Cybersecurity
Leadership and Governance

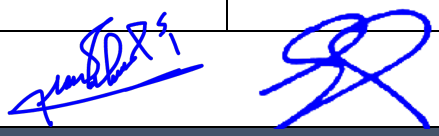
v1.0

Jadarah For Dept Collections Co.

This document is a property of **Jadarah For Dept Collections Co.** and contains sensitive and confidential information which should not be disclosed, transmitted, duplicated, and used in whole or part other than for its intended purpose and recipients

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

Document Control Information **2**
1 Introduction **4**
2 Purpose **4**
3 Abbreviations and Definitions **5**
4 Top Management Leadership and Commitment **5**
5 Delegation of Authority **6**
6 Cyber Security Roles and Responsibilities **6**
6.1 Chief Information Security Officer 6
6.2 Cyber Security Manager 7
6.3 Cyber Security Risk Owner 8
6.4 Other roles with Cyber Security responsibilities 8
7 Cyber Security Governance **9**
8 Cyber Security Strategy **10**
8.1 Objectives of Cyber Security Strategy 10
8.2 Cyber Security Strategy Framework 10
9 Cyber Security Risk Management **11**
9.1 Purpose 11
10 Cyber Security in Project Management **11**
11 Cyber Security Awareness and Training **11**

1 Introduction

This document defines the Cyber Security Leadership and Governance policy of Jadarah For Dept Collections Co. to provide the framework and capacity for making and implementing decisions required to manage, control and monitor IT within the business.

As a modern, forward-looking business, Jadarah For Dept Collections Co. recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

In order to provide such a level of continuous operation, Jadarah For Dept Collections Co. has implemented its Cyber Security Management System in line with the SAMA Cyber Security Framework.

The operation of the Cyber Security has many benefits for the business, including:

- Protection of revenue streams and company profitability
- Ensuring the supply of goods and services to customers
- Maintenance and enhancement of shareholder value
- Compliance with legal and regulatory requirements

Jadarah For Dept Collections Co. has decided to align its Cyber Security operations with the ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated.

This policy applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to [Organization Name] systems.

2 Purpose

The objective of Cyber Security Leadership and Governance is to:

- Demonstrate Jadarah For Dept Collections Co.'s Leadership commitment to Cyber Security
- Ensure cyber security risks are properly managed
- Achieve protection of revenue streams and company profitability
- Create a common approach for addressing cyber security within Jadarah For Dept Collections Co. to an appropriate maturity level of cyber security controls
- Compliance with legal and regulatory requirements

3 Abbreviations and Definitions

CS: Cyber Security

CISO: Chief Information Security Officer

CSMS: Cyber Security Management System

SAMA: Saudi Arabian Monetary Authority

Management: Leadership team of Jadarah For Dept Collections Co. responsible to drive business strategy and direction

4 Top Management Leadership and Commitment

Commitment to Cyber Security extends to senior levels of the Jadarah For Dept Collections Co. and will be demonstrated through this manual and the provision of appropriate resources to provide and develop the Cyber Security and associated controls.

Top management will also ensure that a systematic review of performance of the programme is conducted on a regular basis to ensure that quality objectives are being met and relevant issues are identified through the audit programme and management processes. Management review can take several forms including departmental and other management meetings.

The Chief Information Security Officer shall have overall authority and responsibility for the implementation and management of the Cyber Security Management System, specifically:

- The identification, documentation and fulfilment of cyber security requirements
- Implementation, management and improvement of risk management processes
- Integration of operational processes, procedures and controls
- Compliance with statutory, regulatory and contractual requirements
- Reporting to top management on performance and improvement

5 Delegation of Authority

Task/Activities	Cyber Security Risk Owner	Cybersecurity Manager	Chief Information Officer (CISO)	Chief Executive Officer (CEO)
Establish the context of Jadarah For Dept Collections Co.		C	A/R	I
Leadership and Governance of Cyber Security	C	R	C	A
Planning and Support of Cyber Security Operations	C	R	A	I
Cyber Security Risk Management	R	C	A	I
Cyber Security Performance Evaluation	C	R	A	

Legend			
R	A	C	I
Responsible	Accountable	Consulted	Informed

6 Cyber Security Roles and Responsibilities

Within the Cyber Security remit of Jadarah For Dept Collections Co., the following major roles are defined and allocated:

- Chief Information Security Officer
- Cyber Security Manager
- Cyber Security Risk Owner

6.1 Chief Information Security Officer

The Chief Information Security Officer has the following responsibilities:

- Establish and maintain the Cyber Security governance.
- Communicate the importance of meeting the objectives and the need for continual improvement throughout the organization
- Ensure that Cyber Security requirements are determined and are met with the aim of minimizing risk and maintaining effective controls for Jadarah For Dept Collections Co. and for our customers
- Determine and provide resources to plan, implement, monitor, review and improve Cyber Security management
- Oversee the management of risks to the organization and its services
- Facilitate top management leadership of Jadarah For Dept Collections Co. with management reviews of Cyber Security, at planned intervals, to ensure continuing suitability, adequacy and effectiveness

- Establish a continual improvement policy with respect to Cyber Security for Jadarah For Dept Collections Co.
    - Review major Cyber Security incidents
    - Ensure that arrangements that involve external organizations having access to information systems and services are based on a formal agreement that defines all necessary security requirements

The Chief Information Security Officer has the authority to:

- Approve significant expenditure on Cyber Security related matters
- Recruit additional resources for the management of Cyber Security
- Approve high-level policies for Cyber Security

6.2 Cyber Security Manager

The Cyber Security Manager has the following responsibilities:

- Reporting to the Chief Information Security Officer on all security related matters on a regular and ad-hoc basis when required
- Communicate the Cyber Security policy to all relevant interested parties where appropriate, including customers
- Implement the requirements of the Cyber Security policy
- Manage risks associated with access to the service or systems
- Ensure that security controls are in place and documented
- Quantify and monitor the types, volumes and impacts of security incidents and malfunctions
- Define improvement plans and targets for the financial year
- Monitor achievement against targets
- Establish and maintain a continual improvement action list
- Report on improvement activities
- Identify and manage information security incidents according to a process
- Attend management review meetings on a regular basis

The Cyber Security Manager has the authority to:

- Declare Cyber Security incidents
- Approve limited expenditure on Cyber Security related matters
- Review the operation of controls within all business areas

6.3 Cyber Security Risk Owner

The Cyber Security Risk Owner has the following responsibilities:

- Responsible for the monitoring and management of specific risks to information security
- Maintain and review security controls that treat the managed risk(s)
- Participate in assessments concerning the risk(s) for which they are the owner
- Liaise with the owner(s) of the information asset(s) affected by the risk(s) they own
- Report on improvement activities
- Identify and manage information security incidents according to a process
- Attend management review meetings on a regular basis

The Information Security Risk Owner has the authority to:

- Escalate to management where one or more of their risks is not adequately addressed
- Approve the level of residual risk after treatment actions have been identified in the Risk Treatment Plan

6.4 Other roles with Cyber Security responsibilities

There are also particular Cyber Security related responsibilities that must be carried out by other internal roles such as, Department Managers who are heading/supervising operational units within Jadarah For Dept Collections Co..

These roles have the following responsibilities:

- Review and manage employee competencies and training needs to enable them to perform their role effectively within the Cyber Security area
- Ensure that employees are aware of the relevance and importance of their activities and how they contribute to the achievement of Cyber Security objectives

7 Cyber Security Governance

The purpose of the Cyber Security Governance is to ensure the effective implementation of security controls which are necessary to ensure the confidentiality, integrity, availability, durability and quality of technology resources and associated information/data. These assets must be adequately protected from unauthorized access, deliberate misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure.

Confidentiality: Data is only accessed by those with the right to view data

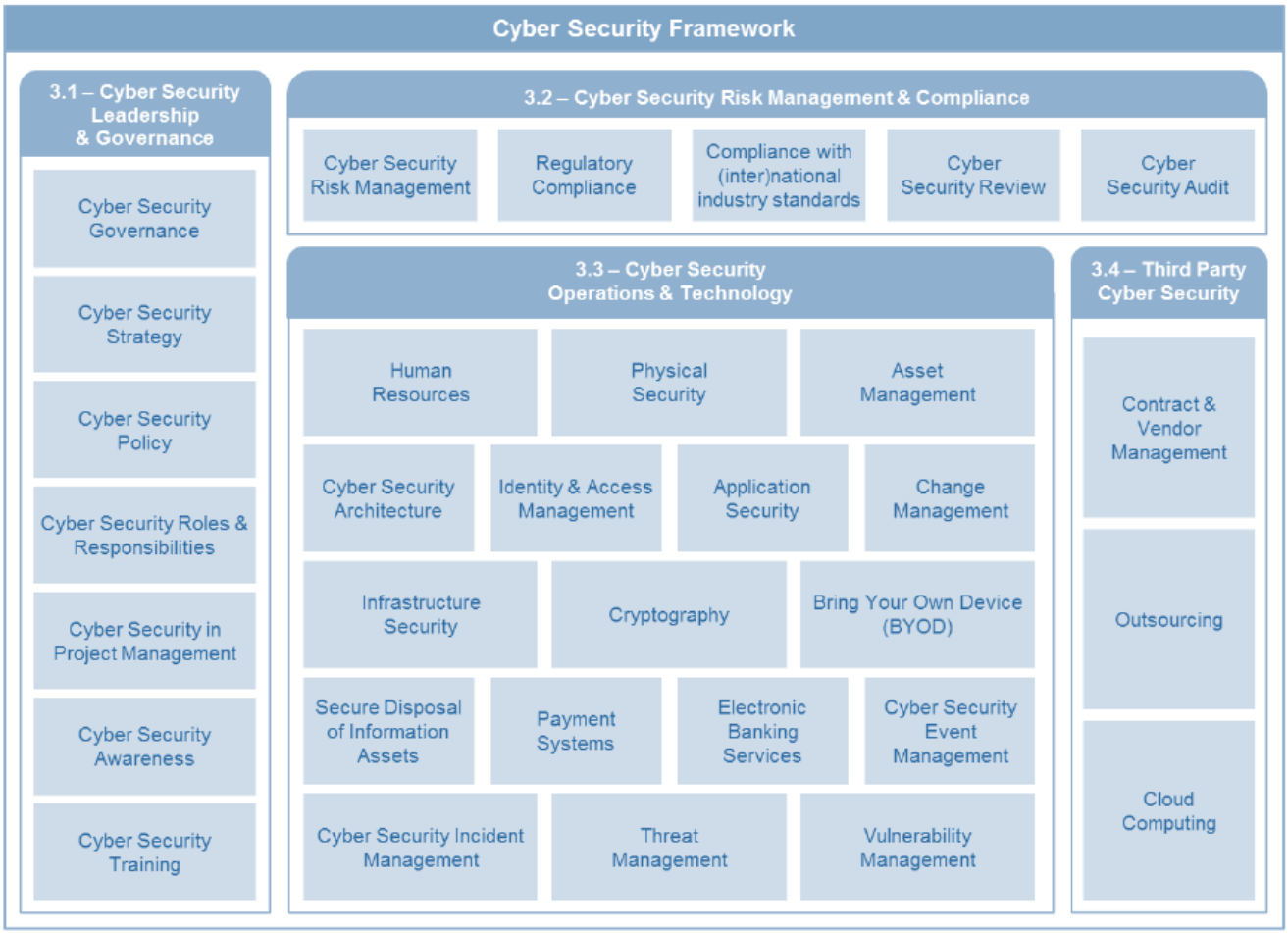
Integrity: Data can be relied upon to be accurate and processed correctly

Availability: Data can be accessed when needed

Quality: Data is fit enough to serve its purpose in a given context

Durability: Data does not suffer degradation, bit rot or any other form of corruption

Jadarah For Dept Collections Co. has aligned its Cyber Security Governance with the SAMA issues Cyber security Framework and extends it to all information assets under Jadarah For Dept Collections Co. with key focus on information in electronic form, supporting systems, network and other communication mechanisms. The figure below illustrates the overall structure of the Framework (as mentioned in SAMA Cyber Security Framework Manual) and indicates the cyber security domains and subdomains, including a reference to the applicable section of the Framework.



8 Cyber Security Strategy

Developing a Cyber Security strategy involves a fairly structured, sequential process that produces a long-term view of the Jadarah For Dept Collections Co.'s technology and business requirements together with a plan for meeting these needs. The Cyber Security strategy aligns with the mission of Jadarah For Dept Collections Co.'s goals and mission but is also pliable enough to accommodate new business priorities and technologies that the potential for driving business growth.

8.1 Objectives of Cyber Security Strategy

The objective of Cyber Security strategy is to cover the overall design and plan of the Cyber Security framework and should identify and overcome the organizational, cultural, and environmental constraints and enablers to achieve the strategic objectives.

8.2 Cyber Security Strategy Framework

The Cyber Security strategy shall include vision and mission, stakeholders, business, workflow and processes, data processing, system access, adoption of best-in-class information security systems, practices and the availability of IT resources. The Jadarah For Dept Collections Co. should also ensure that a proper strategic review process is in place to ensure that the Cyber Security Strategy remains relevant with the organizational strategies and direction to achieve business objectives. A graphical representation of the Cyber Security strategy can be viewed below.



9 Cyber Security Risk Management

Information Security Risk Management is the process of managing risks associated with the use of Information Technology. It involves identifying, assessing and treating risks to the confidentiality, integrity, availability, durability and quality of bank's assets.

9.1 Purpose

The objective of Cyber Security Risk Management is to treat risks in accordance with Jadarah For Dept Collections Co.'s overall risk tolerance. It doesn't expect to eliminate all risks, as it would be next to impossible. On the contrary, Jadarah For Dept Collections Co. seek to identify and achieve an acceptable level for itself.

The Scope of Information Security Risk Management process includes Risk Identification, Risk Assessment and Risk Treatment. For further details please refer to Risk Assessment and Treatment Process.



10 Cyber Security in Project Management

The acquisition, development, implementation and maintenance of new or revised application/management systems makes significant demands upon the financial, human and IT resources of Jadarah For Dept Collections Co.. It is essential for efficiency reasons and to ensure the quality of the system implementation that system development process is managed in accordance with Cyber Security Governance and Risk Management Framework and best practices. This is because all the IT based project requires access management, authentication, and involvement of external parties.

For all the IT related projects Jadarah For Dept Collections Co. make sure that it is aligned with our Cyber Security Program by ensuring following practices for each project:

1. Detailed cyber security requirements (specific regulatory needs)
2. Detailed risk management
3. Access management of resources
4. Post implementation testing (pen-testing)

11 Cyber Security Awareness and Training

Humans are considered the weakest link in the Cyber defence and therefore, Cyber Security awareness trainings are vital to prevent and mitigate user risks.

Jadarah For Dept Collections Co. has put established an integrated approach towards Cyber Security awareness and training to help its employees understand the importance of Cyber Security and their role in identifying and combating any security threats/breaches. We make sure that our Cyber Security awareness and training program follows the latest trends in Cyber Security landscape and is persistent as per the best practices.