Data and System Classification Model

Data Classification	Data		System Class
Highly Confidential	Credit Card/Procurement Card Information Banking Information (account/routing detail) Social Security Number Driver's license number Visa number Passport number TIN/Vendor ID numbers that are SSN Biometric Identifiers (fingerprint, iris scan print, palm print, ear lobe map, etc.) Personal Health Information (includes a separate policy discussion on HIPAA)	Sensitive Systems	1 High Risk
Protected	Personally identifiable information (PII) and/or other university data worthy of protection and discretion in its distribution Data used for university operations and/or mission and that is not HC or public May include data released if/when a FOIA request is filed		2 Medium Risk
	Non-public data used in amounts or circumstances that present little or no risk		3 Low Risk
Public	Web-site, social media, catalog or other content made public by the institution.		4 Public

System Management Plan

This System Management Plan is intended to provide key information necessary to effectively maintain a system. The plan describes the regular activities essential to the support and maintenance of the system as well as the roles and responsibilities of those responsible for administering the system. The System Owner is encouraged to expand upon this template to meet the needs of the system and department. This document should be reviewed on a regular basis and updated as necessary.

System Information

- System Name:

- Purpose:

- Vendor:

- Users of the system (check all that apply):
  - ☐ Students
  - ☐ Faculty
  - ☐ Staff
  - ☐ Affiliates *(specify affiliated group: ___________)*
  - ☐ Other ___________

- How do users access the system (e.g. JMU credentials, user created accounts, etc.)?

- JMU System Management Roles: *(complete the chart below)*

Role	Name	Title	Phone	Email
System Owner				
System Administrator				
Data Custodian				

Contract Information

- Vendor Contact Information: *(complete the chart below)*

Name	Title	Phone	Email

- Procurement Contact(s): *(complete the chart below)*

Contact Name	Title	Phone	Email

- Contract number:

- Contract Term (e.g. 1 year with 9 one-year renewals):

University Data

- Specify data processed, stored, or transmitted in the system *(e.g. student name, email, etc.)*.

- Does the data identified above have compliance or legal restrictions that may apply to the following regulations? *(check all that apply)*
  - □ FERPA
  - □ PCI
  - □ HIPAA
  - □ GLBA
  - □ Other ___________

- Where is the data hosted (e.g. on-campus or by the vendor)?

- Describe data interfaces or manual data transfer loads to or from existing University systems *(e.g. Student Administration System, Human Resources System, etc.)*.

- Will the data be processed/stored outside of the system? If yes, state location and plan for data protection.

- Describe the plan for ensuring the accuracy and integrity of the data being used/produced by the system.

- Describe the plan for ensuring all data stored in the system is securely transferred, returned, or destroyed upon contract expiration or termination.

System Administration

- The following individuals will have administrator rights to the system:

Name	Title	Phone	Email

- Describe the functions the system administrator(s) will perform (e.g. system upgrades, patches, data recovery, etc.):

- Account Creation, Account Changes, Account Deprovisioning and Account Reviews must comply with the Data Stewardship Standard. For each of the sections below, provide the step-by-step process for completing the task (i.e., a new employee should be able to follow the steps in order to complete the task).

Account Creation
* *The Account Creation process must include the employee's supervisor and Data Custodian or Data Manager approving the access request prior to an employee being granted access to the system.*

Account Changes
** The Account Change process must include the employee's supervisor and Data Custodian or Data Manager approving the employee account change prior to the change being granted in the system.*

Account Deprovisioning
** The Account Deprovisioning process must include timely deprovisioning of an employee's account.*

Account Reviews
** Process must specify account review frequency (e.g. annually, semi-annually, etc.) and include the step(s) for retaining documentation of the account review for auditing purposes.*

- Describe the roles/permissions available within the system as well as the associated individuals for each role/permission.

- Provide a contingency plan that includes alternate processing procedures to be used if the system becomes unavailable. The contingency plan should consist of detailed step-by-step instructions that could be followed by a new employee.

- Provide an incident response plan (IRP) that will be followed in the event of a cybersecurity incident. The incident response plan should consist of detailed step-by-step instructions that could be followed by a new employee and ensure that IT Security is notified prior to the vendor.

- Provide a change management plan for when it is determined that a change to the system is needed by the department. The change management plan should consist of detailed step-by-step instructions that could be followed by a new employee.

- Submit a diagram of the system if one is not already on file with IT.

Risk Mitigations

Step 1: List or attach the risk mitigations/recommendations provided by JMU Information Technology.
Step 2: Below each listed mitigation/recommendation, provide detail on how the risk is addressed by the System Owner/System Administrator/Data Custodian.
1. <1st Mitigation> Department Response: 2. <2nd Mitigation>

Department Response:

3. <3rd Mitigation>

Department Response:

System Management Plan Update History:

Date	*Updated By*	*Update Description*