# ICTS Data Access Procedure

The *Data Access Procedure*:

- Defines the roles, responsibilities, data management environment, and procedure for granting access to AUA non-public data
- Applies to university data in electronic format
- Supplements the Change Management Procedure and the Risk Management Procedure

Individuals who access, retrieve, update, process, analyze, store, distribute, or in other manners use university data are responsible for securing and protecting the data in accordance with the Change Management Procedure and the Risk Management Procedure.

## 1. Overview

The American University of Armenia (AUA) shall approve access to Protected Institutional Data (defined below) to ensure that access to sensitive data is authorized, that sensitive data with a need for protection are used appropriately, and that authorized access complies with all applicable RA laws, University Rules, and ICTS' Data Classification Standards, policies and procedures.

## 2. Purpose

This procedure outlines requirements for accessing and handling Protected Institutional Data.

## 3. Scope

This procedure applies to all Protected Institutional Data maintained by AUA or a party acting on behalf of the university. This procedure does not apply to data or records that are personal property of a member of the university community.

## 4. Definitions

- **Data Owner** – The American University of Armenia is the data owner of all university data; individual units or departments have data trustee responsibilities for portions of the data.
- **Data Trustee** – The individual or group who has accountability and authority to make decisions about a specific set of data. The Data Trustee is responsible for the function or functions that collect and use the information, determines the levels of protection for the information, makes decisions on appropriate use of the information, and determines the appropriate classification of the information. This role generally falls to a functional administrative or academic area, such as the Registrar, Human Resources, or the offices of the CFO, COO and Provost. In case of the access to the fileserver, Moodle system – the Dean of the Department.
- **Data Manager** – University officials and their staff with operational-level responsibility for information management activities related to the capture, maintenance, and dissemination of data.
- **Data Administrator** – The persons or unit responsible for implementing controls the Data Trustee identifies. This role often includes Information Technology Services or departmental technology support.
- **Data User** – Any person who interacts with the data. This includes people or programs that create, update, read, or delete information.

- **External Third Party** – Any organization, vendor, contractor, or partner operating on behalf of the university.
- **Incident Response Team** – The individuals responsible for investigating data breaches and other information security incidents. These individuals may include, but are not limited to AUA Information Security Services, AUA Information Security Officer (ISO)
- **Institutional Data** – Any information or data that is gathered, analyzed, or published by any department of the University of Akron in support of its mission(s).
- **Protected Institutional Data** – Any information classified as more restricted than Public Use by the Data Trustee, or appointed Data Manager(s), according to ICTS Data Classification Standards.

## 5. How to Request Access

Regardless of the system you are requesting access for, conceptually, the request process flow should be the same:

| | ***REQUEST*** | ***APPROVAL*** | ***IMPLEMENTATION*** |
|---|---|---|---|
| ***Who?*** | Data Manager | Data Trustee | Data Administrator |
| ***How?*** | Sends approval request to Data Trustee*. | Sends his/her data access approval to the Data Manager, ICTS director and System Administrator | Provides System and Application Specific Access |

Specific data access spreadsheet can be found here:

https://docs.google.com/spreadsheets/d/1ie-fwNhqzSd5ck2H7FTUtaXWVjsRDXfT1uQosEFWZ0o/edit#gid=0

* The DM is responsible for ensuring any required departmental approval is in place before submitting a request.