UMES Data Classification Policy

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 health information (PHI). This includes any files that contain SSN, DOB, driver's license number, credit card or financial information, and any other data that can be considered confidential under the current PII standards as outlines by NIST 800-122 and industry standards such as HIPAA and PCI-DSS. Files with this classification may not be shared unless permission has been granted by the IT Security Officer and the related departmental data steward. All transmittal must be done using an encrypted channel.
Yellow or Level 2	A yellow classification is appropriate for files that contain business sensitive information, but does not contain any personally identifiable information (PII). Examples may include University internal memos, University sponsored research findings, or internal statistics and reports. Files with a yellow classification can be shared internally within the campus, but will require approval from the Department head to share to any non-UMES entity.
Green or Level 1 .	A green classification is appropriate for files that contain information that is publically disclosed or is allowed to be disclosed to the public and any other party. Examples such as Campus announcements, public statements, and recruitment materials may fall into the green category. Files with a green classification do 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:

a. **a.** Social security number (SSN)
b. **b.** Driver's license number or non-driver identification card number
c. **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.
d. **d.** Email address with password (in certain narrow instances)
e. **e.** Health information
f. **f.** Health Insurance Information.
g. **g.** Financial records with name or SSN
h. **h.** Human Resources records with name or SSN
i. **i.** Student records with name or SSN
j. **j.** Any files, not stated above, containing the name or SSN

Subject	Contact	Telephone	E-mail
Policy	IT security officer	410-651-8068	jrsmith@umes.edu

Date: August 16, 2018

Cabinet approval pending. 12/13/18