INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE

1. Purpose

This procedure defines the procedure for the information security management of American University of Armenia (AUA), incuding information security incident reporting, classification, resolution and response. Sanctions to be applied for violation of the current document as well as persons who will be responsible for implementation of this procedure. The purpose of this procedure is also to clearly define IT roles and responsibilities for the investigationand response to Information security incidentsand data breaches.

2. Scope

This procedure applies to all information systems, regardless of ownership and location, as well as Staff, Students and Faculty.

3. Definitions

American University of Armenia – AUA

Information assets - All items of information stored, managed or conveyed either paper based, electronically or verbally. This includes all written or printed information, electronically created, stored or managed information as well as all business or work related verbally expressed information and conversations.

AUA Data – Data in any format collected, developed, maintained or managed on behalf of AUA, or within the scope of AUA activities.

Availability – assurance that information, assets and resources are accessible to authorized users as needed.

Confidentiality - protection of information from unauthorized access regardless of where it resides or how it is stored. The aim is to ensure that information is accessible only to those persons who are authorized accordingly.

Integrity - protection of information, applications, systems and networks from unauthorized change, be it intentional or accidental. The aim is to safeguard the accuracy and completeness of information and processing methods.

Threat is a potential event. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because the incident may harm an organization or system.

Vulnerability is a weakness in an asset or group of assets. An asset’s weakness could allow it to be exploited and harmed by one or more threats.

Information security event – event that indicates that the security of an information system, service, or network may have been breached or compromised. An information security event indicates that an information security procedure may have been violated or a safeguard may have failed.

Information security incident - is made up of one or more unwanted or unexpected information security events that could very likely compromise the security of information and weaken or impair business operations.

4. Responsibility

ISMS Manager is responsible for the maintenance, update and monitoring of compliance with requirements of this procedure.

5. Procedure

In the event that there is a potential or actual security incident, there are procedures defined to ensure that proper reporting of such incidents occur in a timely manner and that these incidents are brought to the attention of the ISMS manager. Proper incident reporting ensures that security issues are addressed and resolved timely to ensure that repeat attempts are not successful

5.1.General Controls

Below follows the list of events that should be reported and handled by AUA staff and ISMS Manager:

- A security breach or violation
- Disclosure of sensitive information
- Unusual activity regarding user/administrator accounts (such as account lockout, unusual last login time, unsuccessful login attempts, etc.)
- Social engineering attempts (e.g. suspicious phone calls, emails, lost USBs, conversations via skype and/or other messengers, etc.)
- Suspicious e-mail (e.g. spam, scam, phishing, etc.) Physical theft, loss (e.g. theft of laptop, computer, information media, etc.)
- Suspicious processes or applications (antivirus alarm, results of network monitoring, new software and/or application downloaded and/or installed from unauthorized sources)
- Unknown network connections
- Misuse of service, system or information
- Unexpected system crash
- Abnormally slow or poor performance
- Unexplained new users, file names, file sizes, modification dates, etc.
- Any other serious information security event, not described above.

In case if AUA employee suspects one of the events listed above he/she must communicate his/her concerns to his/her direct supervisor immediately to speed the identification of any damage caused, any restoration or any repair. The details surrounding the incident must then be communicated to ISMS manager. Resolution of the incident will be handled consistent with this procedure.

The HR, COO and AUA President should also be informed of major security incidents.

Information Security incidents must be properly investigated by suitably trained and qualified personnel.

In the event of security violation or breach, for AUA employees or third parties, disciplinary action will be consistent with the severity of the incident, as determined by an investigation. Disciplinary actions may include, but not limited to, loss of access privilege to data processing resources, dismissal of consultants, cancellation of contracts, termination of employment, or other actions as deemed appropriate. Disciplinary actions are coordinated according to the Incident Reporting standards.

For external incidents or threats, action must be taken to ensure evidential integrity is maintained and the appropriate legal action can be taken, if deemed necessary.

Proper follow up on the reported issues should be done according to the Incident Reporting standards so as to avoid these kinds of incidents in the future.

In cases where:

- The violation is clearly illegal with intent, notification to management shall be immediate.
- The intent is not clear, the violator shall be advised to correct the violation.
- There is a repeat violation, it shall be reported immediately to management and the appropriate disciplinary action will be taken based on the severity of the infraction.
- In case where repeated security violations cause support or resource-sharing problems, the matter must be referred to ISMS Manager who may defer support and/or report the violation to COO and AUA President

5.2. Incident Reporting

ISMS manager is responsible for developing and implementing a procedure for the incident management reporting and handling by ISMS manager, depending on the level of risk of the incident. The purpose is to restore the business services in an efficient and timely manner.

Incident Reporting Plan should address following areas:

- Problem identification (determine if it is IS event or IS incident, registration in Synergy portal and reporting to ISMS manager /management, analysis of root cause and consequences)
- Escalation (in case if the one who is responsible for resolving the incident has no necessary capabilities)
- Resolution and recovery (elimination of root cause and consequences)
- Disciplinary actions (if necessary)

- Follow up (adding resolution to the IS knowledge base, conduct trainings and raise employee awareness where necessary, etc.)

Information security incidents must be reported to outside authorities whenever this is required to comply with legal requirements or regulations and after taking the approval of AUA Management. This may only be done by authorized persons.

5.3 Final Provisions

The present document enters into force upon the COO’s approval, in the established order.

Any amendments or additions to this document shall be approved by COO.