMPLES

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

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

APPLICATION RISK CLASSIFICATION EXAMPLES

An application is defined as software running on a university sanctioned server that is network accessible. If you areunsure whether the server you are running is university

LOW RISK	MODERATE RISK	HIGH RISK	RESTRICTED
• Applications handling **Low Risk Data**	• Applications handling **Moderate Risk Data**	• Applications handling **High Risk Data**	• Applications handling **Restricted Data**
• Online maps	• Mechanisms for salary distribution	• Human Resources application that stores employee SSNs	• Research computing dealing with CUI
• University online catalog displaying academic course descriptions • Bus schedules	• Directory containing phone numbers, email addresses, and titles • University application that distributes information in the event of a campus emergency	• Application that stores campus topology information • Applications that store student/family and employee financial information	• Application accepting CHD for payments • HR, Student Health Service, and provider applications that store health information
• Publicly available salary information	• Online application for student admissions	• 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	• 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

LOW RISK	MODERATE 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	• Point-N-Click • ASPN • HIPAA/PHI enclave(s) • CMMC enclave(s)

APPROVED SERVICES - RESEARCH

Approved Services for research should refer to Research Data Management for Human Participant Protocols listed below. Whenever collecting, using, or storing human subjects

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

Researchers working with human subjects data, visit:
Research Data Management for Human Participant Protocols