Application Security 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

Table of Contents

Document Control Information **2**

1 Introduction **4**

2 Application Policy **4**

2.1 Purchasing Application 4

2.2 Application Registration 4

2.3 Application Installation 4

2.4 Removal of Application 5

2.5 In-house Corporate Application Development 5

2.6 Modifications to Application Packages 5

2.7 Use of Application in a Cloud Environment 5

2.8 Software Development Life Cycle (SDLC) Regulation 5

1 Introduction

Jadarah For Dept Collections Co. uses many types of software applications to perform its business operations and always relies upon the correct functioning and security of that application. It is imperative therefore that steps are taken to ensure that only approved application is used within the organization and that no classified information is put at risk.

This policy sets out how application will be acquired, registered, installed and developed within Jadarah For Dept Collections Co..

This control 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 Jadarah For Dept Collections Co. systems.

2 Application Policy

2.1 Purchasing Application

All application to be used within the organization must be purchased through IT department. This is necessary to ensure that:

- Licensing requirements are addressed
- The application works effectively with the standard corporate application image
- Use of the application can be supported by the IT department
- Best value for money is obtained in procurement
- A record is kept of installed application within the organization

Under no circumstances will application be purchased using local departmental budgets.

2.2 Application Registration

All application in use within Jadarah For Dept Collections Co. must be correctly licensed. All installed application programs will be registered in the name of the organization, not the individual. Purchased application is a corporate asset and licenses will frequently be reused as the shape of the organization changes.

Under no circumstances must corporate software application be copied (other than for backups) or installed for use on non-corporate machines, such as at home.

IT department will maintain a register of all licensed software within the organization and licensed copies of media.

Asset management software will be used to keep track of all installed instances of software titles and regular audits will be carried out. Any user with unlicensed software installed will be asked to remove it; it is the responsibility of users to ensure that all the application on their computer is licensed.

2.3 Application Installation

Licensed software will be installed by the IT department or appropriate technical team or supplier upon request and once any required licenses have been purchased.

No application will be installed prior to a valid license being ordered.

The user must not install any application that is licensed to them personally, whether or not it is free, shareware or commercial. This includes evaluation/trial versions of software programs.

2.4 Removal of Application

If a software program is no longer required the IT department must be informed. The software will then be removed from the device in question and where possible the license will be re-used elsewhere within the organization.

Users must not remove licensed software from their devices without informing the IT department as this potentially represents a waste of a corporate asset.

2.5 In-house Corporate Application Development

If Jadarah For Dept Collections Co. develops its own software for particular purposes where a commercial package is not available or does not fulfil the identified requirements. In such cases a structured development method will be used to ensure that software application is developed to organizational standards and is tested and implemented in a managed way.

Alterations to in-house developed application such as the addition of fields or screen changes may be requested through the change request process. Similarly, any changes to in-house developed software must not be made without following the change management process.

2.6 Modifications to Application Packages

Changes to Commercial Off the Shelf (COTS) software packages will not be made unless absolutely necessary, in which case they will be strictly managed and controlled. Where possible and commercially viable, changes will be made only by the software vendor and supplied as standard updates.

2.7 Use of Application in a Cloud Environment

Any applicable cloud-specific licensing requirements must be identified prior to installing software within a cloud environment. This is particularly relevant in circumstances where the cloud service provision is elastic i.e., the processing capacity increases and decreases with demand.

2.8 Software Development Life Cycle (SDLC) Regulation

1. **Objective**
   This SDLC regulation governs the development, testing, and maintenance of in-house applications to ensure secure, reliable, and high-quality software that meets the business and security requirements of the organization.

2. **Scope**
   The regulation applies to all in-house software development projects initiated within the company. It includes all stages of development, from initial planning to decommissioning, and applies to all employees, contractors, and third-party vendors involved in the development process.

3. **Phases**
   The following SDLC phases must be adhered to:

   - **Planning and Requirements Gathering**
     All project requirements must be documented and approved by stakeholders before development begins. Security and compliance requirements must be identified during this phase.

   - **Design**
     The software design must include architectural, technical, and security considerations.

Documentation should outline all system components and interactions, adhering to best practices and organizational standards.

- **Development**
  The development of software must follow coding standards, ensuring code quality, maintainability, and security. Source control systems must be used to manage code changes.

- **Testing**
  Testing must be conducted at multiple levels, including unit, integration, system, and user acceptance testing (UAT). Security testing and code reviews must be performed to identify and mitigate vulnerabilities.

- **Deployment**
  Software deployment must follow a formal release process, including change management approval, rollback procedures, and communication with relevant stakeholders.

- **Maintenance**
  Ongoing maintenance must include regular updates, security patches, and performance improvements. Bugs and vulnerabilities must be resolved promptly.

- **Decommissioning**
  Decommissioning of any software must ensure that data is securely archived or destroyed, and all dependencies are properly handled.

4. **Security and Compliance**

   - All in-house software must comply with relevant legal, regulatory, and internal security policies. Secure coding practices, such as input validation, encryption, and access controls, must be enforced throughout the SDLC process.

   - Periodic security assessments, such as vulnerability scans and penetration tests, must be conducted during development and after deployment.

5. **Documentation**
   Each phase of the SDLC must be thoroughly documented, including requirements, design, testing results, deployment plans, and maintenance logs. Documentation should be stored in a central repository accessible to relevant personnel.

6. **Version Control and Change Management**
   All code must be maintained in a version control system. Any changes to the software after the initial release must follow a formal change management process, including risk assessments, testing, and stakeholder approval.

7. **Responsibilities**

   - **Development Team**: Responsible for adhering to SDLC processes, developing secure and reliable software, and documenting all development activities.

   - **Project Managers**: Responsible for ensuring the project follows the SDLC process, managing timelines, resources, and ensuring stakeholder involvement.

   - **Security Team**: Responsible for conducting security reviews and ensuring compliance with internal and external security requirements.

   - **Quality Assurance (QA) Team**: Responsible for testing software for functionality, performance, and security.