APPENDIX A – Roles and Responsibilities

Division Heads/College Deans/Managers/Supervisors

These individuals shall be responsible for oversight of their employees' authorized use and access to University data in their areas of supervision. They will:

- Ensure that the management and control of risks outlined in this policy are adhered to by employees in their unit.
- Ensure employees' access to University data is appropriate.
- Regularly review and document employee access to University data.
- Identify the necessary Data Security Steward and ensure they receive adequate training to perform this role.
- Provide employees with resources and methods to properly secure equipment where University data is processed, stored, or handled.
- Provide employees with approved resources and methods for external data storage where University data is processed, stored, or handled.

IT Specialist

These individuals are responsible for being the technical support within a business unit, college/school, or department.

Data Security Steward

These individuals who are responsible for business processes within their areas of supervision will:

- Understand current Information Security policies, standards and guidelines and act as a point of contact for questions regarding Information Security and direct the user to the appropriate source (e.g., the ISO, policies, or standards).
- Operate as Information Security monitors in their divisions or colleges.
- Attend and participate annually in Data Security Steward Training provided by the ISO.
- Be the primary point of contact for suspected or actual data breaches and report the information to the ISO.
- Promote Information Security events/training and generate a culture of Information Security awareness.
- Recommend employees with access to Sensitive Information to the ISO for additional levels of training.
- Provide recommendations for revisions to this policy as appropriate.

Employees, including department chairs, faculty, staff, and student workers

These individuals:

- Shall not disclose Sensitive Information to unauthorized individuals.
- Shall not modify or delete University data unless authorized to do so.
- Shall maintain University data in a secure manner.
- Shall complete the employee/student confidentiality training.
- Shall be required to sign a University confidentiality/FERPA agreement before access is granted to Sensitive Information.
- Shall complete specific confidentiality training if they have job related responsibilities that require access to Sensitive Information.

Network Security Administrator

This individual, within the IT Division will:

- Implement adequate Security measures for computing systems containing University data within their jurisdiction.
- Implement appropriate Security strategies for both the transmission and the storage of University data.
- Notify appropriate units of possible Security infringements.
- Report any Security breach to the ISO.
- Disseminate technical guidelines related to Security to the appropriate IT Specialists.

Information Security Task Force

A group of individuals appointed by the President to review and evaluate University Security issues such as:

- Current practices and the associated risks to the institution.
- Actions needed to address those risks through appropriate policy and associated guidelines.
- Identify new processes that are needed.
- Implement new Security standards as needed.
- Disseminate general guidelines related to Security to the appropriate IT Specialists.
- Function as the Incident Response Team
    - Responsible for immediate response to any breach of Security.

- Responsible for determining and disseminating remedies and preventative measures that are developed as a result of responding to and resolving Security breaches.

Information Security Office

This office, within the IT Division will:

- Assist the campus in identifying internal and external risks to the Security and confidentiality of information.
- Provide guidance for handling University data in the custody of the University.
- Provide guidance for the Security of the equipment or data storage devices where the information is processed and/or maintained.
- Promote and encourage good Security procedures and practices.
- Develop and maintain Security policy, plans, procedures, strategies, and best practices.
- Provide standards and guidelines consistent with University policies.
- Develop and provide Information Security training.

Internal Audit

Internal Audit will:

- Evaluate the effectiveness of the current safeguards for controlling Security risks.
- Provide recommendations for revisions to this policy as appropriate.
- Develop and perform random audits of departments and individuals as deemed necessary.