Cybersecurity Training & Awareness Policy

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. **Purpose** **4**
2. **Scope** **4**
3. **Policy** **4**
4. **Cyber Security Awareness** **5**
5. **Cyber Security Training** **6**
6. **Cyber Security Training Records** **6**
7. **Cyber Security Training baselines** **7**
8. **Management Commitment** **7**
9. **Roles and Responsibilities** **7**
10. **Policy Management** **9**
11. **Enforcement and Compliance** **9**
12. **Reference Documents** **9**

1. Purpose

To provide Jadarah staff with guidance in developing and implementing the appropriate protective safeguards to support the confidentiality, integrity, and availability of Jadarah ’s assets and information.

To ensure that staff of the Jadarah are equipped with the skills and required knowledge to protect the Jadarah ’s information assets and to fulfil their cyber security responsibilities.

To create a cybersecurity risk-aware culture where the Jadarah ’s staff, third parties and customers
make effective risk-based decisions that protect the Jadarah ’s information assets.

2. Scope

This Policy applies to all staff/ users that are employed by Jadarah or its subsidiaries or any entity conducting work on behalf of Jadarah that involves the use of information assets owned by Jadarah.

3. Policy

- All employees, contractors, and anyone accessing Jadarah information systems must understand how to protect the Confidentially, Integrity, and Availibity of information and IT systems.
- In order for Jadarah to comply with SAMA Framework Requirement, a formal security training and awareness program must be in place. There are many aspects to consider when meeting this requirement.

- The best practices included in Cybersecurity policy and procedures are intended to be a starting point for Jadarah without a program in place, or as a minimum benchmark for those with existing programs that require revisions to:
    - Meet SAMA Cyber Security Framework requirements.
    - Address the quickly and ever-changing cyber security threat environment.
    - Reinforce JADARAH business culture.
- Establishing and maintaining Cyber-security awareness through a security training and awareness program is a very important to Jadarah success.
- A robust and properly implemented security awareness program assists Jadarah with the education, monitoring, and on-going maintenance of security awareness within the organization.
- Cybersecurity training reflects common security and privacy awareness specific to Jadarah ’s environment including, but not limited to, physical access, restricted areas, potential incidents, how to report incidents, laptop best practices, and how to spot a phishing scam.
    - Organizational Security Awareness: A successful security awareness program

within an organization which includes assembling a security awareness team, role-based security

awareness, metrics, appropriate training content, and communication of security awareness within the organization.

- Security Awareness Content: A critical aspect of training is the determination of the type of content. Determining the different roles within an organization is the first step to developing the appropriate type of content and will also help determine the information that should be included in the training.
- Security Awareness Training Checklist: Establishing a checklist will help Jadarah when developing, monitoring, and/or maintaining a security awareness training program.

4. Cyber Security Awareness

- The cyber security awareness programs should be defined, approved and conducted to promote cyber security awareness and to create a positive cyber security culture.
- A cyber security awareness program should be defined and conducted for:
  - Staff of the Jadarah.
  - Third parties of the Jadarah.
  - Customers of the Jadarah.
  - Trainees.
  - Part-time employees.
- The cyber security awareness program should target cyber security behaviours by tailoring the program to address the different target groups through multiple channels.
- Jadarah will provide on-going training through the Security and Privacy Awareness and Training activities. Which will provide information on selected topics.
- Jadarah will also conduct quarterly based refresher training for all employees and anytime there are significant changes to the environment. This will be administered via available resources and tracked for completeness and passing grade to show adequate understanding of the material.
- This policy will be reviewed on an annual basis or whenever there are significant changes to the environment.
- With the intention of protecting information assets, attitudes, and cybersecurity behaviour of user in different business departments should be target by cybersecurity awareness programs combined with knowledge. It implies that the users understand the threats they are facing, and they can apply appropriate measures to prevent such threats.
- Users are provided basic security awareness training as part of initial training for new users, as well as when required by system changes. All users must take refresher cybersecurity awareness

and training at least quarterly. Employees or contractors shall be having received the security awareness training either in writing or electronically as part of the training course completion.

- Security awareness training in Jadarah should focus on familiarizing the employees with the cybersecurity policy. The cyber security awareness focus for users should be measured and evaluated for the effectiveness of cyber security activities.
- Cyber security department should regularly update to information on relevant emerging cyber security events and cyber threats (e.g., spear-phishing, whaling) by following Cybersecurity.
- Cyber security awareness is scheduled quarterly and whenever there is an immediate requirement to make employees aware of emerging cyber security threats and vulnerabilities.
- The retail and commercial customers cybersecurity awareness mechanisms should be addressed for mitigating risks by sharing awareness information via Jadarah websites with awareness programs like phishing.

5. Cyber Security Training

To ensure that staff of the Jadarah are equipped with the skills and required knowledge to protect the Jadarah 's information assets and to fulfil their cyber security responsibilities.

- Cyber security skills training should be provided to staff in the Jadarah 's relevant functional area
  categories in line with their job descriptions, including:
  - Users
  - system administrators
  - Managers
  - business or non-technical user
  - Cyber security staff
  - Staff involved in asset and risk management
- Cyber security training should be provided to equip Jadarah staff to manage and operate information assets securely.

6. Cyber Security Training Records

Jadarah Cyber Security Department must ensure activities for monitoring and documenting basic security awareness training, as well as role-based training conducted. Employees and contractors will be reminded and monitored for successful course completion.

Jadarah will measure its baseline to understand how effective the cybersecurity wareness training is.

7. Cyber Security Training baselines

To understand Cybersecurity measure provided Jadarah would perform below baselines

- Results of simulated phishing assessments and social engineering assessments.
- Documented employee surveys and opinions on what they think about the existing security awareness training (if any) and, most importantly, how engaged they feel with it.
- Number and types of key security incidents over the past year. This should include phishing incidents, lost or stolen devices, malware incidents arising from employee behaviour, and any incident that can directly attribute to human error or oversight.

8. Management Commitment

Jadarah Senior Management will commit to the development of a security and privacy awareness program allocating staff and resources. Cyber Security Department will give access to both the compliance and training departments if required for completion and update of training materials and tracking results from Learning Management system.

Managers of respective business units should be responsible to track and confirm the attendance and completion of Cybersecurity awareness trainings.

9. Roles and Responsibilities

All employees and contractors are responsible for understanding and following all security related policies and procedures and communicating their manager for clarification if needed.

Managers are responsible for ensuring all employees complete required security training.

Roles	User	User Manager	CISO	System Admin	Cyber Security
Tasks					
Complete security awareness training	R	R			A
Develop and update the security awareness and training program			R		A
User acceptance of Security policies	R	A			
Create role-based security related training materials			R	R	A
Document and monitor system security training		I			A
Relations with security groups and associations for emerging cyber security events and cyber threats awareness.					A
Complete role-based security related training. (assigning related cybersecurity awareness trainings as per roles & responsibilities of employees)	R	A		R	I
Security training records		I			A/R

***R**: Responsible – Who is assigned to work on this task? **A**: Accountable – Who has the authority to take decisions?*

***C**: Consulted – Anyone who can tell more about this task? **I**: Informed – Who has to be kept updated about the progress?*

- The Cyber Security Department will oversee JADARAH 's Security Awareness and Training
  program, including development, implementation, and testing.
- The Cyber Security Department will coordinate, monitor, and track the completion of the Security Awareness Training for all JADARAH employees and business partners and report incomplete training to the respective managers.

10. Policy Management

Technological advances and changes in the business requirements will necessitate periodic revisions. Therefore, this Policy may be updated to reflect changes or define new or improved requirements.

Deficiencies within this Policy shall be immediately communicated to the Cyber Security Department. Policy changes will require the approval of the Cyber Security Committee and CISO of Jadarah.

Change log shall be kept current and will be updated as soon as any change has been made.

11. Enforcement and Compliance

Compliance with this Policy is mandatory and Jadarah managers shall ensure continuous compliance monitoring within their departments. Compliance with this Policy is a matter of periodic review by Cyber Security Department. Any violation will result in disciplinary action by Company's Management.

Disciplinary action will be depending on the severity of the violation which will be determined by the investigations. Actions such as termination or others as deemed appropriate by Jadarah and Human Resources Department shall be taken.

12. Reference Documents

- Cyber Security Policy
- Acceptable Use Policy
- Access Control Policy
- Physical Security