Infrastructure 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

Contents

Document Control Information **2**
1 Introduction **4**
2 Infrastructure Security Management **4**
3 Network Security Management **6**
3.1 Network Management 6
3.2 Wireless Management 7
3.3 Firewall Security Management 7
3.4 Servers Management 8
3.5 Wireless Network Management 9
3.6 Desktop Management 11
3.7 Laptop Management 12
3.8 Storage Management 13

1 Introduction

This document, “Infrastructure Security Policy, defines the cyber security control and requirements associated with the use of infrastructure security techniques within Jadarah For Dept Collections Co.. It defines the required protection level to maintain the Confidentiality, Integrity and Availability of the confidential information assets and systems.

This Standard follows Best Practices, Regulatory and Compliance requirements such as the ISO/IEC 27001:2013 and SAMA Security Requirements.

Jadarah For Dept Collections Co. is committed to ensuring the safety of its information and technology assets and takes it very seriously. This policy sets out the safeguards that must be taken into account as part of our Cyber Security Framework.

This control applies to all infrastructure including operating systems, servers, virtual machines, firewalls, network devices, gateways, integrations, database, laptop, and mobile devices that are being used for Jadarah For Dept Collections Co. by its employees, contractors, third parties, and vendors.

2 Infrastructure Security Management

- The infrastructure security standard shall be based on Original Equipment Manufacturer (OEM) recommendations and industry best practices.
- The compliance with the infrastructure security standards shall be monitored periodically.
- The effectiveness of the infrastructure Cybersecurity controls shall be measured and periodically evaluated as per the policy of Jadarah For Dept Collections Co..
- The infrastructure security standards shall cover all critical infrastructure available in the datacentre(s), the disaster recovery data site(s), and office spaces vital for the operation of Jadarah For Dept Collections Co..
- The infrastructure security standards shall be prepared for the following list (but not limited to) of components:
    - Operating systems (servers, laptops, workstations, virtual machines, mobile devices)
    - Web Server software (…. etc.)
    - Database Servers (Oracle, MS-SQL, MySQL, etc.)
    - Network devices (Routers, Wireless Access Points, gateway servers, proxy servers, email gateways, PBX, etc.)
    - Security Devices (Firewalls, VPNs, IDS, IPS, etc.)
- The infrastructure security controls shall include:
    - The implementation of cybersecurity controls (Such as, configuration parameters, events to monitor and retain [including system access and data], data-leakage prevention (DLP), identity and access management, remote maintenance)
    - A documented authorization matrix that supports the segregation of duties within the infrastructure component
    - The protection of classified data aligned with the (agreed) classification scheme (including the privacy of customer data and, avoiding unauthorized access and (un)intended data leakage)
    - Assurance on the use of approved software and secure protocols
    - Segmentation of networks to prevent unauthorized access
    - Protection from malicious code/software and virus (and applying application whitelisting and advanced persistent threat (APT) protection)
    - Implement vulnerability and patch management according to policy requirements.

- DDOS protection (where applicable) shall be ensured, by means of using scrubbing, specifying bandwidth, testing DDOS scrubbing and implementing it for main datacenters and disaster recovery sites.
- The back-up and recovery procedures for information, software, and system images shall be defined
- The infrastructure security standard shall be subject to a periodic cyber security compliance review.

3 Network Security Management

- Networks shall be adequately managed and controlled, be protected from threats, and maintain security for the systems and applications using the network, including information in transit.
- Infrastructure elements and software(s) exposed to un-trusted or semi-trusted networks/users (e.g., internet-facing systems, third party etc.) shall be adequately protected by firewalls and limited connectivity.
- Network devices shall be hardened as per documented and approved hardening procedures or security standards before connecting to the Jadarah For Dept Collections Co.'s infrastructure.

3.1 Network Management

- Implementation of network cybersecurity controls shall be periodically reviewed.
- Critical infrastructure elements within IT networks that support AAA (Authentication, Authorization, and Accounting) integration shall be configured for AAA.
- Network Based Intrusion Prevention/Detection System shall be deployed to provide network forensics capabilities to cover critical network segments within IT infrastructure as per the risks identified.
- All end user systems connecting to the Jadarah For Dept Collections Co.'s infrastructure shall be hardened, patched, and installed with updated anti-malware software
- Remote access to Jadarah For Dept Collections Co.'s network resources over an un-trusted network (Internet/Extranet) shall be integrated into the overall network security management
- Internet and browsing security shall be implemented, including strict restriction of suspicious websites, file-sharing and storage sites and remote access software.
- Internet browsing channels shall be protected from Advanced Persistent Threats (APT) by implementing APT protection.
- Vulnerability assessment of these infrastructure elements shall be carried out as per Jadarah For Dept Collections Co.'s Vulnerability Management procedures.
- All network physical ports and diagnostic ports, shall be disabled when not used and their status shall be formally recorded
- The use of unsecure protocols such as (but not limited to) Telnet or FTP, which rely on clear text communications, shall not be allowed without compensating controls
- Domain Name System (DNS) security shall be in place to protect against DNS attacks such as DDOS attacks. All systems and system components like protocol stack shall be adequately patched for any identified vulnerabilities
- Permission to connect other networks and computer systems in Jadarah For Dept Collections Co.'s network shall follow exception management process
- End user systems used by IT vendors to manage Jadarah For Dept Collections Co. infrastructure elements and software(s) shall be configured as per Jadarah For Dept Collections Co. security policies for end user systems;
- Adequate redundancy shall be provided for network links and network devices. All single points of failure within the Jadarah For Dept Collections Co. network shall be identified and the risks in such a design shall be assessed and
- Logs generated by critical network devices shall be collected and analysed to identify threats and exceptions. Network security shall be monitored through a Security Operations Centre (SOC) to provide immediate response to threats.

3.2 Wireless Management

- Wireless may be used for Jadarah For Dept Collections Co. business communications if it meets the requirements outlined however, wireless shall not be used for management of production infrastructure elements and software(s)
- Security and protection of wireless networks shall be implemented using secure means for identity verification and encryption
- Wireless network shall not be connected with Jadarah For Dept Collections Co. internal network except on the basis of integrated study of the risks of doing so and how to deal with them to ensure the protection of the technical assets of Jadarah For Dept Collections Co..

3.3 Firewall Security Management

- Firewall(s) shall be used to limit and control the interactions between networks.
- Perimeter firewall shall control all traffic entering and leaving the internal network of Jadarah For Dept Collections Co. and defend from all types of malicious threats.
- Firewall administrators are responsible for maintenance, operation and support of all firewalls.
- Firewall administrator shall create a backup user, for an emergency administration with "Full Access Admin" privileges.
- Direct manager shall change related password for any resigned administrator.
- Account privileges shall comply with Jadarah For Dept Collections Co.'s Access Management Policy.
- User request for administrative access shall be subject to direct manager approval.
- Firewall administrator shall comply with the password policy.
- User authentication and access control shall comply with Jadarah For Dept Collections Co. Access Control Policy.
- Access to firewall management shall be done through a single approved interfaced that is guarded through MAC address filtering.
- Logical access to Firewall shall be limited only to the management subnet.
- Strong authentication technique (e.g., two-factor) shall be used to access the equipment configuration and services.
- All changes to firewall rules or configuration shall be approved by the respective manager.
- Firewall logs shall be securely stored.
- Firewall logs for "Deny", "Accept", "Dropped" or "Rejected" shall be maintained in syslog Server.
- All packet filtering through firewall shall be logged.
- Any changes to the firewall configuration shall be logged.
- Firewall(s) activity and audit logging shall be enabled and audited on event basis during and after a security event.
- Firewall(s) shall be configured for real-time monitoring and reviewed to ensure service availability and security.
- Firewall(s) shall be connected to a monitoring system that has messaging and notification capability.

3.4 Servers Management

- Server Security Management shall be applicable to all physical and virtual servers included but not limited to such as database servers, file share server, gateway servers, proxy servers, email gateways in Jadarah For Dept Collections Co.'s infrastructure
- Servers shall be adequately managed and controlled, to be protected from threats.
- Servers and installed its Operating System and software(s) exposed to un-trusted or semi trusted networks/users (e.g., internet facing systems, third party etc.) shall be adequately protected by firewalls and limited connectivity.
- Servers shall be hardened as per documented and approved hardening procedures or security standards before connecting to the Jadarah For Dept Collections Co.'s production infrastructure.
- Generic administrator accounts shall only be retained for emergency administration purposes, and their passwords shall be managed using Jadarah For Dept Collections Co.'s Password Policy.
- Application owner shall not have administrative rights on server's operating system.
- Administrator accounts and passwords shall be renamed from their default values.
- Staff shall only be granted server administration privileges after this has been authorised by the Information Owner, or the relevant Operations Manager who has been delegated with this authority for the system.
- Each person who requires server administrator access shall be assigned a specific administrator account, which is separate from their normal user account.
- Administration staff who leave shall have all of their passwords changed and user accounts disabled. The passwords shall also be changed for any other administrator accounts that they know.
- Access Management Group shall review user activity for dormant accounts on a periodic basis.
- All servers shall be located in approved data centres with strong physical security controls.
- Backup shall be carried out for all servers in compliance with Jadarah For Dept Collections Co.'s Backup process.
- Operating system and application configuration data on servers shall be backed up periodically (at least once per month) or upon change.
- Application data and end-user content on servers shall be backed up frequently (e.g., daily).
- All backups of confidential information shall be encrypted so that disclosure risks are minimized.
- Restore processes shall be tested periodically to validate the integrity of backups and the backup process.
- System logs on production servers shall be retained for at least 1 year.
- Server events that relate to the availability of a server or its key subsystems shall raise alerts to Jadarah For Dept Collections Co.'s Event Management System.
- Security-related events shall be logged centrally, and shall raise alerts to Jadarah For Dept Collections Co.'s Security Event Monitoring system.
- Centralised logs of security events on production servers shall be retained for at least 1 year.
- All Windows servers shall have anti-malware software installed, with real-time monitoring and alerting for abnormal activities.
- All internet-connected servers (e.g., web servers) shall have anti-malware software installed, with real-time monitoring and alerting for abnormal activities.

- The integrity of critical files on critical servers shall have real-time monitoring and alerting for unexpected changes.
- Reporting of incidents shall be carried out as per Jadarah For Dept Collections Co.'s Incident Management Process.
- All standard server software (including the operating system) shall follow a patch management process to ensure that security patches are assessed, prioritized and then applied in an appropriate timeframe.
- All patches shall be tested before they are deployed on production servers.
- Critical security patches shall be installed within one month of their release.
- Users shall comply with Jadarah For Dept Collections Co.'s Identity and Access Management Policy when accessing servers remotely.
- Security design reviews and risk assessments shall be completed for all systems before servers are deployed to production as per Jadarah For Dept Collections Co. Risk Assessment Process.
- All unnecessary services shall be removed or disabled for production servers.
- Administrators shall secure the operating system and other standard software as per the relevant technical control guidelines.
- Servers shall not be operated or administered from uncontrolled areas.
- All Jadarah For Dept Collections Co. servers shall have UPS sufficient for at least 30 minutes of operation in case of mains power failure.
- Pre-production vulnerability assessments shall be carried out on all new servers before the systems are deployed in production.
- Periodic vulnerability assessments shall be carried out on all servers on a regular basis.
- Information Owners and relevant Managers shall conduct a business needs analysis prior to retiring or disposing of any production servers.
- All confidential information shall be securely erased when servers are retired or sent for disposal.
- Servers shall only be sent for offsite maintenance after all server data has been backed-up, and confidential data has been securely erased.
- Any change to server configuration shall be maintained and documented as per the Change Management Process and Procedures.

3.5 Wireless Network Management

- Wireless Networks shall be adequately managed, controlled and, to be protected from threats.
- Wireless devices and software(s) exposed to un-trusted shall be adequately protected by firewalls and limited connectivity.
- Wireless devices shall be hardened as per documented and approved hardening procedures or security standards before connecting to the Jadarah For Dept Collections Co.'s production infrastructure.
- Generic wireless Access point's administrator accounts shall only be retained for emergency administration purposes, and their passwords shall be managed using the Password Repository. Generic used ID and accounts shall be removed.
- Administrator accounts and passwords shall be renamed from their default values.
- Limit wireless Access point's accounts to only those absolutely necessary, such as the administrator and reporting.
- The wireless Access points shall provide the capability to authenticate users before permitting access to Jadarah For Dept Collections Co. network.

- Only Administrator(s) shall be permitted to logon to wireless Access points.
- Access shall be provided through network authentication from centralized authentication server using a login and password.
- All access to the Wireless LAN (WLAN) system, including its data and resources, shall be restricted unless authorized.
- Outsiders/Guests, excluding approved vendors and contractors, shall not have access to WLANs that connect to Jadarah For Dept Collections Co. data network.
- File sharing on the computers connecting via wireless medium shall be disabled
- Wireless Administrator shall use WPA2 as well as Media Access Control (MAC) address filtering while employing WLAN solution.
- Web-based management of access points shall be from pre-defined management stations controlled by access lists on the access point.
- Logging and Notifications
- Logging and audit facilities provided by the wireless LAN Equipment shall be fully utilized.
- Access logs and system audit trails shall be reviewed and monitored on periodic basis.
- Wireless users/Network administrators are required to report any misuse, loss, or theft of wireless devices or systems immediately to the respective manager
- Security-related events shall be logged centrally, and shall raise alerts to the Security Event Monitoring system.
- Activity logging shall be enabled and audited on event basis during and after a security event.
- Real Time monitoring for the wireless LAN shall be in enabled and configured in secure manner.
- Controls and mechanisms shall be implemented to monitor rouge access points on Jadarah For Dept Collections Co. network.
- A Network Monitoring System (NMS) System shall be configured for real time alerting.
- Compensating controls shall be deployed in case of NMS absence.
- Wireless Administrator shall ensure that all wireless access points and wireless network interface cards (if applicable) are up to date with latest patch or firmware upgrade.
- All wireless access points shall follow a patch management process to ensure that security patches are assessed, prioritized and then applied in an appropriate timeframe.
- All patches shall be tested before they are deployed on wireless access points.
- Critical security patches shall be installed within one month of their release.
- Wireless administrator shall ensure that all Access Points have strong administrative passwords and ensure that all passwords are being changed as per Jadarah For Dept Collections Co. password policy.
- Disable Dynamic Host Configuration Protocol and shall use static IP addresses for wireless access points.
- Users that access public wireless networks (e.g., in airports, conference centres, coffee shops) shall install personal firewall and antivirus software on all WLAN client.
- In areas where utilization is not required on a 24 hours per day, 7 days per week basis, access points shall be turned off during all hours during which they are not used (e.g., after hours and on weekends) to minimize potential exposure to malicious activity.
- Wireless networks shall be scanned on periodic basis at least once every quarter for any rouge access points, unauthorized access points, unauthorized wireless devices or any other vulnerabilities. Incidents shall be reported as per Jadarah For Dept Collections Co. Incident Management immediately.

- IDS/IPS shall be configured to automatically generate an alert, of any/all unauthorized device detected during a manual wireless scan. Incidents shall be reported as per Jadarah For Dept Collections Co. Incident Management immediately.
- Authentication server shall be used to authenticate users on wireless network.
- Wireless Network key passwords shall use strong encryption methods.
- All WLAN traffic shall be encrypted to limit eavesdropping and ensure confidentiality.
- Service Set IDs (SSIDs) shall be changed from the factory default to something that is meaningless to outsiders. SSID character strings shall not reflect Member or Committee name, location, or product being used.
- Broadcast mode of SSIDs shall be disabled in products that permit it and configure client's SSID to match that of the access point.
- Placement of access points and channel assignments shall be such that coverage/throughput is maximized while interference is kept to a minimum between different access points or WLANs.
- To keep interference to a minimum, access point channels shall be at least five channels different from all other nearby access points on different WLANs. Some coordination may be required if multiple WLANs are to be used within close proximity.
- Jadarah For Dept Collections Co. wireless network shall be scanned on periodic basis at least once every quarter.
- Wireless networks shall be protected via intrusion detection (IDS) or prevention systems (IPS) and configured to identify any rouge network.
- In case IDS or IPS system is implemented, relative configuration shall be secured and configured to generate appropriate alarms and notification messages to security or network operations centres.
- All incidents from IDS and IPS shall be documented and adhere to Jadarah For Dept Collections Co. Incident management.
- Wireless devices shall only be sent for offsite maintenance after all wireless device configurations have been backed-up, and confidential data has been securely erased.
- Wireless Administrators shall follow the "Operational Administration" procedure for any maintenance activity request.
- Default factory settings shall be restored prior to sending the equipment to maintenance and after testing the backup.

3.6 Desktop Management

- Desktop shall be adequately managed, controlled and, to be protected from threats.
- Desktop devices shall be hardened as per documented and approved hardening procedures or security standards before connecting to the Jadarah For Dept Collections Co.'s production infrastructure.
- Desktop issued to any individual shall remain the property of Jadarah For Dept Collections Co.. When the desktop is allocated to the individual, the user assumes temporary "custodianship" of the desktop.
- Desktop users shall agree to take shared responsibility for the security of their desktop and the information it contains.
- Desktop users shall comply with the password policy.
- Access rights on desktop's operating systems and applications shall be given as per the business requirement.
- User shall not share his/her User ID and Password with any user.

- User authentication and access control shall comply with Jadarah For Dept Collections Co. Identity and Access Management Policy.
- User shall backup critical files by transferring or duplicating files onto the local area network, which shall be backed up on a weekly basis by domain/ system administrator.
- All desktops shall be configured for real time monitoring for abnormal activities like Virus attack, desktop compromise etc.
- Administrator/manager shall report any suspicious activity like virus attack to the respective manager as per the incident management process.
- Domain/System administrator shall ensure that all desktops are at the latest patch-level.
- Domain/System administrator shall deploy all patches, hot-fixes and/or service pack as per the manufacturer recommendation and according to the patch, hot-fix or service pack severity level recommended timeframe.
- In case of any abnormal behaviour while deploying any fix, domain/system administrators shall report the incident to direct manager or manufacturer.
- Domain/System administrator shall submit a detailed activity report for all the successful/unsuccessful patch updates. Report is to be documented as per the Document Management process and sent to the direct manager.
- System Administrator shall secure operating system and any related technology as per the technical controls guidelines.
- Domain/System administrators shall install anti-virus software, keep it updated and configure real-time monitoring.
- Domain/System administrator shall ensure the host-based firewall is installed and configured; as a minimum windows firewall needs to be enabled.
- Domain/System administrator shall ensure that the anti-spyware software is installed and active on all desktops.
- Domain/System administrator shall ensure software licensing requirements are met by obtaining adequate number of licenses for planned use and providing proof of ownership.
- Any change or upgrade request shall be approved by direct manager.
- Domain/System administrators shall take full back up of desktop data and delete all Jadarah For Dept Collections Co. related data before sending the desktop to any out of premises maintenance activity.

3.7 Laptop Management

- Laptops shall be adequately managed, controlled and, to be protected from threats.
- Laptop devices shall be hardened as per documented and approved hardening procedures or security standards before connecting to the Jadarah For Dept Collections Co.’s production infrastructure.
- Laptop issued to any individual shall remain the property of Jadarah For Dept Collections Co.. When the laptop is allocated to the individual, the user assumes temporary "custodianship" of the laptop.
- Laptop users shall agree to take shared responsibility for the security of their laptop and the information it contains.
- Local Administrator Accounts shall be renamed.
- User authentication and access control shall comply with Jadarah For Dept Collections Co. Identity and Access Management Policy.
- User shall backup critical files by transferring or duplicating files onto the local area network, which shall be backed up on a weekly basis by domain/ system administrator.

- All laptops shall be configured for real time monitoring for abnormal activities like Virus attack, laptop compromise etc.
- Administrator/Project manager shall report any suspicious activity like virus attack to the respective manager as per the incident management process.
- Loss or theft of any laptop shall be reported to respective manager immediately.
- Domain/System administrator shall ensure that all laptops are at the latest patch-level.
- Domain/System administrator shall deploy all patches, hot-fixes and/or service pack as per the manufacturer recommendation and according to the patch, hot-fix or service pack severity level recommended timeframe.
- In case of any abnormal behaviour while deploying any fix, domain/system administrators shall report the incident to direct manager or manufacturer.
- Domain/System administrator shall submit a detailed activity report for all the successful/unsuccessful patch updates. Report is to be documented as per the Document Management process and sent to the direct manager.
- All the patch update history shall be documented as per the Document Management Process and Procedures.
- System Administrator shall secure operating system and any related technology as per the technical controls guidelines.
- Domain/System administrators shall install anti-virus software, keep it updated and configure real-time monitoring.
- Domain/System administrator shall ensure the host-based firewall is installed and configured; as a minimum windows firewall needs to be enabled.
- Domain/System administrator shall ensure that the anti-spyware software is installed and active on all laptops.
- Domain/System administrator shall ensure software licensing requirements are met by obtaining adequate number of licenses for planned use and providing proof of ownership.
- Domain/System administrator and Information Owners shall conduct a business needs analysis prior to disposing or retiring any production laptop.
- Any change or upgrade request shall be approved by direct manager.
- Domain/System administrators shall take full backup of laptop data and delete all Jadarah For Dept Collections Co. related data before sending the laptop to any out of premises maintenance activity
- Domain/System administrators shall follow the “Operational Administration” procedure for any maintenance activity request.
- User shall follow Jadarah For Dept Collections Co. acceptable use policy.

3.8 Storage Management

- Backup of essential business information and software shall be taken according to a comprehensive schedule.
- All software shall be copied prior to its initial usage, these master copies shall be stored in a safe and secure location, and these master copies shall not be used for ordinary business activities
- Backup arrangements for individual systems and related data shall be tested according to a formal schedule to ensure that they meet the requirements of business continuity plans.
- This policy applies to all instrumental data under all locations of Jadarah For Dept Collections Co., that cover all types of backup (incremental, full back up, data, operating systems, configuration, etc.,)

- Backup and restoration activity shall be accurate and fast as specified in the recovery time objective (RTO) and recovery point objective (RPO).
- Separate systems specific backup and recovery procedures shall be developed in accordance with system requirements and vendor recommendations. These procedures shall be documented and implemented during (and as part of) system implementation, and updated afterwards from time to time by the system administrator.
- Up-to-date documentation of backup and restoration process is crucial to ensure the backup and restore process are implemented accurately and consistently.
- Backup/restore verification practice is required to ensure that Jadarah For Dept Collections Co. has adequate and reliable data protection.
- It shall be considered integrating backup process with change management process to facilitate the rollback plan in the middle of change process.
- Backed-up confidential data shall be stored safely to protect it against unauthorized read access.
- The frequency of data backup for each system shall be determined by considering the 'Availability' and 'Integrity' criteria in accordance with Jadarah For Dept Collections Co. Information Classification and Asset Management Process.
- Data disaster recovery (DR) shall be considered, and backup shall be integrated with DR plan utilizing DR site to protect Jadarah For Dept Collections Co. data in case of disaster.
- Group of users, systems, applications shall be adequately segregated through creation of Virtual LANs, to prevent unauthorized access; and
- Appropriate logical segregation shall be done between and within IT, Network, and Physical Security infrastructures through creation of zones. Traffic flows between different zones shall be documented.