تمـــــوّل®
Tamawal®

TAMAWAL

Title: Data Privacy and Protection Policy
Policy Reference: CS-POL-17

Document Author

Division	Job Titel
Cybersecurity	CISO (Acting)

Revision History

Job Titel	Date
Head of CS Committee	31-03- 2024

Document Approval

Version	Job Title	Action	Date	Reason of Update
0.1	CISO (Acting)	Created	Jan 2024	Initial Draft
0.2	Consultant	Reviewed	02-08- 2024	Reviewed
1.0	Head of CS Committee	Approval	05-08-2024	Final Reviewed
2.0	Head of CS Committee	Approval	05-08-2024	Enhancement of version

Document Classification

Classification Level	Restricted

Contents

1. INTRODUCTION

The Cybersecurity Policy aims to ensure that Tamawal information assets are protected in a manner that reduces the risk of unauthorized information disclosure, modification, or destruction, whether accidental or intentional. The policy also aims to ensure continuous resilience from emerging global threats to information security, to protect Tamawal and customer information, and to ensure a safe and secure banking experience for its customers.

2. PURPOSE

The Cybersecurity Department has established this Cybersecurity policy to support the effective management of Cybersecurity / Information Security risks at Tamawal. This policy delivers the minimum-security requirements that Tamawal must comply with

3. SCOPE

All Tamawal users are responsible for complying with the Cybersecurity Policy, standards, and procedures including this policy. All users are mandated to acknowledge this policy as part of Tamawal's code of conduct document. All department heads must ensure continuous compliance monitoring within the organization.

4. COMPLIANCE AND ENFORCEMENT

Compliance with the Cybersecurity Policy defined in this document is mandatory for Tamawal Contaminators, Managed Service Staff, and Third-Party Organizations having access to Tamawal Information Assets. The policy and principles defined in this document shall be enforced by the Cybersecurity Department, in coordination and support from the Tamawal Department.

5. RESPONSIBILITIES

- **Data Controller:** means a person or organization that, alone or jointly with others, determines the purposes and means of the Processing of Personal Information.
- **Data Owner:** Potential or existing customers who share their data with Tamawal.

6. DATA PRIVACY AND PROTECTION

Tamawal respects the privacy of its employees and third parties such as customers, business partners, vendors, service providers, suppliers, former employees, and candidates for employment residing in the Kingdom of Saudi Arabia and recognizes the need for appropriate protection and management of Personal Information including the living and deceased individual. Tamawal is guided by the following principles in Processing Personal Information:

- Notice
- Choice
- Accountability for onward transfer
- Security
- Data integrity and purpose limitation
- Access
- Recourse, Enforcement, and Liability
- The owner of the personal data shall

- Have the right to be informed, which includes informing him/her of the legal or practical justification.

  for collecting his/her data, and the purpose of that, and that his/her data should not be processed later.

in a manner inconsistent with the purpose of its collection or cases other than those stipulated in Article (10) of the Personal Data Protection Law (PDPL).

- Have the right to have access to his/her data available to the Tamawal, including access to their data, and obtaining a copy of it in a clear format and conformity with the content of the records, and free of charge-as determined by the PDPL - without prejudice to the provisions of the credit information system about the financial consideration, and without prejudice as required by Article (Ninth) of the PDPL.
- Have the right to request correction, completion, or updating of his/her data held by the controller.
- The right to request that his data available to the control authority be destroyed without prejudice to the provisions of Article (18) of the PDPL.
- Except for the cases stipulated in the Law, personal data shall not be processed or the purpose of its processing changed without the consent of its data owner.
- The data owner shall provide his/her consent for data processing and Tamawal shall define all the terms and conditions for processing the data of the owner. Where the customer is incompetent to provide consent, the legal consent can be provided by a legal guardian with approval from the data owner.
- In all cases, the owner of personal data shall withdraw the consent as referred to in paragraph (1) of the article in PDPL at any time.
- The processing of personal data is not subject to the, in the following cases:
    - When the processing achieves a real interest in the data subject contact with him is impossible or difficult to achieve.
    - When the processing is under another system or in implementation of a previous agreement to which the owner of the personal data is a party.
    - If the controller is a public entity, and that processing is required for security purposes or to satisfy judicial requirements.
- The consent may not be a condition for the provision of a service or the provision of a benefit unless the service or benefit is related to the processing of personal data for which the consent was issued.
- All the third parties involved in storing the data of the owner in the cloud shall abide by the PDPL and Tamawal shall conduct periodic audits on such third parties to ensure adherence to the provisions and the articles in the PDPL.
- No third party shall subsequently share the personal data of Tamawal's customer. Any violation of this clause shall lead to legal actions against the third party.
- Tamawal shall specify periods of the right to access personal data and restrict access to personal data in the following cases:
- If it is necessary to protect the subject of personal data or others from any harm; According to the provisions specified by the regulations.
- Tamawal shall not enable the owner of personal data to access it when any of the conditions stipulated in Paragraphs (1), (2), (3), (4), (5) and (6) of Article (16) in PDPL are fulfilled.
- The data controller in Tamawal shall only collect personal data directly from its owner, and such data shall only be processed to achieve the purpose for which it was collected. However, the controller may collect personal data directly from someone other than its owner, or process it for a purpose other than the one for which it was collected, in the following cases:
    - If the owner of the personal data agrees to this, by the provisions of the PDPL.
    - If personal data is publicly available or collected from a publicly available source.
    - If compliance with the Tamawal – Data Privacy Policy may harm the subject of personal data or affect his vital interests.
    - If the collection or processing of personal data is necessary to protect the health or safety of the public, or to protect the life or health of a particular individual or individuals.

- If the personal data will not be recorded or stored in a form that makes it possible to identify and know its owner directly or indirectly

- The purpose of collecting personal data must be directly related to the purposes of the controller, and not conflict with any legally established provision.
- The methods and means of collecting personal data shall not conflict with any legally established provision, and be appropriate to the circumstances of the owner, direct, clear secure, and free from methods of deception, misleading, or extortion.
- The content of personal data must be appropriate and limited to the minimum necessary to achieve the purpose of its collection while avoiding including that which leads to the specific knowledge of its owner when the purpose of collection has been achieved.
- If it turns out that the personal data collected is no longer necessary i.e. post full payment of loan or completion of a 10-year data retention period, the Data Controller in Tamawal must stop collecting it and immediately destroy what it previously collected.
- The Data Controller shall adopt the Tamawal - Data Privacy Policy and make it available to the data owners to view as part of the terms and conditions before collecting their data.
- The terms and conditions shall include the purpose of its collection, the content of the personal data to be collected, the method of collection, the means of storing it, how to process it, how to destroy it, the rights of its owner about it, and how to exercise these rights.
- Tamawal shall take adequate means to inform the data owner of the following elements before starting to collect his/her data:
- The legal or practical justification for collecting his data.
- The purpose of collecting the personal data, and whether collecting all or some of it is mandatory or optional, and informing him as well that his data will not be processed later in a manner inconsistent with the purpose of its collection or cases other than those stipulated in Article (10) of the PDPL.
- The entity or entities to which the personal data will be disclosed, its description, and whether the personal data will be transferred, disclosed, or processed outside the Kingdom of Saudi Arabia.
- Possible effects and dangers of not completing the procedure for collecting personal data.
- If the data owner has kept any pre-requisites before processing the personal data.
- The Data Controller may not process personal data without taking adequate steps to verify its accuracy, completeness, timeliness, and relevance to the purpose for which it was collected by the provisions of the PDPL.
- The Data Controller may not disclose personal data except in the following cases:
- If the owner of the personal data agrees to the disclosure by the provisions of the PDPL.
- If the personal data was collected from a publicly available source.
- If Tamawal is requested by Ministries and judicial bodies in the Kingdom of Saudi Arabia to provide the personal data of the data owner.
- If the disclosure is necessary to protect public health or safety or to protect the life or health of an individual or individuals.
- If the disclosure will be limited to its subsequent processing in a way that does not lead to the identification of the owner of the personal data or any other individual in particular.
- It poses a threat to security, harms the reputation of the Kingdom, or conflicts with its interests.
- It affects the kingdom's relations with other countries.
- It prevents the detection of a crime, affects the rights of an accused to a fair trial, or affects the integrity of existing criminal proceedings.
- It endangers the safety of an individual or individuals.
- It entails violating the privacy of an individual other than the owner of personal data as determined by the regulations.

- It is incompatible with an incompetent or incompetent interest.
- It breaches legally established professional obligations.
- It discloses a confidential source of information that the public interest should not disclose.
- If an error is corrected, a deficiency is completed, or an update is made in the personal data, the control authority must notify any other party to which such data has been transferred and provide it with such modification.
- Incorrect processing of personal data shall be notified within 12 hours of incorrect processing of the personal data of the data owner.
- The Data Controller in Tamawal shall retain the personal data of the customer personal data 10 years from the data personal data collection.
- The controller shall keep the personal data even after the purpose of its collection has ended in the following two cases:
- If there is a legal justification that requires keeping it for a specific period, and in this case, it shall be destroyed after the expiry of this period or the purpose of its collection, whichever is longer.
- If the personal data is closely related to a case under consideration before a judicial authority and its retention is required for this purpose, and in this case, it shall be destroyed after completing the judicial procedures related to the case.
- The Data controller shall take the necessary organizational, administrative, and technical measures and means to ensure the preservation of personal data, including when it is transferred; This is by the provisions and controls specified by the regulations.
- Tamawal shall notify the SAMA as soon as it becomes aware of the occurrence of leakage or damage to personal data or the occurrence of illegal access to it.
- The Data Controller shall notify the owner of personal data in the event of leakage, damage to, or illegal access to, his data. If the occurrence of any of the above would cause serious harm to his data or himself, the control authority must notify him immediately.
- Tamawal shall respond to the requests of the owner of personal data regarding his rights stipulated in the system within a specified period and through an appropriate means indicated by the SAMA.
- The Data Controller shall evaluate the effects of processing personal data for any product or service provided to the public according to the nature of the activity practiced by the Data Controller.
- The privacy of credit data of the data owner shall be assured at all times and the rights in the Tamawal systems shall ensure the following:
- Take what is necessary to verify the availability of the personal data owner's written consent to collect this data or change the purpose of collecting, disclosing, or publishing it by the provisions of the system and the credit information system.
- The obligation to notify the owner of personal data when a request for disclosing his credit data is received from any party.
- Tamawal shall not use personal means of communication - including postal and electronic addresses of the owner of personal data to send advertising or awareness materials, except by the following:
- To obtain the consent of the target recipient to send this material to him.
- The sender of the materials provides a clear mechanism - as determined by the regulations - that enables the target recipient to express his desire to stop sending it to him when he so desires.
- Except for sensitive data, personal data may be processed for marketing purposes, if it was collected directly from its owner and agreed to do so by the provisions of the system. The regulations specify the necessary controls for this.
- Personal data may be collected or processed for scientific, research, or statistical purposes without the consent of its owner, in the following cases:

- If the personal data does not include evidence of the specific identity of its owner.
- If evidence of the identity of the owner of the personal data will be specifically destroyed during the process of processing it and before it is disclosed to any other party, and if such data is not sensitive data.
- If the collection or processing of personal data for these purposes is required by another system or in the implementation of a previous agreement to which its owner is a party.
- Official documents that identify the owner of personal data may not be photocopied or copied, except when this is in implementation of the provisions of a system, or when a competent public authority requests that such documents be photocopied or copied.
- Except in cases of extreme necessity to preserve the life of the data subject outside the Kingdom or his vital interests or to prevent, examine, or treat a disease infection, the controlling authority may not transfer personal data outside the Kingdom or disclose it to a party outside the Kingdom, unless this is in implementation of an obligation under an agreement that is The Kingdom is a party to it, or to serve the interests of the Kingdom, or for other purposes as determined by the regulations after the following conditions are met:
- The transfer or disclosure shall not prejudice national security or the vital interests of the Kingdom.
- Provide sufficient guarantees to preserve and confidentiality of the personal data that will be transferred or disclosed, so that the standards for protecting personal data are not less than the standards outlined in the law and regulations.
- The transfer or disclosure is limited to the minimum amount of personal data that is needed.
- The approval of the competent authority for the transfer or disclosure is determined by the regulations.
- Tamawal shall appoint a Data Privacy Officer to be responsible for its commitment to implement the provisions of the PDPL.
- Tamawal shall cooperate with the competent authority to carry out its tasks related to supervising the application of the provisions of the law and regulations, and it shall also take the necessary measures regarding issues related to this that the competent authority refers to. The competent authority may request the necessary documents or information from the control authority to ensure its compliance with PDPL.
- The Data Controller shall keep records for 10 financial years. Provided that the records include a minimum of the following data:
- Contact details of the controller.
- Purpose of processing personal data.
- Description of the categories of personal data subject
- Any party to whom personal data has been (or will be) disclosed.
- Whether personal data has been (or will be) transferred outside the Kingdom or disclosed to a party outside the Kingdom.
- The expected length of time for retention of personal data.
- The owner of personal data may submit to the office any complaint arising from the application of the system and regulations. The regulations specify the controls for the office's handling of complaints submitted by the owner of personal data arising from the application of the system and regulations.
- Anyone who has undertaken a personal data processing business is obligated to maintain the secrets. related to the data even after the termination of his employment or contractual relationship.

7. EXCEPTION HANDLING

Exceptions to this policy in case of any business requirement or limitation should follow Tamawal's exception-handling process. The same needs to be reviewed and approved by the CEO and CISO.

8. MONITORING, EVALUATION, AND REVIEW

A review of this document should be conducted at least every 12 months by stakeholders and the department responsible for drafting the document. The review should cover the results, non-conformities detected resulting from an audit, or other observations such as changes via external or internal laws and regulations and other factors.

9. RECORDS

The master of this document shall be maintained with the Cybersecurity Department