Information Security Project Management Policy

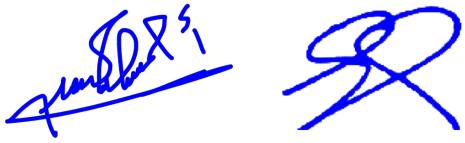
v1.0

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 Introduction **4**

2 Objective **4**

3 Scope **4**

4 Policy Statement **4**

4.1 General Statements 4

4.2 Initiation Phase 5

4.3 Planning Phase 5

4.4. Information Security Risk Management 5

4.5. Implementation Phase 6

4.7. Closing Phase 6

1 Introduction

A project is defined as a unique set of coordinated activities, with definite starting and finishing points, undertaken by an individual or team to meet specific business objectives within defined time, cost and performance parameters.

2 Objective

This document aims to ensure that all the JADARAH projects meet information security requirements and make sure that information security objectives are included in projects objectives.

3 Scope

This policy applies to the use of JADARAH information assets, whether owned or leased by JADARAH.

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 JADARAH employees, contractors and consultants 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 or leased by JADARAH. Access to JADARAH information should be limited where possible in compliance with the "Information Classification Guidelines".

4 Policy Statement

4.1 General Statements

4.1.1. Information Security Department should ensure that Information Security controls, requirements and objectives are incorporated into the project management life cycle of all JADARAH defined projects, irrespective of type, owner, or Project management methodology.

4.1.2. Ensure that Information Security objectives are applicable to be included and aligned with JADARAH project objectives.

4.1.3. Information Security Department is responsible for defining the Information Security threats and risks associated to every project that is done in JADARAH, regrades if the project is IT related or non-IT related, then specify the needed information security

controls to be implemented.

4.1.4. Ensure the defined information security requirements for every project in JADARAH, are shared to all stakeholders, along with the phases of implementing these requirements.

4.1.5. If any Project in JADARAH needs Information Security review (such as penetration testing and vulnerability assessment). ensure the information security reviews is performed by an independent internal or external party that does not relate to the project.

4.1.6. Ensure that all project's documentation and communications that contains classified, commercially sensitive, or Personally Identifiable Information (PII) are classified, and labelled. The various aspects of ending a service should be carefully considered at initial contract negotiation time.

4.2 Initiation Phase

4.2.1. Information Security department should specify the information security requirements and considerations that related to every project in JADARAH.

4.2.2. The Project Manager may assign information security roles to project team members. Also, he may involve JADARAH operations staff members as early in the project and he might request their input on the information security requirements during planning phase. This will minimize the risk of last-minute security fixes.

4.3 Planning Phase

4.3.1. JADARAH project management communications plan should include the method, frequency, and audience for these communications, in addition, it may consider some best practices and guidelines for securing these communication channel, such as Secure documentations sharing. and secure documentations transfer and storage.

4.3.2. Secure JADARAH Project communication channels such as Telephone, conference calls and online Meetings should be password protected, this is to ensure that only specified stakeholders are online when the communications established. Also, to ensure that meetings passcodes are periodically changed.

4.3.3. Ensure the information Security requirements in any JADARAH project management are matching the global JADARAH information security policy and the related regulatory requirements.

4.4. Information Security Risk Management

4.4.1. Information security risk assessment should be performed by the Information security department at the start of every project to determine the Information Security risks and to ensure that Information Security requirements are addressed.

4.4.2. Information Security risks should be registered and tracked in the project risk-register.

4.4.3. Information security controls that are determined to mitigate any project's information

security Risks, should be under the responsibility of JADARAH Information Security department.

4.4.4. Information security risk treatments are handled according to the Project's risk management plans and the project's risk appetite.

4.5. Implementation Phase

4.5.1. Ensure that information security's access control considerations such as (The Need to Know and Least Privilege) applies to all project stakeholders' roles and responsibilities. The project stakeholders should only have access permissions based on their job functions in the project.

4.5.2. Ensure that any access to JADARAH project information and resources is recorded, in addition, the project manager and the project team must define and document a clear procedure for granting and revoking access rights during onboarding and off-boarding stakeholders in the project.

4.5.3. Ensure the project manager and the project team review every stakeholder's access rights

to the project information assets and resources and update these access rights periodically.

4.5.4. Ensure a strict requirement for secure credentials in JADARAH projects are followed during the project lifecycle, with the following considerations:

- Eight characters long, complex passwords
- Don't reuse passwords for multiple accounts
- Change passwords periodically.
- Don't share accounts with other team members
- Use two-factor authentication where appropriate

4.5.5. Ensure that any physical access to JADARAH Projects information assets such as (laptops and printers and servers) is recorded, in addition to the access recording of any printouts and papers documents.

4.5.6. Ensure that any JADARAH Project's sensitive paper documents never left unattended in an insecure location. Also, in case of disposal it should be shredded with cross-cut shredders.

4.6.1. Ensure the information security change controls in JADARAH projects are formally defined and documented. Also, should include Information security management responsibilities and procedures.

4.6.2. Ensure that Information security changes are evaluated on a risk matrix, i.e., probability vs. impact, benefits vs. costs, and ensure to manage to minimize impacts to the business needs.

4.6.3. Ensure the Implementations of Information security change management in JADARAH projects are undertaken before and after appropriate testing and approval by stakeholders

4.7. Closing Phase

4.7.1. Ensure the information security's lessons learned in every JADARAH project has defined and documented. As the lessons learned is valuable resource for JADARAH future projects

4.7.2. Ensure to archive every JADARAH project's information security documents for potential use in the future projects and audits.