Assets Classification and Coding Policy

V1.1

Document Details

Document Name	Asset Classification and Coding Policy
Document Classification	For Internal Use
Last Issue Number	1.1
Type of Document	Update
Document Owner	Cyber Security Department
Document Reference	ISO/IEC 27001:2013 NCA ECC-1:2018

Table of Amendments to the Document

Description of the Change	Prepared by	Issuance Number	Date
Document Preparation	Cyber Security Department	1.0	02-September-2021
Document Update	Cyber Security Department	1.1	13-March-2022

Document Review Schedule

Next Revision Date	Signature	Date	Reviewer/ Conducted by
March 2022		10/10/2021	Director of Cybersecurity Department, Eng. Khalid Ibrahim Al-Fifi.
March 2023		26/5/2022	Deputy Director of Cyber Security Department, Samer Mohammed Ahmed Al-Duwaymer.

Document Accreditation Schedule

Accredited by	Date	Signature	Next Revision Date
Tabuk University President	11/10/2021		March 2022
Tabuk University President	29/5/2022		

Table of contents

Contents

1. Introduction

This document represents the Asset Classification and Coding Policy of the University of Tabuk, referred to as “the University” within this document.

This document consists of nine main sections **including** this introduction, which is followed by the Purpose, Scope, Roles and Responsibilities, Policy Items, References, Commitment, Criteria for Exceptions, and finally Terms and Definitions.

All users should carefully read, **fully understand** and comply with the Asset Classification and Coding Policy. If any of the information in this document or any part of it is unclear, please contact the Cybersecurity Department for explanation and clarification.

The University's Cybersecurity Department is the owner of this document.

The validity period of this document is three (3) years from the date of its issuance, and the Cybersecurity Department must review and update this document at least once a year, or it may also be updated immediately after any amendments or changes related to the relevant legislative and regulatory requirements. The **issue** number of the document will be changed in the event of any modification, whether it is **substantive** ~~substantial~~ or secondary. Such updates or amendments should be approved by the Supervisory Committee for Cybersecurity of the University.

2. Purpose

This policy aims to ensure an accurate and detailed record of information and technical assets in order to support the operational cybersecurity requirements of the university so that it can maintain the confidentiality, integrity, and availability of data, information, and information, and technical assets, as well as identify appropriate protection responsibilities in accordance with the policies and procedures of the University and relevant legislative and regulatory requirements.

3. Scope

This document applies to all information and technical assets and services provided and to all data received, produced or dealt with by the entities within the University of Tabuk, regardless of its source, form or nature, including paper records, meetings, communications through communication media and applications, emails, and stored data on electronic media, audio or

video tapes, maps, photographs, manuscripts, handwritten documents, data stored in the university's systems such as the Masar system, the electronic learning management system (Blackboard), the admission and registration system (E-Register), the electronic portal and all university systems and any other form of recorded data, as well as all its employees, whether they work permanently or temporarily, or working full-time or part-time, or contractors as employees of outsourcing companies, as well as users and employees of all external parties such as contractors, suppliers, consulting companies, government agencies, managed services companies, hosting and cloud computing companies, and others.

4. Roles and Responsibilities

Responsible Party	Preparation, Updating and Revision	Accreditation	Publishing	Commitment and Implementation
Cybersecurity Supervisory Committee				
Cyber Security Department				
All University Staff and ~~all~~ Internal/ External Interested Parties				

5. Policy Items

5.1 Classification of Data, Information, Informational and Technical Assets

5.1.1 The Cybersecurity Department must determine the appropriate classification levels for all data, information, **informational**~~information~~ and technical assets during their secure storage, processing, transfer, sharing and disposal.

5.1.2 All users and employees must adhere to the specified **classification** ~~rating~~ levels.

5.1.3 The classification of data, information, informational and technical assets should be reviewed at least once a year or in case of any material changes.

5.1.4 The Cybersecurity Department must determine the classification levels based on the sensitivity, importance, confidentiality, value of data and the degree of their impact, taking into account the balance between their value and the degree of confidentiality of data, information, informational~~information~~ assets, and technology.

5.1.5 All data, information and **informational** ~~information~~ and technical assets should be classified on the basis of the following classification scheme:

- **Highly Confidential: This** applies only to data, information, and informational and technical assets that may include sensitive, extremely valuable, proprietary, or equally personal information, which shall not be disclosed outside or inside the university without the express written permission of the owner of the data and information. If disclosed or accessed, (Remove the comma) by unauthorized persons, it may adversely affect public or private interests, have a negative impact on the social life of individuals and negatively affect the image or reputation of the university or may result in (The sentence ends abruptly here) hacking or accessing it without permission leads to criminal charges and huge legal fines, or causing irreparable damage to the University. These documents, during the period of restriction, can only be accessed by the relevant senior officials, or by courts that have jurisdiction in cases that relate to the interests of national security and to the extent necessary to decide on these issues.
- **Confidential: This** Applies only to data, information, informational and technical assets for which specific permission and/or **authorization** must be obtained and the consent of the owner of the data and information before disclosure to anyone inside or outside the University. A reasonable level of security controls must be applied to the restricted data.
- **Restricted:** This applies only to data, information, informational and technical assets, the disclosure of which may lead to a minor and limited impact on the work and can be shared and communicated internally within the University. The consent of the owner of the data and information must be obtained before disclosure to anyone outside the University in particular,

and the data classified at a restricted level can be classified into sub-levels based on the scope of impact as follows:

- Restricted-level (A): If the scope of the impact is at the level of an entire sector or general economic activity.
- Restricted-level (B): If the scope of the impact is at ~~on~~ the level of activities of several entities or on the interests of a group of individuals.
- Restricted-level (C): If the scope of the impact is at the level of the activities of one entity or the interests of a particular individual.

- Public**:** This applies to data and information that may be widely distributed without causing harm to the university, its employees, and customers. The owner of the data and information of the university must give prior consent to the use of this classification. These documents may be disclosed or passed on to people outside the University. This classification applies to general, unclassified topics that have been circulated and disclosed to anyone. These documents relate to, but are not limited to, laws, regulations, plans, programs, statistics, statistical studies and reports.

5.1.6 The University's Cybersecurity Department should determine the evaluation criteria to help evaluate all information and technical assets at the University according to the levels of Confidentiality, Integrity, ~~safety~~ and Availability (CIA) of relevant information, and if the levels of CIA (Confidentiality, Integrity, and Availability ~~and safety~~) of any assets differ, the highest value of the information and related assets will be taken.

5.1.7 The following table will identify the different levels of Confidentiality, Integrity and Availability (CIA):

Security Goals	**Impact Level**		
	Low	**Moderate**	**High**
Confidentiality			

Safeguard information by maintaining and enforcing authorized restrictions against unauthorized access or disclosure.	The unauthorized disclosure of information that is expected to result in a limited negative effect on the university's institutional processes, assets, users, or personnel.	The unauthorized disclosure of information that is expected to result in serious adverse effects on the university's institutional processes, assets, users, or employees.	The unauthorized disclosure of information that is expected to cause serious or catastrophic damage to the university's institutional processes, assets, users, or employees.
Integrity Safeguard the integrity of information by preventing unauthorized or improper alteration or destruction, ensuring accuracy, and enforcing non-repudiation.	The unauthorized alteration or destruction of information that is expected to result in a limited negative effect on the university's institutional processes, assets, users, or employees.	Unauthorized alteration or destruction of information that is expected to result in serious adverse effects on the university's institutional processes, assets, users, and employees	Unauthorized alteration or destruction of information that is expected to result in significant or catastrophic adverse effects on the university's institutional processes, assets, users, and employees.
Availability	Disruption or unavailability of information or information systems that is expected to result in a limited negative effect on	Disruption or unavailability of information or information systems that is expected to result in serious adverse effects on	Disruption or unavailability of information or information systems that is expected to result in significant or catastrophic

	the university's institutional processes, assets, users, or employees.	the university's institutional processes, assets, users, or employees.	effects on the university's institutional processes, assets, users, or employees.

Impact indicator:

Key impact area	University's interests
Impact component(Sub-	University's reputation
Considerations	Could the information attract local or international media attention, or otherwise negatively influence public perception of the University?)

Impact Level			
Highly confidential	**Confidential**	**Restricted**	**Public**
High	**Moderate**	**Low**	**No impact**
Significant impact on the university's reputation.	**Moderate impact on the university's reputation.**	**No impact on the university's reputation.**	**No impact**

Key impact area	University's interests
Impact component	University's economical status
Considerations	Does disclosing information lead to financial losses at the university level?

University's functions

Could the disclosure of information impede or limit the university's capacity to perform its daily functions and operations?

Impact level Impact level			
Strictly confidential	**Confidential**	**Restricted**	**` Public**
High **Long-term impact on the economy with an irreversible decline in the gross domestic product, stock market prices, unemployment rate, purchasing power, or other relevant indicators, which negatively affects the university's facilities.**	**Moderate**	**Low**	**No impact**
The university is unable to perform its core functions and operations for a long period.	**The university is unable to perform one or more of its core functions and operation for a short period of time.** **unemployment rate, purchasing power, or other relevant indicators, which negatively affects the one or more sectors. .**	**The university is unable perform one or more of its non-core functions and operations for a short period of time.** **purchasing power, negatively affecting only one sector.**	**No impact.**

Key impact area	
Impact component	
Considerations	

Key impact area	
Impact component	University's functions
Considerations	

University profits

Impact level			
Strictly confidential	**Confidential**	**Restricted**	**Public**
High	**Moderate**	**Low**	**No impact**
The entity incurs substantial financial losses that could lead to bankruptcy.	**A significant adverse impact on the university that could be detrimental to its interests.**	**Limited detriment, reflected in a minor financial loss to the entity or to any of its assets.**	**No impact.**

Could the disclosure of information result in financial losses, potential bankruptcy of the university, increase the risk of fraud, unauthorized fund transfers, or illegal confiscation of assets?

Key impact area	University's activities
Impact component	University functions
Considerations	Could the disclosure of information cause detriment to the University? Could it result in the loss of the University's leading position or any of its assets? Could it result in the termination of personnel or otherwise constrain the University's competitiveness in its sector?

Impact level			
Strictly confidential	Confidential	Restricted	Public
High	Moderate	Low	No impact
Significant adverse effect on private entities that results in harm to the national vital interests.	The entity cannot fulfill its core functions and experiences a significant loss of competitive ability.	The entity cannot fulfill a core function and experiences a limited loss of competitive ability..	No impact on the activities of the entities

Key impact area	Personnel
Impact component	Personnel Health / safety.
Considerations	Could the disclosure of this information result in the exposure of personnel names, locations, or other personal information?

Impact level			
Strictly confidential	**Confidential**	**Restricted**	**Public**
High	**Moderate**	**Low**	**No impact**

Significant loss of personnel lives, impacting one or a group of individuals.	**Critical or life-threatening injury**	**Minor, non-life-threatening injury**	**No impact on personnel.**

Key impact area	Personnel
Impact component	Privacy
Considerations	Could the disclosure of this information violate the privacy of personnel at the University of Tabuk?

Impact level			
Strictly confidential	Confidential	Restricted	Public
High	Moderate	Low	No impact
Disclosure of personal information of key personnel at the University of Tabuk.	Disclosure of personal information of key personnel at the University of Tabuk.	Disclosure of personal information of personnel at the University of Tabuk.	No impact on personnel at the University of Tabuk.

Key impact area	Personnel
Impact component	Personnel Health / safety.
Considerations	Will this infringe any intellectual property rights of Tabuk University?

Impact level			
Strictly confidential	Confidential	Restricted	Public
High	Moderate	Low	No impact
Affects the national interest			

Key impact area	Environment.
Impact component	Environmental resources
Considerations	Could the disclosed information be exploited to develop products or services that could destroy natural or environmental resources?

Impact level			
Strictly confidential	Confidential	Restricted	Public
High	Moderate	Low	No impact
Permanent, catastrophic impact on environmental or natural resources.	Long-term impact on environmental or natural resources.	Short-term or limited impact on environmental or natural resources.	No impact on environmental or natural resources.

5.1.8 If any data or information with different classifications is collected, the most restrictive classification should be applied to all the data.

5.1.9 By default, all university data that has not been clearly classified should be treated as confidential data.

5.1.10 For all new and current data, information, and informational and technical assets, the owner is responsible for selecting the appropriate classification to be used by all asset sponsors, users, and employees who create, compile, or modify operational information.

5.1.11 Any writable and modifiable storage media, such as floppy disks, magnetic tapes, CDs, DVDs, hard drives, and portable storage devices containing any confidential data or applications, must be reclassified at a confidential level.

5.1.12 When recording information with a higher classification on any storage media, and also in the case of transferring it to lower classified media, the lower classified media must be upgraded to reflect the highest classification level of the stored data and information.

5.1.13 The owner of data, information, and information and technical assets may raise or lower the applied classification by changing the classification label and notifying all employees, asset sponsors, and relevant users, and so on.

5.1.14 The principle for data is to be available (in the field of development) unless its nature or sensitivity requires higher levels of classification and protection, and highly confidential (in the political and security field) unless its nature or sensitivity requires lower levels of classification and protection.

5.1.15 Data is classified upon its creation or when received from other entities, and the classification occurs within a specified time period.

5.1.16 The separation of tasks and responsibilities of employees at the University of Tabuk - regarding the classification of data, access to it, disclosure of it, use of it, modification of it, or destruction of it - is done in a manner that prevents overlapping of jurisdictions and avoids dispersing responsibility.

5.1.17 Access to data and its use are restricted based on the actual need for knowledge and to the minimum number of employees possible at the University of Tabuk.

5.1.18 The management of employee permissions at the University of Tabuk is restricted to the minimum privileges necessary to perform their assigned tasks and responsibilities.

5.1.19 The data that has not been classified at the time of issuing this policy must be classified within a specified timeframe according to a work plan prepared by the University of Tabuk and approved by the university's top official.

[ISO/IEC 27001:2013, A.8.2.1]

5.2 Encoding of data, information, and information and technical assets

5.2.1 The coding process must be in accordance with the recognized and approved labeling within the university, and the coding process must align with the classification scheme for informational and technical assets.

5.2.2 All printed documents containing data and information classified as "confidential" or "highly confidential" must be stored in locked drawers or cabinets when the employee is not present in the office. Additionally, any office containing confidential or highly confidential documents must be locked.

5.2.3 Labels must be placed on documents, devices, and removable media after determining the appropriate classifications according to the university's asset classification and coding policy.

5.2.4 Media containing information classified as "Highly Confidential" shall not be delivered to any external entity or third party unless authorized and approved by the administration after providing logical justifications for such action.

5.2.5 Confidential information that is not encrypted must not be sent through any external party, including but not limited to courier companies, postal services, and internet service providers. This is to ensure that confidential information does not fall into the hands of any unauthorized parties.

5.2.6 It is prohibited to make additional copies or print additional copies of highly confidential information without obtaining prior approval from the data and information owners.

5.2.7 In the case of making additional copies of highly confidential information, the number of additional copies and the recipients of these copies must be recorded in a log, and all employees or entities receiving these copies must be notified that no additional distribution or copying **shall** occur without the approval of the data and information owner.

5.2.8 Authorized personnel must be present to inspect the printed information in the case of printing "Highly Confidential" information, if physical access controls are not used to prevent unauthorized persons from entering the area surrounding the printer.
[ISO/IEC 27001:2013, A.8.2.2]

5.3 Handling data, information, and information technology assets

5.3.1 Data, information, and technological asset processing methods must be developed and applied to protect them from unauthorized disclosure or misuse. The methods and procedures for processing data and information, as well as the specified protection controls, must be in accordance with their classification.
5.3.2 The following controls must be considered when handling data and information:
▪ Handling all media and labeling them, in addition to applying text protection marks on paper and electronic documents (including emails) according to each classification level.
▪ Imposing access restrictions to identify any unauthorized individuals so that:
o Access to data – logical and physical – is granted based on the principle of "the minimum privileges and the need to know."
o Access to data must be denied immediately upon the termination or end of professional service of employees at the University of Tabuk.
▪ Keeping an official record of the authorized recipients of the data.
▪ Ensuring the completeness of data entry, the correct processing, and the application of output validation.
▪ Maintaining data distribution to a minimum, especially when related to any confidential data and information.
▪ Review distribution lists and approved recipient lists at least once a year.
▪ Classified data is used according to the requirements of classification levels. For example, the use of "Strictly Confidential" classified data is restricted to specific locations, whether physical, such as offices, or virtual, using device encryption or special applications.
▪ Do not leave classified data marked as "Strictly Confidential," "Confidential," and "Restricted," as well as mobile devices that process or store this data, without supervision.

▪ Classification data labeled as "Strictly confidential," "Confidential," and "Restricted" must be protected from unauthorized access during their physical or electronic storage using one of the encryption methods approved by the National Cybersecurity Authority.

[ISO/IEC 27001:2013, A.8.2.3]

5.4 Declassification (Lifting the Secrecy)

The classification of data must be canceled or its classification level reduced to the appropriate extent after the classification period ends when protection is no longer required or no longer needed at the original classification level.

In case the data is classified incorrectly, the data user must notify the data representative to determine the need for reclassifying it appropriately.

5.4.1 Factors that help in the declassification of data should be determined when setting classification levels for the first time, and they should be recorded in the data asset register. These factors may include the following:

● A specific time period after the creation or receipt of the data, for example: two years after creation.

● A specific time period after the last action on the data, for example: six months from the last use date.

● After the expiration of a specified date, for example, when it is scheduled to be reviewed on January 1, 2024.

● After certain circumstances or events that have a direct impact on the data, for example: events that change strategic priorities or changes in government agency personnel.

● Canceling classification - lifting secrecy - or reducing classification levels requires, aside from the factors that clearly assist in canceling classification, a sound understanding of the content of the classified statements and the context in which they were issued.

[SDAIA, 2021]

5.4 Steps Required for Data Classification

Step 1 – Identifying All Entity Data

The first step taken by the University of Tabuk is to inventory and identify all data owned by the university in accordance with the Data Classification Model (Model A) and the Document Classification Model (Model B). (The models are attached in the annexes).

Step 2 – Assigning a Data Classification Officer

Each entity within the university must establish an internal committee or appoint an individual responsible for the classification process, including identifying all data and documents within the entity. The entity must assume responsibility for conducting the initial classification.

Step 3 – Conducting an Impact Assessment

1. The entity must follow the required steps for the impact assessment process using Model A, which involves assessing the consequences of:

- • Disclosure of data or unauthorized access to it
- • Alteration, destruction, or both, or unavailability of data in a timely manner

2. The impact assessment process begins with the principle of “data availability as the default” (in the developmental context), unless the nature or sensitivity of the data requires higher levels of classification and protection (e.g., “Highly Confidential”). In political and security contexts, unless the nature or sensitivity of the data requires lower levels of classification.

Step 3A – Identifying the Impact Category

The first element of impact assessment involves determining the main and sub-category of potential impact within the following main categories:

- • University interests
- • University entity activities
- • Health or safety of university staff and members
- • Environmental resources

Step 3B – Determining the Impact Level

1. The second element requires the entity to assign a level to each potential impact based on:

- • Duration of impact and difficulty of controlling the damage
- • Time required to recover and repair damage after occurrence

- • Scope of impact (national, regional, multiple entities, single entity, several individuals, etc.)

2. These criteria define four impact levels:

- • High: Unauthorized access or disclosure causes severe or extremely critical long-term damages that cannot be remedied or repaired.
- • Medium: Unauthorized access or disclosure causes serious or critical damages that are difficult to control.
- • Low: Unauthorized access or disclosure causes limited damages that can be controlled, or short-term intermittent damages that can be managed.
- • No Impact: Unauthorized access or disclosure does not cause any short-term or long-term damage.

3. All potential damages identified during the impact assessment must be specific, evidence-based, and not based solely on subjective judgment.

4. The Business Data Representative determines the data classification level based on identified impacts:

- • High: Classified as “Highly Confidential.”
- • Medium: Classified as “Confidential.”
- • Low: Requires further evaluation (see Steps 4 and 5).
- • No Impact: Classified as “Public.”

5. A detailed description of the main considerations for each impact category and level is provided in Table (2): “Impact Categories and Levels for Data Classification.”

6. Steps 4 and 5 must be considered when the identified impact level is Low.

7. Proceed to Step 6 if the data is classified as “Highly Confidential,” “Confidential,” or “Public.”

Step 4 – Identifying Related Regulations (Only if Impact Level is Low)

1. Additional evaluations are required if the identified impact level is Low, in order to ensure that “Public” data is classified at the maximum appropriate level.

2. The University of Tabuk's Business Data Representative must examine whether disclosure of such data conflicts with the regulations of the Kingdom of Saudi Arabia (e.g., the Anti-Cybercrime Law, the E-Commerce Law, etc.).

- • If disclosure violates applicable regulations, the data must be classified as "Restricted."
- • Otherwise, the Business Data Representative proceeds to Step 5.

Step 5 – Balancing the Benefits of Data Disclosure and Negative Impacts (Only if Step 4 Result is "No")

1. Confirm the low impact level and ensure disclosure does not violate any applicable regulations.

2. Assess the potential benefits of disclosure and determine whether they outweigh the negative impacts. Potential benefits may include:

- • Using data to develop new value-added services
- • Increasing transparency of government processes
- • Enhancing public participation with government entities

3. If the benefits outweigh the negative impacts, the data is classified as "Public."

4. If the benefits are outweighed by the negative impacts, the data is classified as "Restricted."

Step 6 – Reviewing the Classification Level

The Cybersecurity Department must review all classified data to ensure the level assigned by the entity is appropriate.

Step 7 – Applying Appropriate Controls

1. The final step in data classification is to protect all data according to its classification level by implementing the relevant control measures (see "Data Classification Controls").

2. The classification process is complete when all University of Tabuk data has been classified, levels verified, and relevant controls applied.

3. Once data is properly classified, university entities may share it with other entities or make it available as Open Data if classified as "Public."

(SDAIA, 2021)

5.5 Roles and Responsibilities within the University of Tabuk

All university entities must assign internal committees responsible for fulfilling the obligations associated with each role in the data classification process and its protection requirements, as outlined below:

- • Internal Data Governance Committee (per entity): A committee responsible for data collected or retained by the entity at the University of Tabuk. It is recommended that members be experienced. Its tasks include:

1. Data Collection: Inventory all documents and data available within the entity and its departments using Models A and B.

2. Data Classification: Classify data collected by the entity according to Models A and B.

3. Post-Classification Review: Consolidate and review classified data, ensuring that data aggregated from multiple sources within the entity is classified at the highest applicable level used for any individually classified data.

4. Classification Coordination: Ensure data exchanged between departments or entities within the university is consistently classified and protected.

5. Compliance with University Policies: In coordination with the Cybersecurity Department and the Data Governance Unit, ensure that data is protected in accordance with specified controls.

- • Data Classification Reviewer (Cybersecurity Department Representative): A staff member from the Cybersecurity Department who reviews and approves classification levels determined by the entity.
- • Business Data Specialist (Deanship of Information Technology): A specialist from the Cybersecurity Department or the Deanship of Information Technology (or both) responsible for protecting data by applying approved controls defined in the “Data Classification Controls” section. Responsibilities also include maintaining systems, databases, and servers that store data, as well as providing technical support, the responsibilities of the Business Data Specialist consist of:

1. Access control: Ensure that access controls are implemented, monitored, and reviewed in accordance with the data classification levels specified by the business data representative at Tabuk University.

2. Revision reports: Send an annual report to data officials at Tabuk University addressing the availability, integrity, and confidentiality of classified data.

3. Data backup: Perform regular data backups.

4. Data validation: Periodically validate data.

5. Data restore: Restore data from backup media.

6. Monitoring activity: Monitor and record activities performed on data, including data related to the person accessing such data.

7. Compliance with data classification (in conjunction with data controllers): Ensure that Tabuk University data is classified and protected according to the process outlined in this policy and in accordance with the specified controls.

Data user: An employee at Tabuk University who handles, accesses, uses, or updates data for the purpose of performing a task assigned to them by the institution. Users shall use the data in a manner consistent with the specified purpose and comply with this policy and all policies related to data use at Tabuk University. The head of the entity shall assign the person he deems competent to perform these roles.

System Administrator: Any person authorized to manage one of the university's electronic systems, responsible for adding users to the system data as required by the nature of their work.

[SDAIA, 2021]

6- References

- ISO/IEC 27001:2013, A.8.2
- ECC-1:2018, 2-1
- ECC-1:2018, 2-7
- Saudi Data and Artificial Intelligence Authority [SDAIA, 2021]

7- Compliance

- The asset classification and coding policy must comply with the basic cybersecurity controls issued by the National Cybersecurity Authority (ECC:1-2018) and with all requirements of the international ISO standard for information security (ISO/IEC 27001:2013).

- All users, employees and relevant parties must adhere to the asset classification, and coding policy, and all department and division managers must ensure ongoing compliance with its implementation.

- Compliance with the policy should be reviewed periodically by the cybersecurity department, and senior management should take all necessary corrective measures in the event of any violation. The severity of disciplinary measures should be proportionate to the seriousness of the violation or incident, as determined after completing the necessary investigations. **These** measures may include, but are not limited to:

▪ Loss of privileges to access information and technical assets.

▪ The application of appropriate penalties by senior management in accordance with the regulations, instructions, and legislation of the National Cybersecurity Authority, as well as official laws relating to cybercrimes.

8- Exemption Criteria

- This document is intended to address all cybersecurity requirements. Therefore, a formal request must be submitted if an exemption is needed. The request must be submitted to the Cybersecurity Department, clearly stating the reasons for the exemption and the expected benefits of the exception, so that a decision can be made and final approval granted by the Director of Cybersecurity or the Cybersecurity Oversight Committee, unless this conflicts with relevant legislative or regulatory requirements.

- The exemption period shall be for a maximum of one year. However, the exemption request may be re-evaluated and renewed for up to three consecutive years if necessary, and the exemption may not be extended beyond the end of the aforementioned three years.

9- Terms and Definitions

Term	Definition

Cybersecurity	According to the provisions of the National Cybersecurity Authority Regulation, issued by Royal Decree No. (6801) dated (11/2/1439 AH), cybersecurity is the protection of networks, information technology systems, and operational technology systems, including their hardware and software components, the services they provide, and the data they contain, from any intrusion, disruption, modification, access, use, or illegal exploitation. The concept of cybersecurity includes information security, electronic security, digital security, and similar areas.
NCA	National Cybersecurity Authority
ISO	International Organization for Standardization (ISO).
ECC	Core Cybersecurity Controls.
Asset	Anything tangible or intangible that has value to the entity. There are many types of assets; including obvious examples, such as people, machinery, facilities, patents, software, and services. The term can also refer to less obvious items, such as information and characteristics (e.g., the entity's reputation and public image, or skills and knowledge).
The Confidentiality	Maintaining authorized restrictions on access to and disclosure of information, including measures to protect privacy and proprietary information.
Information security	Protection against unauthorized modification or destruction of information, including ensuring non-repudiation and reliability of information.
Availability	Ensuring that information, data, systems, and applications are accessible and usable when needed.
Incident	A security breach in violation of cybersecurity policies, acceptable use policies, practices, controls, or cybersecurity requirements

Verification	Confirming the identity of a user, process, or device, often a prerequisite for allowing access to resources in a system.
User permissions	The ability to determine and verify user rights or licenses to access certain resources, as well as the security of the entity's information and technical assets in general and access controls in particular.
Regulation	A measure for limiting and managing risk.
Risks	Risks affecting the entity's business operations including its vision, mission, management, image, or reputation, or the assets of the entity, individuals, other entities, or the state, due to unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
Weakness	Any weakness in a computer system, its software or applications, a set of procedures, or any other aspect that makes cybersecurity vulnerable to threats.
Attack	Any malicious activity that attempts to illegally access, collect, disrupt, prevent, damage, or destroy information systems or the information itself.
Security Breach	Disclosing or obtaining information by persons not authorized to receive or obtain it, or violating the entity's cybersecurity policy by disclosing, altering, tampering with, or losing something, whether intentionally or unintentionally. A security breach is defined as disclosing, obtaining, leaking, altering, replacing, or using sensitive data without authorization (including encryption keys and other critical cybersecurity standards).
Threat	Any circumstance or event that could adversely affect an entity's operations, including its mission, functions, credibility, or reputation, assets, or personnel by exploiting an information system through unauthorized access to, destruction, disclosure, alteration, or denial of service. It also

	includes the capability of the threat source to successfully exploit a vulnerability in a specific information system. This definition encompasses cyber threats.
Classification of Data and Information	**Assigning** a sensitivity level to data and information, resulting in security controls for each classification level. Sensitivity levels are assigned according to predefined categories where data and information are created, modified, enhanced, stored, or transferred. The classification level is an indicator of the value or importance of the data and information to the entity.
Marking or Labeling	Displaying information in the form of labels (with specific and standardized names and codes) placed on the entity's assets (such as devices, applications, documents, etc.) to indicate information related to classification, ownership, type, and other details relevant to asset management.