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

المملكة العربية السعودية
وزارة التعليم
جامعة تبوك
وحدة حوكمة البيانات

University of Tabuk Data Privacy Policy

V.1.0

Document Details

Document Title	**University of Tabuk Data Privacy Policy**
Institution	**University of Tabuk**
Document Owner	**Data Governance Unit**
Version Number	**1.0**
Status	**Issued**
Version Date	**10/10/2024 AD**
Document Classification	**Public**

Document Approval Table

Release	History	Modifications	Release	Review	Approval
1.0	10/10/2024 ad	**None**	**Dr. Haifa Eid Abu Shuail Personal data protection officer**	**Dr. Hussein Al-Azizi Legal officer**	**Dr. Mohamme Mutaib Al-Otaibi Supervisor of the data governance unit**

Name:	Position	Date	Signature
Dr. **Mohammed Mutaib Al-Otaibi**	**Supervisor of the data governance unit**		
Standing executive committee for data management and governance at the University			

Table of Contents ……..……..……1

1. Introduction

This document outlines (represents) the data protection policy of Tabuk University, which will be referred to as the University in this document.

The document is organized into nine main sections: this introduction, purpose, scope, roles and responsibilities, policy provisions, references, compliance, exception criteria, and terms and definitions.

All users must carefully read, fully understand, and strictly follow the University of Tabuk Data Protection Policy. If any part of this document is unclear, please don't hesitate to contact the University Data Governance Unit for assistance.

The Data Governance Unit is the sole owner of this document.

This document remains valid for three years from the date of its issuance. The Data Governance Unit is responsible for reviewing and updating it at least annually or promptly after any legislative or regulatory changes. Any amendments, whether large or small, will result in a new version number, which the University Standing Committee must approve for Data Governance and Management purposes.

2. Purpose

The purpose of this policy is to establish data protection requirements for University Tabuk data, thereby reducing risks from internal and external threats. It aims to achieve the main protection objectives of information confidentiality, information systems integrity, and availability. This policy aligns with the controls and standards issued by the National Cybersecurity Authority and relevant regulatory and legislative requirements.

3. Scope

This document governs all information and technology assets and services, as well as all users, including both permanent and temporary employees, full-time and part-time staff, and contractors, such as employees of outsourcing firms. It also covers users and employees from third-party entities, such as contractors, suppliers, consulting firms, government agencies, managed service providers, hosting and cloud companies, and other relevant organisations.

4. Roles and Responsibilities

1- Policy approval: Permanent Committee for Data Management and Governance

2- Policy review and update managed by the Data Governance Unit.

3- Policy implementation and enforcement: General Administration of Information Technology, Cybersecurity Department, and Data Governance Unit.

4- Policy Compliance Measurement: Data Governance Unit.

5. Terms of Policy

1. General Terms

1.1. The University must comply with legislative and regulatory requirements. The University is obligated to comply with the data protection laws and regulations of the Kingdom of Saudi Arabia, as well as the policies and procedures established at the University of Tabuk.

1.2. The University must regularly review and update its data cybersecurity requirements.

1.3. The University must ensure proper management of data cybersecurity requirements, aligning with the Human Resources Cybersecurity Policy and the University of Tabuk Asset Management Policy.

1.4. The University must ensure that mobile devices are protected in accordance with the mobile device security policy.

1.5. The University should implement data leak (theft) prevention technologies and solutions.

1.6. It is prohibited to use University data outside the production environment unless a risk assessment is conducted and controls, such as data masking or scrambling techniques, are implemented to safeguard that data.

1.7. The University must determine the techniques, tools and procedures for securely destroying data according to the classification level.

1.8. The University must develop and implement a clear cloud services exit strategy to ensure the secure destruction of data when the contract with the cloud service provider ends or expires.

1.9. The University shall ensure the appropriate and effective use of encryption technologies to protect its data in accordance with the University of Tabuk encryption policy and standards and relevant legislative and regulatory requirements.

1.10. The University must establish roles and responsibilities for cybersecurity to ensure that data complies with legal and regulatory requirements.

1-11 The university must use a secure method for extracting, transferring data, extracting and transferring virtual infrastructure.

1-12 The university must prevent the transfer of any sensitive systems data from the production environment to any other environment.

1-13 The university must use a watermark feature to encrypt the entire document when it is prepared, stored, printed, or displayed on screen, and ensure that each copy of the document contains a traceable number.

1-14 Key performance indicators (KPIs) must be measured to ensure continuous improvement of cybersecurity requirements for data protection.

2- Classification and Secure Information Handling (handling of information)

2-1 University data must be classified in accordance with the approved origin classification and encryption policy at Tabuk University.

2-2 All university data must be classified in all of the following formats:

2-2-1 Digital formats (e.g., word documents, spreadsheets, and databases).

2-2-1 Digital formats (e.g., word documents, spreadsheets, and databases).

2-2-2 Electronic communications (such as emails, voice communications, conference calls, telephone calls, etc.)

2-2-3 Physical forms (such as printed materials, paper copies of contracts, and notebooks).

2-2-4 Oral conversations (such as meetings and interviews).

2-3 employees should refrain from discussing Tabuk University data verbally in public areas or anywhere they might be overheard. Such discussions should be held on Tabuk University campuses and in secure locations within the campuses.

All data stored by the University of Tabuk across all systems, including sensitive and cloud computing systems, must be classified and encrypted in accordance with relevant legislative and regulatory requirements and the University of Tabuk's classification and encryption policy.

2-5 Data custodians, appointed by the University of Tabuk to collaborate with relevant parties involved with the University of Tabuk, must be responsible for classifying and encrypting origins as set forth in this policy.

2-6 Any violation of this policy and data classification controls must be immediately reported to the data governance unit at Tabuk University through the designated electronic system.

2-7 Remote access controls for data must be implemented in accordance with the approved remote work policy model at Tabuk University.

2-8 Classified data (confidential, top secret) must not be stored on portable storage devices such as external hard drives or USB drives, regardless of the level of encryption used on the portable storage device.

2-9 Classified data (confidential, top secret) must not be entered, processed, altered, stored, or transferred to devices owned by employees (known as bring your own device (BYOD)), unless the data is employee’ specific.

2-10 Classified data (confidential, top secret) that can be accessed, processed, stored, or transferred through remote access systems must be protected, unless the data is employee’ specific.

2-11 The subsets of classified data (e.g., confidential, top secret) that may be accessed, processed, stored, or transferred through remote work systems, must be identified in accordance with relevant regulatory requirements.

2-12 The technical origins used to manage Tabuk University's social media accounts, must not contain classified data, in accordance with relevant regulatory requirements.

3- Record Retention

3-1 Tabuk University must keep approved records provided by data owners and must maintain records of withdrawal or revocation of consents for a specified period of time in accordance with legislative and regulatory requirements.

3-2 Tabuk University must maintain a record of all secure data destruction processes implemented.

3-3 Tabuk University must keep data for the period specified in accordance with legislative and regulatory requirements, or when sensitive data is no longer required for the purpose for which it was collected.

3-4 Tabuk University must create and update a record of processing activities, keeping copies for the designated period in accordance with legislative and regulatory requirements.

3-5 The retention period for all systems-related data must be determined in accordance with relevant legislation, and only data required for production must be retained.

6. Update and Review

The cybersecurity department must review the policy at least annually, or whenever changes occur to Tabuk University's organizational policies or procedures, or relevant legislative and regulatory requirements.

7. Policy Commitment

1- The cybersecurity department must periodically ensure that Tabuk University commits to this policy.

2- All employees at Tabuk University must commit to this policy.

3- Any violation of this policy may subject the violator to disciplinary punishment in accordance with Tabuk University procedures.