AUA Risk Management Procedure

1. Purpose

To establish a process to manage risks to the American University of Armenia that result from threats to the confidentiality, integrity and availability of University Data and Information systems.

2. Applicability

This procedure applies to all data created, stored, processed or transmitted By AUA and the Information Systems used with that data.

3. Definitions

Information System: An individual or collection of computing and networking equipment and software used to perform a discrete business function. Examples include Moodle (eLearning system), Jenzabar SONIS and JRM (Student Information System), set of servers and desktop computers used to perform general duties in all Departments and Labs

Restricted Data: Data in any format collected, developed, maintained or managed by or on behalf of the University, or within the scope of University activities that are subject to specific protections under State law or regulations or under applicable contracts. Example include, but are not limited to medical records, social security numbers, credit card numbers, student records and research protocols.

AUA Data: Data in any format collected, developed, maintained or managed by or on behalf of the University, or within the scope of University activities. The terms “Data” and “Information” are used interchangeably in the context of information security program.

4. Procedure Specifies

1. All Information systems must be assessed for risk to AUA that results from threats to the integrity, availability and confidentiality of AUA. Assessments should be completed prior to purchase of, or significant changes to an information system and at least every 2 years for systems that store, process or transmit Restricted Data.
2. Risks identified by a risk assessment must be mitigated or accepted prior to the system being placed into operation.
3. Residual risks may only be accepted on behalf of the University by a person with appropriate level of authority as determined by a Chief Operating Officer and/or Chief Information Security Officer. Approval authority may be delegated if documented in writing, but ultimate responsibility for risk acceptance cannot be delegated.
4. Each Information system must have a system security plan, prepared using input from risk, security and vulnerability assessment.

5. Review and Adjudication

The Vice President (COO) and or Chief Information Officer (CIO) are responsible for implementing systems and specifications to facilitate unit compliance with this procedure.

6. Procedure Violations

Failure to comply with this procedure could result in disciplinary action for employees, up to and including termination.