Data Classification Policy
USG Policy 6 (2.10) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

Data are strategic assets of USG and must be handled in compliance with regulatory and legal obligations. The following standards set the criteria for classifying institutional data into categories and for determining what baseline security controls provide an appropriate protection to confidentiality, integrity or availability the institutional data.

The data classification also assists data stewards, IT system owners and custodians in the assessment of information systems to determine what level of security is required to protect data on the systems for which they are responsible.

This classification exists in addition to all other USG IT security policies and federal and state regulations governing the protection of USG's data. Compliance with this classification standard will not ensure that data will be properly secured. Instead, any data classification should be integrated into a comprehensive technology control plan.

All USG employees, students, affiliates and third-party agents who handle institutional data should follow these standards.

USG is the owner and/or custodian of all institutional data that are stored, processed, or transmitted on campus resources or other resources where USG business occurs. All institutional data should be classified into one of the four categories defined below. Any personal data belonging to the operator of a system that may be stored, processed, or transmitted on a USG IT resource as the result of incidental personal use is not considered institutional data. USG data stored on non-USG OIT resources must still be verifiably protected according to the respective USG minimum security standards.

Based on the data classification, IT system owners and custodians are required to implement appropriate technical security measures to protect the data consistent with the USG's policies and applicable federal and state regulations.

The Universities at Shady Grove is hereinafter referred to as "USG" and the Office of Information Technology as "OIT." This policy will be reviewed annually to ensure continual compliance with USM IT Security Standards and other pertinent policies, laws and industry standards.

II. Definitions

A. *Authentication*: a security method used to verify the identity of a user and authorize access to a system or network.

B. *Encryption*: the process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

III. Policy Statement

A. The data classification list below specifies the four categories and examples that must be maintained and disseminated by OIT (see Appendix A in this policy for USG's Data Classification Table). All institutional data should be classified into one of four categories described below:

1. **CATEGORY LOW (Level 1)**

   Data and systems likely do not require management of risks, vulnerabilities, and threats.

   - Data and systems are classified as LOW information technology risk.
   - The information can be publicly disclosed.
   - The loss of confidentiality, integrity or availability of information would have no adverse impact on USG mission, safety, finances, or reputation.
   - USG has permission or individual authorization to publish the information.

2. **CATEGORY MODERATE (Level 2)**

   Data and systems generally require management of risks, vulnerabilities, and threats.

   - Data and systems are classified as MODERATE information technology risk.
   - The information is to be kept confidential as a matter of institutional policy or practices.
   - The loss of confidentiality, integrity or availability of information could have a moderate adverse impact on USG's mission, safety, finances, or reputation.
   - USG may notify individuals of any breach as a matter of policy or practice.

3. **CATEGORY HIGH (Level 3)**

   Data and systems require active management of risks, vulnerabilities, and threats.

   - Data and systems are classified as HIGH information technology risk.
   - The information is to be kept confidential as a matter of law, regulation, or contractual obligation.
   - The loss of confidentiality, integrity or availability of information could result in civil penalties and damages and/or have a significant adverse

impact on USG's mission, safety, finances, or reputation.

- USG is required by laws and regulations to notify individuals of any breach in confidentiality.

4. **CATEGORY RESTRICTED (Level 4)**
   Data and systems require specific management of risks, vulnerabilities, and threats.
   - Data and systems are classified as RESTRICTED information technology risk.
   - The information must be kept confidential as a matter of law, regulation, or contractual obligation.
   - The loss of confidentiality, integrity or availability of information could result in civil and criminal penalties and damages and/or have a severe adverse impact on USG's mission, safety, finances, or reputation.
   - USG is required by laws and regulations to notify individuals of any breach in confidentiality.

B. Classification of the data can be performed in consultation with the appropriate data steward and/or in conjunction with institutional offices responsible for information security, compliance and ethics. System selection, data security controls, and compliance measures must be implemented commensurate with the categorization of the data.

It is the responsibility of the applicable data manager to evaluate and classify data for which he/she is responsible according to the classification system adopted by USG. If data of more than one level of sensitivity exists in the same system or endpoint, such data shall be classified at the highest level of sensitivity.

IV. Enforcement

A. The enforcement of this policy will be carried out by authorized USG OIT personnel designated by the Director of OIT and USG Senior Leadership. Violations may result in disciplinary actions, which may include suspension, restriction, or revocation of access. Where illegal activities or theft of USG property (physical or intellectual) are suspected, USG may report such activities to the state/federal law enforcement authorities.

V. Revision History

Date	Description	Revised By
05/31/2018	Initial Policy Creation	Russell Schlosburg
10/28/2021	Updated Elevated to High and High to Restricted to align with UMD's Data Classification Policy	Russell Schlosburg

VI. Related Documents

A. USM IT Security Standards v4
http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

B. Maryland Public Information Act
http://www.marylandattorneygeneral.gov/Pages/OpenGov/pia.aspx

Appendix A

CATEGORY LOW (Level 1)	CATEGORY MODERATE (Level 2)	CATEGORY HIGH (Level 3)	CATEGORY RESTRICTED (Level 4)
Data and systems likely do not require management of risks, vulnerabilities, and threats.	Data and systems generally require management of risks, vulnerabilities, and threats.	Data and systems require active management of risks, vulnerabilities, and threats.	Data and systems require specific management of risks, vulnerabilities, and threats.
Data and systems are classified as **LOW** information technology risk. The information can be publicly disclosed. The loss of confidentiality, integrity or availability of information would have no adverse impact on USG mission, safety, finances, or reputation. USG has permission or individual authorization to publish the information.	Data and systems are classified as **MODERATE** information technology risk. The information is to be kept confidential as a matter of institutional policy or practices. The loss of confidentiality, integrity or availability of information could have a moderate adverse impact on USG's mission, safety, finances, or reputation. USG may notify individuals of any breach as a matter of policy or practice	Data and systems are classified as **HIGH** information technology risk. The information is to be kept confidential as a matter of law, regulation, or contractual obligation. The loss of confidentiality, integrity or availability of information could result in **civil** penalties and damages and/or have a significant adverse impact on USG's mission, safety, finances, or reputation. USG is required by laws and regulations to notify individuals of any breach in confidentiality.	Data and systems are classified as **RESTRICTED** information technology risk. The information must be kept confidential as a matter of law, regulation, or contractual obligation. The loss of confidentiality, integrity or availability of information could result in **civil and criminal** penalties and damages and/or have a severe adverse impact on USG's mission, safety, finances, or reputation. USG is required by laws and regulations to notify individuals of any breach in confidentiality.

EXAMPLES

✓ Information disclosed in the public domain (websites and social media) ✓ Information disclosed in USG's administrative and academic websites ✓ Information required by law and regulations to be made public ✓ Email addresses (except student assigned) ✓ Public USG policies and procedure manuals ✓ Job postings ✓ Schedule of Classes	✓ Unclassified research information and pre-publication data (at researcher's discretion) ✓ Faculty/staff employment information, personnel files, salary, and personnel data ✓ Institutional and SG ID Numbers ✓ Non-public contracts (unless required to be Category 3 or 4) ✓ Patent applications ✓ Non-public documents, policies, and procedure manuals ✓ Information exempt from disclosure under the Public Information Act (e.g., pre-decisional documents, pre-award procurement data) ✓ Invoices and budgets ✓ Intellectual property not yet protected by provisional patent application or patent ✓ Privileged information (attorney work product, attorney-client privilege, etc.)	✓ Personally identifiable information ✓ Protected health information used for research purposes ✓ Information governed by FERPA* such as student records and admission applications. ✓ Donor contact information ✓ Information that is contractually required to comply with NIST 800-171 or DFARS ✓ RFP responses ✓ Federal government information deemed Sensitive But Unclassified (SBU) or For Official Use Only (FOUO), unless covered by Category 4 ✓ Government Rights & Restricted Rights Data (federal government designation) ✓ Institutional review board applications ✓ Confidential business or financial information obtained via a non-disclosure agreement (including trade secrets, intellectual property, teaming strategies, and proposal documents) *Family Educational Rights and Privacy Act (FERPA) (20 U.S.C.§ 1232g; 34 CFR Part 99).	✓ [✻] Protected health information governed by HIPAA ✓ [✻] Export controlled information governed by ITAR or EAR ✓ Social Security Numbers ✓ [✻] Customer credit card information ✓ Financial account numbers ✓ Health insurance policy ID numbers ✓ Driver's license numbers ✓ Passport and visa information ✓ Contracts (and related information) with the NSA/Maryland Procurement Office ✓ [✻] Materials deemed For Official Use Only (FOUO), Controlled Unclassified Information (CUI) pursuant to the National Security Agency Act of 1959, P.L. 86-36 § 6; 50 U.S.C.§ 3605 or NIST SP800-171. [✻] Special data storage and handling requirements are required. Please contact usg-oit@umd.edu for advice.