

UMES Data Classification Policy

Last modified on September 27, 2024

UMES Data Classification Policy

1. I. Policy

The purpose of this policy is to provide a template for the classification of all electronic documents and files based upon the business use and contents of those files.

1. II. Scope:

This policy governs all electronic data that is owned or handled by UMES, its employees and contractors, and any 3rd party that has a binding business agreement.

1. III. Classification:

Files can be classified into one of the following three categories.

Red or Level 3	A red classification is given to any files that contain personally identifiable information (PII), or protected information that may contain SSN, DOB, driver's license number, credit card or financial information, and any other data that do not meet the security standards as outlined by NIST 800-122 and industry standards such as HIPAA and PCI-DSS. Files with this classification must have been granted by the IT Security Officer and the related departmental data steward. All transmittal must be approved by the IT Security Officer.
Yellow or Level 2	A yellow classification is appropriate for files that contain business sensitive information, but does not contain PII. Examples may include University internal memos, University sponsored research findings, or internal statistical data. This information may be shared internally within the campus, but will require approval from the Department head to share to an external party.
Green or Level 1	A green classification is appropriate for files that contain information that is publicly disclosed or is otherwise available to the public. Examples such as Campus announcements, public statements, and recruitment materials may fall into this category. This information does not require special handling and can be freely disseminated to any party.

1. IV. Examples of Personally Identifiable Information (PII):

Examples of PII include, but are not limited to, any information concerning a natural person that can be used to identify such natural person, such as name, number, personal mark or other identifier, in combination with any one or more of the following:

1. a. Social security number (SSN)

2. **b.** Driver's license number or non-driver identification card number
3. **c.** Account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.
4. **d.** Email address with password (in certain narrow instances)
5. **e.** Health information
6. **f.** Health Insurance Information.
7. **g.** Financial records with name or SSN
8. **h.** Human Resources records with name or SSN
9. **i.** Student records with name or SSN
10. **j.** Any files, not stated above, containing the name or SSN

Subject	Contact	Telephone
Policy	IT security officer	410-651-7640

Date: August 16, 2018