DATA MANAGEMENT POLICY

SECTION ONE
Purpose, Scope, and Definitions

1. Short Title
"Arkın University of Creative Arts and Design (ARUCAD) Data Management Policy".

2. Definitions
For the purposes of this Policy Document, the following terms shall have the meanings set out below;

a) University: ARUCAD University,
b) Board of Trustees, Senate, or the relevant Administrative Board: ARUCAD Board of Trustees, ARUCAD Senate, or the relevant ARUCAD Administrative Board,
c) Rector: the Rector of ARUCAD,
d) Data Security: The entirety of administrative, technical, and legal measures aimed at ensuring the protection of the confidentiality, integrity, and availability of data assets,
e) Data Assets: All kinds of data, documents, systems, and infrastructures (databases, software, hardware, printed documents, servers, etc.) that are produced, processed, stored, or transmitted within the scope of institutional activities,
f) Confidentiality: The accessibility of data only by authorized persons, systems, or processes,
g) Integrity: The protection of the accuracy and completeness of data against unauthorized alterations,
h) Availability: The ability of authorized users to access data and information systems when needed,
i) Personal Data: All kinds of information relating to an identified or identifiable natural person,
j) Access Authorization: The authorization determining the level at which a user may access data assets,
k) Incident Response: The technical and administrative activities carried out to reduce the impact of data security incidents and to prevent their recurrence,
l) PDCA Cycle (Plan-Do-Check-Act): The quality management model based on the planning, implementation, monitoring of institutional activities and their improvement according to the results obtained.

3. Purpose
The purpose of this policy is to protect the confidentiality, integrity, and availability of the data assets owned by the university, to manage data security risks, and to establish and maintain an institutional data security culture.

4. Scope
This policy covers academic and administrative units, employees, students, graduates, and authorized third parties, and all data assets in physical, digital, and electronic environments.

SECTION TWO
Fundamental Principles and Data Security Management

5. Fundamental Principles

Our University ensures data security in line with the following principles:

(a) Confidentiality: Preventing unauthorized access to data
(b) Integrity: Protecting the accuracy and consistency of data
(c) Availability: Ensuring that authorized users can access data when needed
(d) Legal Compliance: Acting in compliance with national and international legislation (BTHK, KVKK, etc.)
(e) Risk-Based Approach: Identifying data security risks and taking preventive and corrective measures
(f) Continuous Improvement: Regularly reviewing and improving data security practices
(g) Management Commitment: Senior management commits to allocating resources to the data security system and ensuring its effective implementation.

6. Resource Planning and Management

(1) The administrative, technical, and institutional resources required for the execution of data security processes are determined and their continuity is ensured.
(2) A sufficient number of competent personnel are assigned for data security management system activities.
(3) Necessary hardware, software, and technological infrastructure investments are planned and kept up to date in order to ensure the security of data systems.
(4) The financial resources required for activities aimed at reducing data security risks are included in institutional budget planning.
(5) Resources are allocated for training and awareness programs in order to improve the knowledge and skills of personnel regarding data management.
(6) The continuity, maintenance, and update requirements of the tools and systems used in data management processes are regularly planned. Data security risks are regularly analyzed and monitored.
(7) Data management responsibilities are determined through authority and duty definitions.

7. Data Management Objectives

(1) Ensuring the continuity of data systems,
(2) Increasing awareness,
(3) Ensuring compliance with legal and contractual requirements,
(4) Keeping technical security controls continuously up to date.

8. Protection of Data Assets

(1) Data assets are classified and appropriate security levels are determined.
(2) Access to physical and digital data assets is provided based on authorization principles.
(3) Necessary technical and administrative measures are taken against data loss, unauthorized access, and cyber threats.

9. Protection of Personal Data

(1) Personal data are processed and protected in accordance with the relevant legislation.
(2) Confidentiality and security are taken as a basis in data processing processes.
(3) Measures are implemented against unauthorized data sharing and breaches.
(4) Risk levels are determined and control measures are defined.

10. Data Security Awareness

(1) Trainings are organized to increase the data security awareness of academic and administrative personnel and students.

(2) Notification mechanisms regarding data security violations are established.

11. Incident Management and Breaches

(1) Data security breaches are recorded and analyzed.

(2) Rapid response and corrective actions are implemented against breaches.

(3) Relevant authorities and stakeholders are informed when necessary.

(4) All users are obliged to comply with the acceptable use rules of data systems.

12. Monitoring, Audit, and Continuous Improvement

(1) Data security practices are regularly monitored and audited.

(2) Improvement measures are taken in line with audit results.

(3) Processes are continuously improved within the framework of the **PDCA cycle.**

SECTION THREE
Other Provisions

13. Cases Not Covered in the Principles

In cases where there is no provision in this policy; the relevant other legislative provisions of ARUCAD and the decisions of the Board of Trustees, Senate, or the relevant Administrative Board shall apply.

14. Entry into Force

These policies shall enter into force as of the date they are adopted by the Senate of Arkin University of Creative Arts and Design.

15. Authority to Execute

The provisions of these policies shall be executed by the Rector of Arkin University of Creative Arts and Design.