Cyber Security Policy

v1.0

Document Control Information

Document Version Control Information				
Version	Date	Author	Reviewer	Approver
1.0	**03 Oct 2024**	Abdulrahman AlJamani	Ahmed Al-Kelani	Misfer Al-Ajmi

Document Change History Information			
Author	Date	Version	Change Description

Contents

1 Introduction 5
2 Purpose and Applicability 5
3 Scope 5
4 Cyber security Policy Objectives 5
5 References 6
6 Access control 6
6.1 Access to the Information Systems 6
6.2 Remote Access 6
7 Data classification and handling 7
8 Acceptable use 8
9 Cyber security training and awareness 8
10 Cyber security risk management 9
11 Business continuity and disaster recovery plans 9
12 Cyber security events and weaknesses 10
12.1 Incident Management 10
13 Responsibilities 10
13.1 Leadership and Commitment 10
13.2 Organizational roles, responsibilities and authorities 10
13.3 Review 16
13.4 Monitoring 17
13.5 Security Violation 17
14 Contractual obligations 17
15 Cyber security policy exception 17
16 Related Policies and Processes 17
17 Terms & Definitions 19

1 Introduction

Cyber security is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect JADARAH 's information assets against internal and external threats.

Cyber Security Policy forms the basis of JADARAH Cyber Security in line with International Standard (ISO/IEC 27001) and SAMA Cyber Security Framework to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the Cyber Security at JADARAH.

This Cyber Security Policy is a formal set of rules by which those people who are given access to company technology and information assets must abide.

2 Purpose and Applicability

JADARAH is committed to protecting the confidentiality, integrity and availability of its information assets. The main purpose is to inform company users, employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of JADARAH. The Cyber Security Policy describes the technology and information assets that we must protect and identify many of the threats to those assets.

3 Scope

This policy applies to JADARAH and all parties, its affiliated partners or subsidiaries, including data processing and process control systems, that are in possession of or using information and/or facilities owned by JADARAH. This policy applies to all information, information systems, networks, applications, locations and staff/ users that are directly or indirectly employed by JADARAH, subsidiaries or any entity conducting work on behalf of JADARAH that involves the use of information assets owned by JADARAH.

4 Cyber security Policy Objectives

The objectives of the corporate cyber security policy are to demonstrate and express the intention and commitment of JADARAH to:

- Protect information assets from all threats, whether internal or external, deliberate, or accidental thereby ensuring uninterrupted services to Employees, Customers and Stakeholders.

- Manage the risks to an acceptable level through design, implementation, and maintenance of an effective Information Security Management system.
- This policy forms the basis and identifies key principles all Information Security initiatives and policies in JADARAH.

5 References

- ISO/IEC 27001:2013 – Information Technology-Security, Techniques-Information Security, and Management Systems – Requirements.
- SAMA Cyber Security Framework 3.1.3.

6 Access control

Access to JADARAH resources and information assets should only be granted following a controlled, auditable process based on operational and security requirements by the nominated information owner.

6.1 Access to the Information Systems

The access control shall be in place to protect JADARAH networks, information systems and assets from unauthorized access.

The Access to JADARAH systems and data will be granted on a "need to know basis", the minimum access needed to perform duty. Access is defined in Access management policy to protect the systems and data in them from accidental or intentional loss.

6.2 Remote Access

The remote connections made to JADARAH network shall be used strictly in accordance with acceptable use policy.

The access via remote connections shall be regularly reviewed and any connections that are no longer required shall be removed immediately.

7 Logging and monitoring of User Activities

1. **Mandate for Logging**: The organization requires comprehensive logging of all user activities across its systems and networks. This includes, but is not limited to, login attempts, access to sensitive data, and modifications to system configurations.

2. **Retention Period**: All logs must be retained for a minimum period defined by applicable compliance requirements to ensure that historical data is available for review and analysis.
3. **Regular Reviews**: It is mandatory to conduct regular reviews of the logs to identify unusual activities or potential security incidents, thereby enhancing the organization's ability to detect and respond to threats.
4. **Importance of Monitoring**: The failure to implement effective logging and monitoring measures compromises the organization's capability to identify and address security threats in a timely manner.

8 Data classification and handling

- The Data Classification Policy section defines a framework for the classification of the information according to its importance and risks involved. It is aimed at ensuring the appropriate integrity, confidentiality and availability of the Organization information.

- Ensure all user information found in assets/computer system files and databases shall be classified. Which details how information assets of different sensitivities shall be managed, handled, processed, encrypted, stored, transmitted, dispatched and disposed of when no longer required.

- Each information asset shall have a nominated owner. The information asset owner has the responsibility of classifying the asset based on the data classification scheme and related guidelines.

- Cyber security department shall identify and approve the security controls for the protection of the information in accordance with classification of data.

- All data stored, extracted, created, or accessed via JADARAH's systems must be given a
  sensitivity classification.

Data classification levels at JADARAH have been defined as:

- Secret

- Confidential
- Internal
- Public

9 Acceptable use

1.1 Ensure that all personnel, contractors and third-party users comply with the Acceptable Use Policy of JADARAH which will detail how information assets and their supporting assets should be used in an acceptable manner and in accordance with all Cyber Security related policies and processes.

Acceptable use policy shall have detailed acceptable methods of use of information processing systems, networks and other resources within the Scope of this Policy.

10 Cyber security training and awareness

- An ongoing awareness program is established and maintained in order to ensure that staff awareness is refreshed and updated as necessary. Every quarter, awareness sessions are conducted to all JADARAH employees and contractors/vendors associated with JADARAH.
- Apart from investing in Cyber Security team training and development, JADARAH also ensures that relevant and other personnel are aware of Cyber Security policy, activities and contribution to the effectiveness of the Cyber Security including the benefits of improved Cyber Security performance and the implications of not to conforming with the Cyber Security requirements.

11 Cyber security risk management

- JADARAH Information and information systems security risks must be identified, assessed, mitigated and monitored to help protect the confidentiality, integrity and availability.
- JADARAH follows structure risk assessment methodology; rating techniques to evaluate the risks faced which requires the identification and quantification of information security risks in terms of their perceived value of asset, severity of impact and the likelihood of occurrence.
- Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks which is part of Enterprise risk management.
- Cyber security risk appetite ties operational, cyber security, and enterprise risk together for
    - Managing the JADARAH ’s business effectively, efficiently
    - To know where to invest time, resources and to set the boundaries for prioritizing which risks need to be treated.
- Cyber security risk appetite is set by the CISO and head of risk to determine how much risk is accepted to achieve business goals & objectives, where cyber security risk is calculated through assessment using defined methodologies.

10.1 Outsourcing

a. **Vendor Selection**: Only vendors with certified cybersecurity expertise and a proven track record are eligible. All vendors must undergo a thorough security risk assessment before being contracted.
b. **Contract Requirements**: Contracts must include clear cybersecurity obligations, data protection measures, and compliance with relevant standards (e.g., ISO, NIST). Vendors must agree to notify the organization immediately of any security incidents.
c. **Monitoring & Auditing**: Regular audits and continuous monitoring of the vendor's cybersecurity practices are mandatory. Access to sensitive data must be limited and closely tracked.
d. **Incident Response**: Vendors must have a defined incident response plan. Any breaches or security incidents must be reported and remediated swiftly according to agreed procedures.

10.2 Business continuity and disaster recovery plans

JADARAH will ensure that information security is a key consideration and will produce the Business Continuity Management Policy, Business impact assessment and disaster recovery plans so that the security of JADARAH information assets is not compromised with unplanned business interruptions.

10.3 Cyber security events and weaknesses

1.2 All JADARAH employees, contractors and third-party users (if any) shall be made aware of their responsibility to report any Cyber security event, near misses, and suspected weaknesses as quickly as possible to the Incident response team.

This will be compiled with below Incident management process

13.1 Incident Management

All Information Security Incidents shall be managed in accordance with the Information Security Incident Management Response Procedure. The severity of the incident shall be assessed, and the management response shall be proportionate to the threat.

Cyber security incident response processes include:

- Identification of the incident.
- Investigation of the incident.
- Containment of the incident.
- Recovery of business operations.
- Planning of corrective action.
- Implementation of corrective action to prevent recurrence.
- Reporting action taken.

12 Responsibilities

14.1 Leadership and Commitment

Top management including Board of Directors, Consultant, and Cyber Security Committee are responsible for effective implementation and improvement of the Cyber security management. The Board of Directors demonstrates full commitment to the Cyber Security Management System by:

a. Ensuring that enough budget for Cyber Security is allocated.
b. Approving the Cyber Security committee charter.
c. Endorsing (after being approved by the Cyber Security committee)
    1. The Cyber Security governance.
    2. The Cyber Security strategy.
    3. The Cyber Security policy.

14.2 Roles of Chief Information Security Officer

The Chief Information Security Officer (CISO) responsibilities include, but are not limited to:

▪ Developing and maintaining:
• Cyber security strategy;
• Cyber security policy;
• Cyber security architecture;
• Cyber security risk management process.
▪ Ensuring that detailed security standards and procedures are established, approved and implemented
▪ Delivering risk-based cyber security solutions that address people, process and technology
▪ Developing the cyber security staff to deliver cyber security solutions in a business context
▪ The cyber security activities across JADARAH Company, including:
• Monitoring of the cyber security activities
• Monitoring of compliance with cyber security regulations, policies, standards and procedures;

• Overseeing the investigation of cyber security incidents;
• Gathering and analyzing threat intelligence from internal and external sources;

• Performing cyber security reviews;
• Monitor security operation center (SOC) activities, reports and performance to ensure the security requirements are met.

▪ Conducting cyber security risk assessments on the JADARAH Company's information assets

▪ Proactively supporting other functions on cyber security, including:
• Performing information and system classifications;
• Determining cyber security requirements for important projects;
• Performing cyber security reviews.
▪ Defining and conducting the cyber security awareness programs
▪ Measuring and reporting the KRIs and KPIs on:

• Cyber security strategy
• Cyber security policy compliance
• Cyber security standards and procedures
• Cyber security programs (e.g., awareness program, data classification program, key cyber security improvements)

▪ Prepare High and Medium incidents Report to SAMA and to the Cyber Security committee
▪ Include the Cyber Security in project management
▪ Ensure physical security measures are identified and implemented
▪ obtain 'no objection' from 'SAMA IT Risk Supervision' before any media interaction related to the incident

▪ Implementing the controls for the compliance with relevant regulatory requirements affecting cyber security across the Organization
▪ Implementing the controls for the compliance with the secure disposal standard and procedure.
▪ Reviews the information security Internal/External audit reports and ensure findings are probably addressed.
▪ Evaluate new technologies and processes that enhance cyber security capabilities.

14.3 Organizational roles, responsibilities and authorities

Top management ensured the responsibilities and authorities for roles relevant to Cyber Security by establishing a Cyber Security committee and appointment of CISO.

14.3.1 External Stakeholders

Identification criteria of external stakeholders are as follows:

- All those who are in indirect relationship or concern with JADARAH.
- All those whose business existence does not rely on the existence of JADARAH.
- All those who can influence the activities of JADARAH by their change in trends, performance, or policies.

External Stakeholders can be:

- Strategic business partners.
- Suppliers or vendors.

- Legislative bodies.
- Government Agencies.

14.3.2 Internal Stakeholders

Internal stakeholders are all those who are accepted as part or team members of JADARAH by top management and can be identified as:

- All those who have direct concern with the performance of JADARAH
- All those professional and business growth relies on the growth of JADARAH.

Internal stakeholders and their roles and responsibilities:

Role / position	Responsibilities
Cyber Security Committee	• Approving, supporting, and monitoring Cyber Security governance, strategy and policy. • Monitoring, reviewing, and communicating JADARAH Cyber Security risk appetite, and risks potential likelihood, frequency, and severity of cyber-attacks and data breaches. • Responsible to ensure the Enterprise Cyber Security strategy aligns with the JADARAH objectives. • Discuss JADARAH Cyber Security policies as to risk assessment and risk management, including the review of the guidelines and policies established by JADARAH to assess, monitor, and mitigate JADARAH significant Cyber Security risk exposures. • Review and approve Cyber Security programs such as awareness program, data classification program, data privacy, data leakage prevention, key Cyber Security improvements. • Reviewing reports, and recommendations for development and adequacy of an incident response plan, adequacy of resources to respond to a breach and risks. • Review with management, at least annually, any major security incidents that have occurred and steps that have been taken to mitigate against reoccurrence. • The Committee shall review and reassess Cyber Security Committee Charter, including the Committee's purpose and oversight role, at least annually and submit recommendations.

Board of Director/ Founders	• Ensure cyber security function is defined and approved.
	• Review and approve the cyber security strategy to ensure that it supports JADARAH objectives and vision in compliance with related regulatory requirements.
	• Ensure the cyber security strategy is executed within JADARAH.
	• Review and approve the cyber security standard, process, and procedures.
	• Allocate budgets for Cyber Security.
	• Ensure sufficient resources are allocated for CS function Approve Cyber Security Projects.
	• Establish cyber security committee.
	• Approve the cyber security committee charter.
	• Endorsing (after being approved by the cyber security committee)
	  ○ The cyber security governance.
	  ○ The cyber security strategy.
	  ○ The cyber security policy.

CISO	• Define the cyber security function's objective. • Develop, Review and approve CS policies, procedures, guidelines and standards and ensure its implementation. • Review non-conformances raised during Internal/external audits. • Review and conduct the cyber security awareness. • Conduct Cyber Security risk assessment and Project Risk assessment • Report cyber risks and cyber incidents to CSC on quarterly basis. • Present cyber security KPI to CSC members. • Developing the cyber security staff to deliver cyber security solutions in a business context. • Overseeing the investigation of cyber security incidents. • Proactively supporting other functions on cyber security. • Determining cyber security requirements for important projects. • Performing Cyber security review. • Conduct cyber security risk assessment.
Head of Risk	• Review and approve cyber security risk management methodology or process. • Review the cyber security risk register. • Discuss and approve cyber security treatment plan.

Head of Compliance	• Conduct cyber security compliance review on annual basis. • Present the cyber security compliance report to the cyber security committee. • Review SAMA self-assessment. • Maintain the communication with SAMA regarding all the compliance requirements.
Head of internal Audit	• Develop Cyber security audit plan. • Performing cyber security audits. • Present the internal audit result to cyber security committee.
Head of HR	• Review and approve the cyber security policies, procedures, guidelines and standards, related to Human Resource and administration responsibilities. • Ensure implementation of HR and administration policy, procedures, guidelines and standards. • Maintain Employee security training and awareness record. • Coordination with Cyber security team to implement the cyber security awareness program. • Making sure all employees sign and agree to cyber security acceptable use policy when they join the organization. • Involved in Cyber security incident investigation related to internal employee.
Head of IT	• Review and approve Technology related CS policies, procedures, guidelines and standards. • Ensure implementation for the cyber security operation and technology g domain from SAMA cyber security framework. • Monitor implementation of Cyber Security technology projects. • Provide IT resource for Cyber Security projects as required. • Making sure all IT infrastructures including network devices, servers, are configured in align and compliance with the cyber security policies, process, and standards.
Head of Finance	• Approve the budget for Cyber Security projects. • Allocate budget for Cyber Security function.
Head of Legal	• Provide the expert legal advice that is necessary for other departments to provide services in a manner that is fully compliant with existing regulations and instructions.

14.4 Review

Upon the completion of the creation of Information Security common policies, the documents shall be submitted annually to the cyber security Committee for review and approval. Inputs will be taken from all stakeholders for verifying the acceptability of policies created. The cyber security Committee will either accept or reject the Policies created. Rejected policies will be subject to change as per the cyber security Committee comments.

14.5 Monitoring

JADARAH has in place routines to regularly audit compliance with this and other policies. In addition, it reserves the right monitor activity where it suspects that there has been a breach of policy.

14.6 Security violation

Ensure that all personnel, contractors and third-party users who use the technology and information resources of company must be aware that they can be disciplined if they violate this policy. Upon violation of this policy, an employee of company may be subject to discipline up to and including discharge and taking into consideration the nature and severity of the violation of the Cyber Security Policy.

14.7 Contractual obligations

- JADARAH will develop standard SLAs to address security, non-disclosure agreements and disaster recovery issues to improve the quality obligations of vendor security contracts.

14.8 Cyber security policy

Information security considerations such as confidentiality, integrity, availability, regulatory and compliance requirements are met when JADARAH employees, contractors, vendors and other authorized users employ centrally supported or recommended standards.
All Information technology resources connected to JADARAH are expected to comply with security polices and standards which are designed to establish necessary control to protect JADARAH Information assets. All policies exceptions must be approved by CISO, provided with a reasonable, justifiable business and/or research case a for a Cyber Security policy exception. Any additional Approvals may be required based on the level of risk the exception represents.

14.9 Related Policies and Processes

The below list enables and addresses consolidated inputs for policies, procedures and standards and the rules in support of this Policy.

- IT Policy & Procedures
- Data classification policy.
- Password Policy.
- Encryption policy.
- Application Security policy.
- Asset management.
- Bring your Own Device.
- Incident Management.
- Event and threat management.
- Vulnerability Management.
- Enterprise Risk management.
- Compliance.
- Business Continuity Management plan.
- Human Resources security.
- Training and Awareness.
- Contract and Vendor Management.

14.10 Terms & Definitions

SAMA	Saudi Arabian Monetary Authority which is a Cyber Security Framework
BOD	Board of Director / Founders
Top Management	CEO, CFO, CRO, COO, BOD.
CSF	Cyber security framework
JADARAH	JADARAH Debt Collection Company
Asset	Anything tangible or intangible that has value to the organization. There are many types of assets, and some of which include obvious things, such as: persons, machineries, utilities, patents, software and services. The term could also include less obvious things, such as: information and characteristics (e.g., organization's reputation and public image, as well as skill and knowledge).
Availability	Ensuring that authorized people have access to the information or information systems at all times.
Confidentiality	Ensuring access to information or information systems to authorized people.
Integrity	Ensuring authorized modification by authorized people.
Authorization	It is the function of defining and verifying access rights/privileges to resources related to organization's information and technical assets security in general and to access control in particular
Information Security (Cyber security)	Maintaining the confidentiality, integrity and availability of information and information systems.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit particular information system vulnerability.

Incident	An adverse event or A compromise through violation of information security policies, acceptable use policies, practices or information security controls or requirements.
Information risk	The risks to organizational operations (including vision, mission, functions, image or reputation), organizational assets, individuals, other organizations, or the nation due to the potential of unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
Users	All employees, staff, contractors, outsourced and third parties who have access to JADARAH ’s information and/or information systems, facilities, premises etc.
CSC	Cyber security committee
Business Unit	Department or division within the organization