Kingdom of Saudi Arabia
Ministry of Education
University of Tabuk
Data Governance Unit

المملكة العربية السعودية
وزارة التعليم
جامعة تبوك
وحدة حوكمة البيانات

Tabuk University Policy in Electronic Systems Management

V.1.0

Document Details

Document Title	Tabuk University Policy in Electronic Systems Management
Institution	Tabuk University – Data Governance Unit
Document Owner	Data Governance Unit
Version Number:	1.0
Status	Issued
Date of issue	31/07/2024
Document Classification	Internal

Document Accrediting Table

Approved by	Reviewing	Editing	Amendments	Date	*Issuance*
Dr.Mohammed Mutaib Alotaibi Data Governance Unit Supervisor	Dr.Hussien Alozaizi Legal Officer	Mr.Abdullah Atwui Data Governance Unit Director	None	31\7\2024	1.0

Approvals

Name	Job	Date	Signature
Dr.Mohammed Alotaibi	Data Governance Unit Supervisor	**30\8\2023**	
Standing Exceutive Committee for University data manangement and governance			

2 Definitions

The Term	University Staff
All who belong to Tabuk University, including employees, faculty members, administrators, and technicians, whether they are permanent or temporary, full-time or part-time, or contracted as external support contractors.	Data
A collection of facts in their primal form or in an unorganized form, such as numbers, letters, still images, videos, audio recordings, emojis, organizational and procedural pieces of evidence, documents, or manuscripts.	Protected Data
Data classified as (highly confidential, confidential, restricted)	Electronic System Manager
Every individual authorized to manage the electronic systems at Tabuk University is responsible for granting users access to the university's systems in accordance with the user group classification document .	Data owner (Data Steward)
As the original owner of the data, it is the university - a public and controlling entity - and (or) the administration or deanship (processing entity) for which an electronic system was built and developed to meet its needs according to work requirements.	Internal Electronic System User
An employee or contractor at the university who is granted access to data in one of the systems, based on the classification in the user groups document.	External electronic system user
A person from outside the university who is granted access to data in one of the systems according to the classification in the user groups document.	Stakeholders
All beneficiaries of the services provided through the electronic systems at Tabuk University	

3 Introduction

This document outlines (represents) the electronic systems management policy at Tabuk University, hereafter referred to as "the University." It includes main sections such as terms and definitions, an introduction, purpose, scope, roles and responsibilities, policy provisions, references, and appendices.

All users and beneficiaries of this document are required to read it carefully, understand its contents thoroughly, and comply fully with the electronic systems management policy at Tabuk University. The ownership of this document lies with the university's Data Governance Unit (The University Data Governance Unit is the owner representative of this document.).

This document is valid for three years from the date of issuance. The Data Governance Unit will review and update it as necessary in response to changes in related systems, regulations, and policies. Each time an amendment is made, whether substantial or minor, the document's issue number will be updated accordingly (The document issue number will be changed if any amendment is made, whether substantial or minor.). All updates or amendments must be approved by the Data Governance Unit.

4 Purpose

This policy aims to govern electronic systems within the university, unify efforts, and achieve the highest standards of compliance among internal and external university entities to prevent conflicts in data processing and storage, and to regulate the disclosure of information to beneficiaries, employees, officials, and stakeholders and their access to it in all its forms from the university's electronic systems for administrative, organizational, and service reasons.

5 Scope

1 This policy applies to all officials, employees, and contractors as required by work needs, granting them the authority to use the university's electronic systems and access associated data, regardless of classification, in accordance with university controls. This includes electronic records, emails, stored information, audio or video files, maps, photographs, manuscripts, handwritten documents, or any other information recorded, processed, or produced by the university electronic systems.

6 Policy Provisions

1. Key principles of data sharing

6.1.1 Principle 1: Promoting a culture of sharing

1. All entities within the university must share the key data they produce in order to achieve integration between entities, realise the principle of obtaining data from its correct sources, and limit duplication, conflict and multiple sources and outdated data.

2. If data is requested from a source other than its primary source, the department requested to share this data must forward the request to the Data Governance Unit.

3. No entity that does not have data authority is entitled to share it with any other entity, internally or externally.

4. No member of the university staff is entitled to share data unless authorised to do so, except in cases where the data is classified as ‘public’.

6.1.2 Principle 2: Legitimacy of purpose

This policy for managing electronic systems at Tabuk University is based on the relevant systems, legislation, and regulatory and executive regulations enacted for this purpose, and full compliance with them. It is the sharing of data for legitimate purposes based on a systematic basis or a justified practical need aimed at achieving the public interest without causing any harm to national interests, the activities of entities, or the privacy of individuals and all activities of the university.

6.1.3 Principle 3: Authorised access

All parties involved in the exchange and sharing of data shall have the authority to view, access and use the data, in addition to the knowledge and skills of qualified and trained personnel on how to handle shared data.

6.1.4 Principle 4: Transparency

All parties involved in data exchange and sharing must make available all information necessary for data exchange, including: the data required, the purpose for which it is collected, the means of its transmission, the methods of its storage, the controls used to protect it, and the mechanism for its disposal.

6.1.5 Principle 5: Shared responsibility

All parties involved in data exchange and sharing shall be fully responsible for decisions regarding data sharing and processing in accordance with legitimate, systematic, and specified purposes. They shall ensure the application of cybersecurity and data exchange security controls stipulated in the data sharing agreement and relevant regulations, legislation, and policies.

6.1.6 Principle 6: Data security

All parties involved in data exchange and sharing are committed to applying cybersecurity security controls to protect data and share it in a secure and reliable environment in accordance with relevant regulations and legislation and in accordance with the provisions of Tabuk University's cybersecurity management regulations and policies.

6.1.7 Principle 7: Ethical Use

All parties involved in data exchange and sharing are committed to applying ethical practices during data sharing to ensure that data is used in a fair, honest, and respectful manner, and not merely complying with cybersecurity management policies or relevant regulatory and legislative requirements.

7 Roles and responsibilities within and outside Tabuk University, and access to and use of the university electronic systems

7.1 Data Steward

The university (a public and governing body) is the owner of the data.

It is the processing entity that is committed to implementing regulations and tasks and represents the highest authority in the entity. It is the primary responsible party and official representative of the entity, and its tasks include the following:

[1]. Ensure the accuracy and integrity of the data (data quality) contained in the system and work to improve data quality in accordance with the data quality manual approved by the Data Governance Unit.

[2]. Comply with Tabuk University's policies on personal data protection and data sharing in accordance with the Personal Data Protection System Manual and Tabuk University's Data Sharing Policy Manual, available on the Data Governance Unit page.

[3]. Granting access permission to the system:

A. Granting access permission to users and beneficiaries according to the powers granted to them in the document classifying groups of users and beneficiaries of the system after submitting an access permission request according to the form prepared for that purpose.

B. The period of time granted for access to the system is limited to a maximum of one academic year.

C. Assessing data access privileges is one of the tasks of the electronic system administrator in accordance with this document.

[4]. Follow-up and review

1. Follow up on the entity's compliance with the personal data policies and governance at Tabuk University.

2. Periodically review system users and update their data and access permissions on a regular basis, and provide the data governance unit with the necessary reports on this.

[5]. Monitoring:

1. Monitoring activities carried out on the system by observing and recording them, including activities related to the person accessing this data.

2. Notify the Data Governance Unit in the event of suspicious activities and violations by system users or misuse of system data.

[6]. Suspension of access to the system:

1. The system administrator or his delegate must close user accounts after the expiry of the period of access to the data and notify them thereof.

2. In the event that the assignment and authority of a representative of one of the university's entities in the electronic system expires, their account must be suspended after notifying the entity of the expiry of their representative's access to the system and informing them of the need to renew or assign a new representative.

3. In the event that a violation or suspicious transgression is detected and recorded by one of the users or beneficiaries before the expiry of their access privileges to the university's systems, the system administrator must suspend their access to the data.

4. In the event of suspension of access permission for the violator, the data governance unit must be notified to take the necessary action.

7.2 Internal system users

The following procedures shall be followed:

1. Submit a formal request using the form provided to add a user to the system.

2. The beneficiary must submit its representatives to the system using the forms provided to the Data Governance Unit.

3. Comply with the Tabuk University Personal Data Protection System and all relevant policies and regulations.

4. The user is required to follow the procedures outlined in Appendix (A) through the Data Governance Unit.

7.3 External system users

The following procedures shall be followed:

1. Submit a formal request using the form provided to add a user to the system.

2. The beneficiary shall submit its candidates representing it on the system using the forms prepared for this purpose to the Data Governance Unit.

3. Comply with the personal data protection system at Tabuk University and all relevant policies and regulations.

4. The user shall comply with the procedures outlined in Appendix (A) through the Data Governance Unit.

8.1 General Administration of Information Technology (IT)

The following tasks and responsibilities:

1-Providing technical support and assistance to entities that benefit from and implement university policies and systems.

2-Providing software and tools that help grant powers to entities within the university, including artificial intelligence systems and programs

3-Preparing lists of user groups for each electronic system, determining their access privileges, and providing the data owner with a copy of these lists regularly.

4-Adding the powers of the administrators of electronic systems owned by their entities from the date of their appointment as heads of entities, and determining the term of validity of the electronic system administration as the term of administrative appointment.

8.2 Cybersecurity Management

Assumes the following tasks and responsibilities:

Monitoring and ensuring the implementation of Tabuk University's cybersecurity policies on all systems and user behavior, ensuring that data is not leaked and providing the appropriate tools to ensure this, in coordination with the Tabuk University Data.

8.3 Data Governance Unit

It has the following tasks and responsibilities:

1. Overseeing the process of granting access to all university systems and ensuring the implementation of data protection

2. Ensuring the implementation of Tabuk University's data protection policies and the application of related systems and regulations

3. Receiving notifications of violations of the personal data protection system or misuse of personal data from system administrators and dealing with them according to the system.

9- Authority Matrix

	Entity / Task	Electronic System Manager	General Administration of Information Technology	Cybersecurity Administration	Data Governance Unit	Beneficiaries(Internal/ External)	Internal System Users	External System Users
1	Ensure the accuracy and integrity of the	√						

	data within the system (data quality) and work to improve data quality according to the Data Quality Manual approved by the Data Governance Unit.							
2	Grant access to the system:							
2.1	Grant access permission to users and beneficiaries according to the powers granted to them in the document, classifying user and beneficiary groups for the system after submitting an access permission request using the form prepared for this purpose.	√						
2.2	Assessing data access privileges before granting access permission	√						
3	Follow-up and Review:							

3.1	Periodic review of system users, updating their data and access permissions periodically, and providing the Data Governance Unit with the necessary report regarding this.	√						
4	Monitoring:							
4.1	Monitoring activities carried out on the system by observing and recording them, including activities related to the person accessing this data.	√		√				
4.2	Notifying the Data Governance Unit in case of suspicious activities, violations by system users, or misuse of system data.	√		√				
5	Suspension of access to the system							
5.1	Closing user accounts after the expiration of the period of access to the	√						

	data and notify them accordingly.							
5.2	In case the assignment or authority of a representative of a University entity in the electronic system ends, their account must be suspended after notifying the entity of the expiration of the representative's access authority to the system, and notifying them to request renewal or appoint a new representative.	√						
5.3	Suspending data access permission in the event of monitoring and recording a violation or suspicious transgression by a user or beneficiary before the expiration of their access authorities to the university's systems.	√						

5.4	In case of suspending access permission for the violator, the Data Governance Unit must be notified to take the necessary action.	√						
6	Submitting a formal request using the designated form to add a user to the system.						√	√
7	The beneficiary must submit its representatives to the system using the designated forms to the Data Governance Unit					√		
8	Compliance with the University of Tabuk's Personal Data Protection System and all related policies and regulations.	√	√	√	√	√	√	√
9	Providing technical support and assistance to the beneficiary entities and		√					

	those implementing the university's system policies.								
10	Providing software and supporting tools that assist in granting authorities to entities within the university, including AI systems and programs.		√						
11	Preparing lists of user groups for each electronic system, determining the nature of their authorized access permissions, and providing the data owner with a copy of these lists periodically.		√						
12	Add the powers of the administrators of the electronic systems owned by their entities from the date of their appointment as heads of		√						

	those entities, and determine the term of validity of the electronic system administration as the term of the administrative appointment							
13	Follow-up and verification of the application of the University of Tabuk's cybersecurity policies on all systems and user behavior, ensuring no data leakage, and providing appropriate tools to ensure this, in coordination with the University of Tabuk's Data Governance Unit.	√	√	√	√	√	√	√
14	Supervising the workflow of access permission granting for all university systems and ensuring data protection is applied.			√				
15	Receiving notifications of				√			

	violations of the Personal Data Protection System or misuse of data from system managers and dealing with them according to the regulations.							

10. References

1 .Saudi Data and Artificial Intelligence Authority (SDAIA)1

2 . National Data Governance Unit (MDMO)