POLICY & PROCEDURES MANUAL **WAYLAND BAPTIST UNIVERSITY**	**Classification Number: 6.4.1** **Inception: March 9, 2022**

SUBJECT: INFORMATION SECURITY

Purpose

4.1. ***Senior Leadership*** is responsible for:

Final approval of Information Security Policy.
Final approval of risk tolerance and risk acceptance.
Allocating budget and resources for Information Security initiatives and oversight.
Communicating and supporting Information Security awareness and compliance.

4.2. Senior Leadership shall establish ad hoc committees as needed, responsible for:

Reviewing and recommending strategies to implement the Information Security Policy annually and upon major or significant change to the policy.
Proposing risk tolerance and providing recommendations for accepting or rejecting risk related to security threats that impact the confidentiality, integrity, and availability of Institutional Data.
Identifying and documenting Information Owners.
Identifying and documenting Information Custodians.

4.3. ***Information Owners*** are responsible for:

Determining the appropriate criteria for obtaining access to University Information.

5.2. Separation of Duties

Separation of duty, as a security principle, has as its primary objective the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific security process among multiple users and chains of command. Owners and custodians of information

countermeasures) and business operations.

5.3. Confidentiality

confidentiality is the unauthorized disclosure of information.

5.4. Integrity

information non-
unauthorized modification or destruction of information.

5.5. Availability

availability is the disruption of access to or use of information or an information system.

Information Security Risk Management Framework

Wayland Baptist University shall establish a framework for Information Security Risk Management. The

7.2.2.

7.7.8. information systems shall be promptly identified, assessed, and remediated according to the associated risks they present to the University.

7.7.9. Audit activities involving verification of production information systems shall be carefully planned, formally authorized, and executed by qualified personnel only.

7.8. Communications Security

The University shall implement the following communications security controls:

7.8.1. devices shall be limited to authorized personnel only.

7.8.2. Network traffic traversing University owned networks shall be filtered to address any

resources.

7.8.3. Network traffic traversing University-owned networks shall be inspected for active attacks

effectively block attacks that present appreciable risks to the University.

7.8.4. Network services, users, and information services shall be segregated on networks based on trust levels and associated risks.

7.8.5. Transfer methods and controls shall be defined and adhered to protect University sensitive information traversing all forms of communication facilities to both internal and external senders and recipients.

7.8.6. Protection measures shall be established to safeguard University electronic messaging solutions from unauthorized access, modification, or denial of service. Retention of electronic messaging communication shall be maintained in an approved manner.

7.8.7. Confidentiality agreements shall be used to establish legally enforceable terms of utilization

employees.

7.9. Information Systems Acquisition, Development and Maintenance

The University shall implement the following security controls for acquisition, development, and maintenance of Information Systems:

7.9.1. The development and acquisition of information systems shall include the regular evaluation of security requirements in the earliest possible stages of related information system projects.

7.9.2. Secure program techniques and modeling methods shall be employed to ensure that coding practices adhere to best practices to limit potential for abuse.

7.9.3. Change control procedures shall be documented and enforced to ensure the confidentiality, integrity, and availability of information systems throughout maintenance efforts.

7.9.4. System acceptance testing shall include security testing and validation of effectiveness of controls related to any identified information security requirements.

7.9.5. If viable options are available, data that contains sensitive information shall not be used for system or application testing purposes. Test systems that do contain this data must adhere to common data security standards.

7.10. Third Party Access

Access to University information systems by third party vendors (i.e., contractors, partners, vendors, lessees) requires appropriate controls to protect University information assets. All third parties that

security policies and may be required to show proof of such compliance at any time.

7.10.1. Security requirements will be documented and agreed with each supplier that may access, process, store, or communicate University owned data.

7.10.2. Periodic review of supplier services will be conducted to ensure that related security agreements are being adhered to and enforced.

7.11. Information Security Incident Management

The following controls shall be implemented for Information Security Incident Management.

7.11.1. Information security events shall be reported through an approved channel and reviewed promptly by authorized Information Custodians.

7.11.2. Employees and contractors shall be encouraged to note and report any appreciable information security weaknesses observed in systems or services.

7.11.3. Response actions related to security incidents shall adhere to a documented set of procedures, including appropriate communication and coordination of efforts.

7.11.4. Knowledge gained during the analysis of security incidents shall be captured, reviewed, and appropriately shared to identify security corrections or control measures that may help address similar events.

7.11.5. Methods to preserve electronic evidence shall follow adequate standards of discovery and preservation to prevent spoliation.

7.12. Business Continuity Management

7.12.1. Planning shall be undertaken to ensure that appropriate levels of information security protection measures are maintained during emergencies or other adverse events. Periodic verification of these plans shall be performed on an annual basis.

7.12.2. Information processing facilities shall be implemented with redundancy sufficient to meet identified and documented availability needs.