



Information Security Policy Manual

Abstract

Information Security Policy document has been developed to clearly articulate management expectations towards implementing and maintaining information security



Copyright of the manual

This manual, including all its content, text, images, graphics, and any other materials is the property of Al Tijaria and is protected by copyright law. Unauthorized reproduction, distribution, or transmission of any portion of this Manual, in any form or by any means, without prior written permission from the CEO is strictly prohibited. Any violation of this copyright notice may result in legal action and other remedies available under applicable copyright laws.



Contents

I.	Document Control	6
II.	Key Abbreviations.....	7
1.	Introduction.....	8
1.1	Purpose and Scope	8
1.2	Compliance with information security policy.....	9
1.3	Technical Compliance.....	9
1.4	Responsibility.....	10
1.5	Monitoring & Review.....	13
1.6	Policy Violation	13
1.7	Policy Exceptions	13
1.8	Policy Approval.....	13
2.	Acceptable Usage	14
2.1	Purpose.....	14
2.2	Audience.....	14
2.3	General Policy.....	14
2.4	Access Management Policy	15
2.5	Authentication/Passwords Policy.....	15
2.6	Clear Desk / Clear Screen Policy	16
2.7	Data Security Policy	16
2.8	Email and Electronic Communication Policy	17
2.9	Hardware and Software Policy	17
2.10	Internet Policy	18
2.11	Mobile Devices and Bring Your Own Device (BYOD) Policy.....	18
2.12	Physical Security Policy.....	19
2.13	Privacy Policy	19
2.14	Removable Media Policy	19
2.15	Security Training and Awareness Policy	20
2.16	Social Media Policy	20
2.17	Voicemail Policy.....	20
2.18	Incidental Use Policy.....	21
3.	Information security & IT Operations Management	22



3.1	Change Control	22
3.2	Segregation of Duties	23
3.3	Separation of development, test and production facilities.....	24
3.4	Capacity Planning	24
3.5	Control of technical vulnerabilities	25
3.6	Virus Protection.....	25
3.7	Software Security	26
3.8	Anti-Malware Protection.....	27
3.9	Protection against malicious code threats	27
3.10	Information Backup	28
3.11	Exchange of information	28
3.12	Physical Media in Transit.....	29
3.13	Electronic messaging and internet security	29
3.14	Audit Logging & Monitoring	30
3.15	Security Event Logging & Monitoring.....	31
3.16	Operator Logs	31
3.17	Fault Logging.....	31
3.18	Clock Synchronization.....	32
3.19	Servers	32
3.20	Network Segregation.....	32
3.21	Network Controls	33
3.22	Network Equipment Authentication	34
3.23	Remote Diagnostic and Configuration Port Protection.....	34
3.24	Wireless Network Security	35
3.25	Mobile Computing Devices.....	35
3.26	Use of Cryptographic Controls.....	36
3.27	Public Key Infrastructure	36
3.28	Security Devices and Software	37
3.29	Devices Maintenance	37
3.30	Cyber Security.....	38
4.	Logical Access Security Management.....	39
4.1.	User Access Management	39



4.2.	Secure Log-On	39
4.3.	Privilege Management	40
4.4.	Password Settings & Management	41
4.5.	Administrative Password Use	41
4.6.	Session Time-Out.....	42
4.7.	Directory Management	42
4.8.	Review of User Access Rights	42
4.9.	Authentication of external connections.....	43
4.10.	Information Access Restriction.....	43
5.	Human Resources Security.....	44
5.1.	Enforcement of information Security Policies.....	44
5.2.	Personnel & Candidate Screening	45
5.3.	Disciplinary Process	45
6.	Information Security Incident Management	46
6.1.	Reporting Incidents & Events	46
6.2.	Reporting Security Weaknesses	46
6.3.	Information Security Incident Management Planning	47
6.4.	Responsibilities & Procedures	48
6.5.	Information Security Incident Training & Simulation.....	48
6.6.	Management of Security Incident Responses	49
6.7.	Management of Security Evidence.....	49
6.8.	Post-Incident Analysis, Reporting, and Corrective Action.....	49
7.	Asset Management.....	50
7.1.	Inventory of Assets	50
7.2.	Information Assets Classification	50
7.3.	Retention & Disposal of Information.....	50
7.4.	Management of Removal Media	51
8.	Third-Party Supplier Management	51
8.1.	Identification of Third-Party supplier Requirements.....	51
8.2.	Security-Oriented Supplier Selection	52
8.3.	Managing Third-Party Suppliers Agreements	52
8.4.	Managing Third-Party Suppliers Access	53



8.5.	Third-Party Service Delivery	53
8.6.	Monitoring & Review of Third-Party Services	54
8.7.	Managing changes to Third-Party Services	54
9.	Data Protection and privacy	54
9.1.	Electronic Messaging	55
9.2.	Protection of test data.....	55
9.3.	Privacy and protection of personally identifiable information	55
10.	Secure Design, Development & Testing of Services	55
10.1.	Information System Design & Development	55
10.2.	Information Systems Testing & Implementation	56
10.3.	Control of Operational Software	57
10.4.	Security of Program Source Code	57
10.5.	Software Packages.....	58
10.6.	Security of System Documentation	58
11.	Service Continuity & Availability Management.....	59
11.1.	Service Continuity & Availability Requirements.....	59
11.2.	Service Continuity and Availability Plans.....	59
11.3.	Information Security in Business Continuity Management.....	60
12.	Security Training & Awareness.....	60
12.1.	Information Security Induction	60
12.2.	General Information Security Awareness	61
12.3.	Information Security Education and training Curriculum	61



I. Document Control

Version	Date

Approved by	
Controller	
Custodian	



II. Key Abbreviations

No.	Term	Definition
1.	LAN	Local Area Network
2.	IT	Information Technology
3.	HR	Human Resource
4.	BU	Business Unit
5.	ISS	Information Security section



1. Introduction

1.1 Purpose and Scope

- 1.1.1 Al-TIJARIA Information Security Policy document has been developed to clearly articulate management expectations towards implementing and maintaining information security and the rules that shall be followed to improve the company information security posture
- 1.1.2 The purpose of this policy is to provide direction to preserve the confidentiality, integrity, and availability of information and all supporting business processes, systems and applications.
- 1.1.3 The objective of this policy is to describe the formal set of rules and directions to adhere to in order to protect Al-TIJARIA's information assets from threats whether internal or external, deliberate or accidental. This document addresses the security methods to protect Al-TIJARIA's information assets, including:
- Information held and processed by Al-TIJARIA on behalf of users or for internal purposes.
 - Information held and processed by a third party on behalf of Al-TIJARIA (such as vendors providing technology services with access to Al-TIJARIA systems or vendors to whom business processes are outsourced).
 - Information technology and systems.
 - Al-TIJARIA's personnel.
 - Buildings, facilities, premises, and other properties owned or occupied by Al-TIJARIA.
 - Al-TIJARIA's intellectual capital.
 - Al-TIJARIA's reputation, credibility, and viability.
- 1.1.4 Al-TIJARIA's Information Security Policy document provides direction for all users at Al-TIJARIA's head office (full time, part time, or contractors), Business Units (BUs), and related sites. All users shall follow the instructions provided by these policies to achieve Al-TIJARIA's goals and requirements for the protection of Al-TIJARIA's information assets. This policy applies to all systems owned by and/or administered by Al-TIJARIA personnel, as well as to all systems operated by a third party for the benefit of the company.
- 1.1.5 This Policy is supplemented by a list of other Security Policies developed and maintained by Information Security to address security requirements on various information security areas. These Policies may be supported by various Standards, Processes, Procedures and Guidelines defined to meet the Policy requirements by various departments to provide user directions for user adherence in their day-to-day operations.



1.2 Compliance with information security policy

- 1.2.1 Successful implementation of AL-TIJARIA's Information Security Policies cannot be achieved without the cooperation of all users in AL-TIJARIA. It is imperative to the preservation of a culture of information security that all users are aware of and fully comply with, the security requirements defined within AL-TIJARIA's Information Security Policy document at all times.
- 1.2.2 This policy will be published and circulated within AL-TIJARIA's where employees will be able to read and understand the policies applicable to them.
- 1.2.3 Business Owners within their jurisdiction shall ensure that all employees, contractors and third parties adhere to the information security policy and procedure.
- 1.2.4 All users (employees, contractors, and consultants) shall understand and acknowledge the responsibility towards complying with AL-TIJARIA's Information Security Policy.
- 1.2.5 All users shall acknowledge (e.g. either electronically through email or login banner or manually by signing a formal contract/form) that they will comply with all AL-TIJARIA policies and that any noncompliance or misuse of information processing facilities may result in a compliance breach.
- 1.2.6 Business Owners shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with AL-TIJARIA's Information Security Policy, Procedure, and Standards.

1.3 Technical Compliance

- 1.3.1 Technical reviews shall include compliance with technical policies, procedures, and standards.
- 1.3.2 Any review or technical compliance check shall only be carried out by competent, authorized persons, or under the supervision of such persons. The person shall be an experienced individual who may conduct the review with the assistance of automated tools, generating a technical report for subsequent interpretation by a technical specialist.
- 1.3.3 Results of reviews and the corresponding corrective actions should be recorded and maintained.



1.4 Responsibility

1.4.1 Risk & Audit Committee / BOARD OF DIRECTORS

- Sponsorship of Security Management and Awareness in the company in a way that enhances and maintains information confidentiality, Integrity & Availability.
- Ensure the Effective Management and Monitoring of information security.
- Approve Information Security Policy and other supporting Security Policies & Framework.

1.4.2 Risk Management / CEO Technical Affairs

- Improve security awareness through appropriate communication of security policies and practices.
- Maintain and control the confidentiality, integrity and availability of AL-TIJARIA's information, systems, and applications.
- Minimizing AL-TIJARIA's exposure to the risks arising due to loss, corruption, alteration, misuse or theft of information.
- Adherence of AL-TIJARIA's legal, regulatory obligations, and risk management framework.
- Ensuring consistency, coordination and communication of all related information security initiatives across the AL-TIJARIA's business and technology units.
- Ensure that necessary support is provided across the Company in implementation of Information Security Policies among the AL-TIJARIA employees including third-party vendors and contractors.



1.4.3 INFORMATION SECURITY SECTION

- Develop and maintain the AL-TIJARIA's Information Security Policy, supporting Security Policies, Standards, and Guidelines.
- Approve all Information Security Standards and Guidelines.
- Monitor compliance with this policy and supporting policies to ensure that they address AL-TIJARIA's security requirements.
- Providing assurance to Management that information security is effective, that it addresses the identified risks and is compliant with the defined information security standards.
- Ensuring access to IT Infrastructure; including but not limited to servers, networks and application systems; user roles and access permission are following information security policies.
- Coordinate with business units to ensure that the access permission given to the users are on a "need to know" basis and in accordance with the job roles.
- Monitoring and reviewing practices and mechanisms to compliance with established policy.
- Perform vulnerability assessments on IT systems and develop risk mitigation strategies in coordination with Risk Management.
- Investigate, report and initiate appropriate actions for information security violations and incidents to senior management.
- Guide and advise on the design and implementation of information security requirements.
- Conduct appropriate information security awareness programs covering all users.

1.4.4 HEAD OF INFORMATION TECHNOLOGY

- Designing, developing and applying effective security measures, throughout each system's lifecycle, to ensure systems & applications meet the defined security policies and standards.
- Ensuring that the IT system(s) are managed and operated in accordance with the defined information security standards and guidelines.
- An inventory of AL-TIJARIA's IT assets shall be recorded, maintained and reviewed on a periodic basis.
- Ensuring the overall development of IT disaster recovery plans are undertaken and include the possible scenarios related to cyber incidents.
- Report Security policy non-compliance and information security incidents.



1.4.5 HR Manager

- Personnel Security including the vetting and briefing of new staff and contractors.
- Advise the respective departments including Information Security section about the personnel movements/transfer between business groups.
- Advise and communicate information relevant to the need for the de-activation of both physical and logical access authorities for staff and contractors who no longer need access.
- Organize information security awareness training for the staff and contractors in coordination with the Information Security section.
- Performing the disciplinary actions in accordance with the inquiry and Disciplinary policy.
- Implement the necessary controls to secure physical and environmental related risks.

1.4.6 BUSINESS AREAS HEADS

- Take reasonable and cost-effective steps within the scope of their responsibility and authority to preserve the availability, integrity and confidentiality of information.
- Understanding the security risks affecting their business area. Assume responsibility for security risks related to their business areas and developing requirements based on the mitigation strategies developed by the Information security officer to secure critical business information.
- Accept any residual risks where the security controls are not feasible to implement.
- Communicate information security policy and supporting policies to the personnel under their authority and ensuring effective implementation within their business areas.

1.4.7 AL-TIJARIA EMPLOYEES

- Comply with this policy and all applicable supporting policies & procedures within their business area and day to day operations.
- Ensure no unauthorized disclosure of AL-TIJARIA's customer and business information during and after the employment term with AL-TIJARIA.
- Use only AL-TIJARIA authorized software and systems.
- Report Information security incidents to reporting managers and Information Security, including non-compliance by colleagues.



1.5 Monitoring & Review

This policy will be reviewed annually as part of an overall management review of the effectiveness of AL-TIJARIA's information security management. The policy will also be reviewed in response to significant changes due to security incidents and/or changes to organizational or technical infrastructure.

1.6 Policy Violation

- All personnel must read, understand and adhere to the contents of this policy and all applicable supporting security policies.
- Any personnel who violates the Information Security Policy and any supporting security policies, or who knowingly or negligently allow personnel under their supervision to do so, would be liable to disciplinary action in accordance with AL-TIJARIA's Human Resources disciplinary process.
- Unauthorized disclosure of AL-TIJARIA's customer information shall entail legal action against the user under Kuwaiti Law.

1.7 Policy Exceptions

All exceptions to the policy shall be reviewed by ISS and raised to Risk Management / CEO Technical Affairs/ Risk & Audit Committee depending upon the nature of security exception. All exceptions shall be approved by CEO Technical Affairs.

1.8 Policy Approval

Information Security Policy shall be approved by AL-TIJARIA's Board of Directors.



2. Acceptable Usage

2.1 Purpose

The purpose of the AL-TIJARIA Acceptable Use Policy is to establish acceptable practices regarding the use of AL-TIJARIA Information Resources in order to protect the confidentiality, integrity and availability of information created, collected, and maintained.

2.2 Audience

The AL-TIJARIA Acceptable Use Policy applies to any individual, entity, or process that interacts with any AL-TIJARIA Information Resource.

2.3 General Policy

- Personnel are responsible for complying with AL-TIJARIA policies when using AL-TIJARIA information resources and/or on AL-TIJARIA time. If requirements or responsibilities are unclear, please seek assistance from the ISS.
- In adherence to our commitment to comprehensive data protection practices, this Information Security Policy shall be applied in conjunction with the Data Classification Policy. The Data Classification Policy provides guidelines for categorizing data based on its sensitivity and importance, which in turn informs the appropriate security measures outlined in this policy. Both policies are integral components of our overarching data security framework and shall be implemented and maintained consistently across all organizational functions.
- Personnel must promptly report the theft, loss, or unauthorized disclosure of AL-TIJARIA confidential or internal information to the Information Security section.
- Personnel should not purposely engage in activity that may
 - harass, threaten, or abuse others;
 - degrade the performance of AL-TIJARIA Information Resources;
 - deprive authorized AL-TIJARIA personnel access to AL-TIJARIA Information Resource;
 - obtain additional resources beyond those allocated;
 - or circumvent AL-TIJARIA computer security measures.
- Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, AL-TIJARIA personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any AL-TIJARIA Information Resource. **Except for IT administrators.**
- All inventions, intellectual property, and proprietary information, including reports, drawings, blue prints, software codes, computer programs, data, writings, and technical information, developed on AL-TIJARIA time and/or using AL-TIJARIA Information Resources are the property of AL-TIJARIA.
- Use of encryption should be managed in a manner that allows designated AL-TIJARIA personnel to promptly access all data.
- AL-TIJARIA Information Resources are provided to facilitate District business and should not be used for personal financial gain.



- Personnel are expected to cooperate with incident investigations
- Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using AL-TIJARIA Information Resources.



- Personnel should not intentionally access, create, store or transmit material which AL-TIJARIA may deem to be offensive, indecent, or obscene.

2.4 Access Management Policy

- Access to information is based on a “need to know”.
- Personnel are permitted to use only those network and host addresses issued to them by AL-TIJARIA IT and should not attempt to access any data or programs contained on AL-TIJARIA systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal AL-TIJARIA networks and/or environments must be made through approved, and AL-TIJARIA-provided, virtual private networks (VPNs).
- Personnel should not divulge any access information to anyone not specifically authorized to receive such information.
- Personnel must not share their AL-TIJARIA authentication information, including:
 - Account passwords,
 - Personal Identification Numbers (PINs),
 - Security Tokens (i.e. Smartcard),
 - Access cards and/or keys,
 - Digital certificates,
 - Similar information or devices used for identification and authentication purposes.
- Lost or stolen access cards, security tokens, and/or keys must be reported to the person responsible for Information Resource physical facility management as soon as practical.
- A service charge may be assessed for access cards, security tokens, and/or keys that are lost, stolen, or are not returned.

2.5 Authentication/Passwords Policy

- All personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed, and implemented according to the following AL-TIJARIA rules:
 - Must meet all requirements established in the AL-TIJARIA Authentication Standard, including minimum length, complexity, and rotation requirements.
 - Must not be easily tied back to the account owner by using things like: user name, social security number, nickname, relative’s names, birth date, etc.
 - Should not include common words, such as using dictionary words or acronyms.
 - Should not be the same passwords as used for non-business purposes.
 - Password history must be kept to prevent the reuse of passwords.
 - Unique passwords should be used for each system, whenever possible.
 - User account passwords must not be divulged to anyone. AL-TIJARIA support personnel and/or contractors should never ask for user account passwords.
 - Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with AL-TIJARIA, if issued.



- If the security of a password is in doubt, the password should be changed immediately.
- Personnel should not circumvent password entry with application remembering, embedded scripts or hard coded passwords in client software.

2.6 Clear Desk / Clear Screen Policy

- Personnel should log off from applications or network services when they are no longer needed.
- Personnel should log off or lock their workstations and laptops when their workspace is unattended.
- Confidential or internal information should be removed or placed in a locked drawer or file cabinet when the workstation is unattended and at the end of the workday if physical access to the workspace cannot be secured by other means.
- Personal items, such as phones, wallets, and keys, should be removed or placed in a locked drawer or file cabinet when the workstation is unattended.
- File cabinets containing confidential information should be locked when not in use or when unattended.
- Physical and/or electronic keys used to access confidential information should not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
- Laptops should be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday if the laptop is not encrypted.
- Passwords must not be posted on or under a computer or in any other physically accessible location.
- Copies of documents containing confidential information should be immediately removed from printers and fax machines.

2.7 Data Security Policy

- Personnel should use approved encrypted communication methods whenever sending confidential information over public computer networks (Internet).
- Confidential information transmitted via mail service must be secured in compliance with the [Information Assets Classification](#) Policy.
- Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
- Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity.
- Personnel should not have confidential conversations in public places or over insecure communication channels, open offices, and meeting places.
- Confidential information must be transported either by an AL-TIJARIA employee or a courier approved by IT Management.
- All electronic media containing confidential information must be securely disposed. Please contact IT for guidance or assistance.



2.8 Email and Electronic Communication Policy

- Auto-forwarding electronic messages outside the AL-TIJARIA internal systems is prohibited.
- Electronic communications should not misrepresent the originator or AL-TIJARIA.
- Personnel are responsible for the accounts assigned to them and for the actions taken with their accounts.
- Accounts must not be shared without prior authorization from AL-TIJARIA IT, with the exception of calendars and related calendaring functions.
- Employees should not use personal email accounts to send or receive AL-TIJARIA confidential information.
- Any personal use of AL-TIJARIA provided email should not:
 - Involve solicitation.
 - Have the potential to harm the reputation of AL-TIJARIA.
 - Forward chain emails.
 - Contain or promote anti-social or unethical behavior.
 - Result in unauthorized disclosure of AL-TIJARIA confidential information.
- Personnel should only send confidential information using secure electronic messaging solutions.
- Personnel should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
- Personnel should use discretion in disclosing confidential or internal information in Out of Office or other automated responses, such as employment data, internal telephone numbers, location information or other sensitive data.

2.9 Hardware and Software Policy

- All hardware must be formally approved by IT Management before being connected to AL-TIJARIA networks.
- Software installed on AL-TIJARIA equipment must be approved by IT Management and installed by AL-TIJARIA IT personnel.
- All AL-TIJARIA assets taken off-site should be physically secured at all times.
- Personnel traveling to a High-Risk location, as defined by Kuwaiti government, must contact IT for approval to travel with corporate assets.
- Employees should not allow family members or other non-employees to access AL-TIJARIA Information Resources.



2.10 Internet Policy

- The Internet must not be used to communicate AL-TIJARIA confidential or internal information, unless the confidentiality and integrity of the information is ensured and the identity of the recipient(s) is established.
- Use of the Internet with AL-TIJARIA networking or computing resources must only be used for business-related activities. Unapproved activities include, but are not limited to:
- Recreational games,
- Streaming media,
- Personal social media,
- Accessing or distributing pornographic or sexually oriented materials,
- Attempting or making unauthorized entry to any network or computer accessible from the Internet.
- Access to the Internet from outside the AL-TIJARIA network using a AL-TIJARIA owned computer must adhere to all of the same policies that apply to use from within AL-TIJARIA facilities.

2.11 Mobile Devices and Bring Your Own Device (BYOD) Policy

- AL-TIJARIA does not allow personally-owned mobile devices to connect to the AL-TIJARIA corporate internal network.

OR

- The use of a personally-owned mobile device to connect to the AL-TIJARIA network is a privilege granted to employees only upon formal approval of IT Management.
- All personally-owned laptops and/or workstations must have approved virus and spyware detection/protection software along with personal firewall protection active.
- Mobile devices that access AL-TIJARIA email must have a PIN or other authentication mechanism enabled.
- Confidential data should only be stored on devices that are encrypted in compliance with the AL-TIJARIA Encryption Standard.
- AL-TIJARIA confidential information should not be stored on any personally-owned mobile device.
- Theft or loss of any mobile device that has been used to create, store, or access confidential or internal information must be reported to the AL-TIJARIA Security Team immediately.
- All mobile devices must maintain up-to-date versions of all software and applications.
- All personnel are expected to use mobile devices in an ethical manner.
- Jail-broken or rooted devices should not be used to connect to AL-TIJARIA Information Resources.
- AL-TIJARIA IT Management may choose to execute “email remote wipe” capabilities for mobile devices without warning.
- In the event that there is a suspected incident or breach associated with a mobile device, it may be necessary to remove the device from the personnel’s possession as part of a formal investigation.
- All mobile device usage in relation to AL-TIJARIA Information Resources may be monitored, at the discretion of AL-TIJARIA IT Management.
- AL-TIJARIA IT support for personally-owned mobile devices is limited to assistance in complying with this policy. AL-TIJARIA IT support may not assist in troubleshooting device usability issues.
- Use of personally-owned devices must be following all other AL-TIJARIA policies.



- AL-TIJARIA reserves the right to revoke personally-owned mobile device use privileges in the event that personnel do not abide by the requirements set forth in this policy.
- Texting or emailing while driving is not permitted while on District time or using AL-TIJARIA resources. Only hands-free talking while driving is permitted, while on District time or when using AL-TIJARIA resources.

2.12 Physical Security Policy

- Photographic, video, audio, or other recording equipment, such as cameras in mobile devices, is not allowed in secure areas.
- Personnel must display photo ID access card at all times while in the building.
- Personnel must badge in and out of access-controlled areas. Piggy-backing, door propping and any other activity to circumvent door access controls are prohibited.
- Visitors accessing card-controlled areas of facilities must be accompanied by authorized personnel at all times.
- Eating or drinking are not allowed in data centers. Caution must be used when eating or drinking near workstations or information processing facilities.

2.13 Privacy Policy

- Information created, sent, received, or stored on AL-TIJARIA Information Resources are not private and may be accessed by AL-TIJARIA IT employees at any time, under the direction of AL-TIJARIA executive management and/or Human Resources, without knowledge of the user or resource owner.
- AL-TIJARIA may log, review, and otherwise utilize any information stored on or passing through its Information Resource systems.
- Systems Administrators, AL-TIJARIA IT, and other authorized AL-TIJARIA personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges should not access files and/or other information that is not specifically required to carry out an employment related task.

2.14 Removable Media Policy

- The use of removable media for storage of AL-TIJARIA information must be supported by a reasonable business case.
- All removable media use must be approved by AL-TIJARIA IT prior to use.
- Personally-owned removable media use is not permitted for storage of AL-TIJARIA information.
- Personnel are not permitted to connect removable media from an unknown origin without prior approval from the AL-TIJARIA IT.
- Confidential and internal AL-TIJARIA information should not be stored on removable media without the use of encryption.
- The loss or theft of a removable media device that may have contained AL-TIJARIA information must be reported to the AL-TIJARIA IT.



2.15 Security Training and Awareness Policy

- All new personnel must complete an approved security awareness training class prior to, or at least within 30 days of, being granted access to any AL-TIJARIA Information Resources.
- All personnel must be provided with and acknowledge they have received and agree to adhere to the AL-TIJARIA Information Security Policies before they are granted to access to AL-TIJARIA Information Resources.
- All personnel must complete annual security awareness training.

2.16 Social Media Policy

- Communications made with respect to social media should be made in compliance with all applicable AL-TIJARIA policies.
- Personnel are personally responsible for the content they publish online.
- Creating any public social media account intended to represent AL-TIJARIA, including accounts that could reasonably be assumed to be an official AL-TIJARIA account, requires the permission of the AL-TIJARIA Communications Departments.
- When discussing AL-TIJARIA or AL-TIJARIA -related matters, you should:
 - Identify yourself by name,
 - Identify yourself as an AL-TIJARIA representative, and
 - Make it clear that you are speaking for yourself and not on behalf of AL-TIJARIA, unless you have been explicitly approved to do so.
- Personnel should not misrepresent their role at AL-TIJARIA.
- When publishing AL-TIJARIA-relevant content online in a personal capacity, a disclaimer should accompany the content. An example disclaimer could be; “The opinions and content are my own and do not necessarily represent AL-TIJARIA’s position or opinion.”
- Content posted online should not violate any applicable laws (i.e. copyright, fair use, financial disclosure, or privacy laws).
- Confidential information, internal communications and non-public financial or operational information may not be published online in any form.
- Personal information belonging to customers may not be published online.
- Personnel approved to post, review, or approve content on AL-TIJARIA social media sites must follow the AL-TIJARIA Social Media Procedures.

2.17 Voicemail Policy

- Personnel should use discretion in disclosing confidential or internal information in voicemail greetings, such as employment data, internal telephone numbers, location information or other sensitive data.



2.18 Incidental Use Policy

- As a convenience to AL-TIJARIA personnel, incidental use of Information Resources is permitted. The following restrictions apply:
- Incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, and so on, is restricted to AL-TIJARIA approved personnel; it does not extend to family members or other acquaintances.
- Incidental use should not result in direct costs to AL-TIJARIA.
- Incidental use should not interfere with the normal performance of an employee's work duties.
- No files or documents may be sent or received that may cause legal action against, or embarrassment to, AL-TIJARIA or its customers.
- Storage of personal email messages, voice messages, files and documents within AL-TIJARIA Information Resources must be nominal
- All information located on AL-TIJARIA Information Resources are owned by AL-TIJARIA may be subject to open records requests and may be accessed in accordance with this policy.



3. Information security & IT Operations Management

3.1 Change Control

Purpose

The purpose of the Change Control Policy is to establish the rules for the creation, evaluation, implementation, and tracking of changes made to AL-TIJARIA Information Resources.

Audience

1. The Change Control Policy applies to any individual, entity, or process that create, evaluate, and/or implement changes to AL-TIJARIA Information Resource.

Policy

- Changes to production AL-TIJARIA Information Resources must be documented and classified according to their:
 - Importance.
 - Urgency.
 - Impact.
- Change documentation must include, at a minimum:
 - Date of submission and date of change,
 - Owner and custodian of change,
 - Nature of the change,
 - Change requestor,
 - Change classification(s),
 - Roll-back plan,
 - Change approver,
 - Change implementer, and
 - An indication of success or failure.
- Changes with a significant potential impact to Information Resources on production must be scheduled.
- Information Resource owners must be notified of changes that affect the systems they are responsible for.
- Authorized change windows must be established for changes with a high potential impact.
- Changes with a significant potential impact and/or significant complexity must have usability, security, and impact testing and back out plans included in the change documentation.
- Change control documentation must be maintained in accordance with the Information Retention Schedule.



- All changes must be approved by the Business Owner, Manager of Information Technology, or Change Control Board.
- Emergency changes that require an immediate implementation (i.e. break/fix, incident response, etc.) may be implemented without following the formal change control process, but may not circumvent documentation requirements, even if documented after the change.

3.2 Segregation of Duties

- Authorizing/requesting parties shall not be the same as the parties able to execute the action in order to ensure a good internal control system as well as to minimize the risk of negligent or deliberate system misuse. The responsibility of ensuring adequate segregation of duties shall belong to Section Managers and/or Service Owners. Activities and positions that strictly require segregation of duties shall, at a minimum, include:
 - A. Updating master files & parameter files.
 - B. Approval and entry of payments in any financial system.
 - C. Reconciliation of financial transactions.
 - D. Financial reporting.
 - E. System administration.
 - F. Security audit.
 - G. Systems development & maintenance.
- In situations where segregation of duties is not possible, further compensating controls shall be implemented.
- Management must ensure that proper segregation of duties applies to all areas dealing with system development, system operation or systems administration.



3.3 Separation of development, test and production facilities

- Development and test environments must be at least logically isolated from each other with defined information security controls to ensure their respective integrity.
- Testers and developers shall not have user IDs on production systems (excluding firewall user IDs which are only enabled for use by authorized IT to support employees for specific support purposes). A standard user or superuser IDs shall be created for developers and testers if access is required after the development and testing of information systems.
- Testers and developers shall have access to only those parts of information systems that are required for their job. Access to these areas shall be revoked before the system is brought to the production environment.
- Production data shall only be available on production systems. Development and testing shall use dummy data wherever possible. If production data must be used, fields containing highly sensitive data must first be masked.
- The test environment shall have similar configurations to the corresponding production environment so that results and impact on the production environment can be analyzed accurately.
- Data from one environment shall not be migrated to another environment without the formal approval of the Service Owner & Information Security section.
- On-screen messages or screen colors shall clearly indicate whether a system is a test or production instance to minimize the risk of accidental submission of test transactions on production systems.
- IT has to periodically review the above controls and inform Information Security section in case of non-compliance.

3.4 Capacity Planning

- Information Security section shall monitor and tune its use of resources. ISS shall project future capacity requirements of its information security related resources, based on business criticality, to ensure the required system performance.



3.5 Control of technical vulnerabilities

- Timely information about technical vulnerabilities of information systems being used shall be obtained, exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken to accept or address the associated risks.
- IT Infrastructure and Operations in conjunction with the Information security officer, shall be responsible for vulnerability monitoring, risk assessment, patching, asset tracking, and coordination.
- IT Infrastructure and Operations shall be responsible for maintaining adequate information sources for technical vulnerabilities including IT vendors and various trusted third-party suppliers.
- Depending on the risk and hence urgency, normal change management, emergency change or information security incident response procedures shall be followed in the event technical vulnerabilities are identified.
- A patch shall only be applied to remediate a technical vulnerability after it has been assessed for the associated risks of installing it by the Service Owner. If installing patch introduces new risks, other compensating controls shall be applied.
- The patches shall only be obtained from trusted sources and, if the requirement is not urgent, patches should be applied in batches.
- An automated vulnerability and compliance scanning tool shall be implemented for the immediate detection and remediation, or this function could be outsourced to be executed on periodic basis.

3.6 Virus Protection

- Approved antivirus software shall be installed by the IT Department on applicable IT platforms. The software must be configured for optimum protection and updated promptly when updates to the virus database and protection mechanisms are released.
- Email messages and attachments must be routinely and automatically checked for malicious software before being opened.
- Desktops & laptops must have up-to-date antivirus software installed.



3.7 Software Security

- Requirements for new/additional software shall be approved by the relevant Department Manager where the software is requested. This includes all forms of software programs such as commercial software, operating system software, utilities, shareware and freeware, and evaluation software.
- Any new Software installation on AL-TIRJARIA's systems shall be authorized by the IT Department & Information Security section. Installation of unauthorized software is prohibited. The IT Department shall review and evaluate the requested software to ensure compatibility, and the Information security officer shall verify that the software will not introduce security vulnerabilities or increase security threats.
- Emerging malicious software threats and other security threats shall be identified by the Information security officer and IT Infrastructure and Operations through reliable resources such as trusted information security and technology-related websites and professional journals and advice on applying appropriate security controls.
- A Definitive Software Library (DSL) by the IT Service Desk upon consultation with the Information Security Department shall be maintained by IT with each entry corresponding to an entry in the software catalog. Backup of DSL shall also be maintained.
- Images of software in DSL shall be obtained from verified sources and must be security-tested.
- Only approved networks and IT Infrastructure and Operations Administrators shall have access to DSL, and logs shall be maintained for it.
- The status of information systems shall be maintained up-to-date in the software catalog by IT and should validate by ISS through conducting regular scans, at least on a quarterly basis.
- The software images in DSL shall be managed properly and retired software versions shall only be removed after confirmation has been received that they are no longer required.
- Only designated staff may access operational program & program source libraries. Amendments may only be made using a combination of technical access control and robust procedures operated under dual control.
- Emergency amendments to the software are to be discouraged, except in circumstances previously designated by management as 'critical'. Any such amendments must strictly follow the agreed change control process.



3.8 Anti-Malware Protection

- The devices at the core network's boundary shall be configured in such a way that they will not allow malware to propagate out of the network.
- Anti-malware solutions shall be obtained and deployed from multiple vendors so as to be safe from malware that might not be detected by other malware scanning tool.
- Removable media must be scanned for malware before any information is transferred to them.
- Any infected information system, device or network must be isolated immediately.
- A report shall be produced which will give details about the performance of implemented anti-malware solution.
- A master system image of relevant critical systems shall be maintained so that it can be used to restore the system in case malware cannot be removed.

3.9 Protection against malicious code threats

- The information security threats associated with malicious code shall be identified, assessed and, where necessary, mitigated.
- Procedures must be developed and implemented to address malicious code.
- Regular security updates about malicious code vulnerabilities shall be monitored by IT Infrastructure and Operations and periodically reported to the Information security officer who shall decide required corresponding actions.
- Unauthorized malicious code must be blocked from download and/or execution. The information systems shall be designed in such a way that they generate warning messages before the authorized code is executed.
- Execution of legitimate malicious code shall be limited to logically isolated environments (e.g. JavaScript).



3.10 Information Backup

- AL-TIJARIA shall establish a backup procedure to define retention and protection requirements for backup and take backup copies of information, software, and system images.
- Information system owner must ensure that adequate backup and system recovery procedures are in place.
- Backup of the Company's data files and the ability to recover such data is a top priority. Data owner and management are responsible for ensuring that the frequency of such backup operations and the procedure for recovery meet the needs of the business.
- The storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must be carefully considered and documented, especially where proprietary formats are involved.
- The archiving of electronic data files must reflect the needs of the business, legal and regulatory requirements.
- Management must ensure that safeguards are in place to protect the integrity of data files during the recovery and restoration of data files.

3.11 Exchange of information

- Exchanged information must be suitably protected from interception, copying, modification, misrouting and destruction according to the classification level and risk of compromise.
- Electronic communication facilities must be used in accordance with applicable guidelines and acceptable use policies (Also refer to Acceptable Use.).
- Suitable cryptographic techniques must be used to protect the confidentiality, integrity, and authenticity of exchanged information in accordance with the information
- Exchanged information must be suitably protected from interception, copying, modification, misrouting and destruction according to the classification level and risk of compromise.
- Electronic communication facilities must be used in accordance with applicable guidelines and acceptable use policies (Also refer to Acceptable Usage).
- Suitable cryptographic techniques must be used to protect the confidentiality, integrity, and authenticity of exchanged information in accordance with the information classification. Where cryptographic techniques cannot be used, compensating controls shall be implemented.
- Information exchange agreements shall be established for exchanging information and software between AL-TIJARIA and other organizations. Information exchange agreements shall describe:
 - a) Confidentiality and liability clauses in contractual agreements to limit AL-TIJARIA's accountability for information leakage caused by security failures at other organizations.



- b) Escrow arrangements e.g. to secure source code in case a software vendor becomes bankrupt, loses key staff or is otherwise incapable of providing the necessary level of support.
- c) Information and software ownership and responsibilities for data protection and software copyright compliance.

- Information system interconnection agreements must be approved by the appropriate senior management.
- The person responsible for Human Resources Management is to ensure that all employees are fully aware of their legal and corporate duties and responsibilities concerning the inappropriate sharing and releasing of information, both internally within the organization and external parties.

3.12 Physical Media in Transit

- Reliable transport or couriers must be used to transport physical media between the company premises and other locations. A list of authorized couriers must be agreed with senior management. The transporter shall be required to contractually commit to protecting the removable media and information on it from being accessed, copied or stolen.
- Media packaging must be sufficient to protect the contents from physical damage during transit and in accordance with manufacturers' specifications (e.g. purpose-made lockable tape carriers).
- Additional security controls must be deployed to protect media containing 'Highly Confidential' and 'Confidential' classified information from unauthorized disclosure or modification (e.g. through the use of encryption, locked containers, delivery by hand, tamper-evident packaging, splitting of the consignment into more than one delivery for dispatch by different routes and confirmation of delivery from the recipient).

3.13 Electronic messaging and internet security

- Sensitive information involved in electronic messaging must be appropriately protected according to the information security risks and classification.
- The emails generated from the company's user e-mail accounts shall be owned and monitored by AL-TIJARIA.
- Information of classification 'Confidential' or above must be sent through secure email.
- Outbound emails must be encrypted where possible.
- Outbound emails must contain a disclaimer.
- The IT Department and the Information security officer shall establish the necessary tools to monitor the internet use of all computers and devices connected to the corporate network. The monitoring system must record the source IP Address, the date, the time, the protocol and the destination site or server for all internet traffic. Where possible, the system shall record the User ID of the account initiating the traffic. Internet use records must be preserved for 180 days.



- The Information security officer shall periodically review and recommend changes to web and protocol filtering rules. Changes to web and protocol filtering rules will be reflected in the Internet Use policy of the Acceptable Use policies.

3.14 Audit Logging & Monitoring

- Audit logging shall be applied at all relevant system levels including network devices (also diagnostic ports), operating systems, applications, servers and databases. The attributes to be logged, frequency, retention time and location for logs storage shall be pre-defined by the Service Owners for respective systems.
- Audit logs and audit logging configurations shall be protected from unauthorized access, modification, and deletion. Audit logs shall be archived in accordance with archiving standards to assist with the investigation of security incidents and routine security monitoring.
- Systems and procedures for monitoring the use of information processing facilities through logs shall be implemented to ensure that users are not performing unauthorized or inappropriate activities.
- The level of monitoring required for individual systems must be determined by the Service Owner, Information Security Department, Risk management and IT Department according to the system's classification.



3.15 Security Event Logging & Monitoring

- Where appropriate, logging systems and log files shall be monitored on an ongoing basis to safeguard against unauthorized changes and operational problems such as:
 - a) The security logging facility being de-activated.
 - b) Alterations to log file contents (accidental or intentional modification) or to dates and times of log files or individual entries.
 - c) Deletion or renaming of log files.
 - d) Exhaustion of log file space, thereby causing records to be discarded or overwritten.
- Access to customer data shall be tracked and monitored.
- Relevant message types shall be transferred automatically to a centralized secure logging system where information from multiple sources may be correlated and analyzed in order to help identify significant events for security monitoring purposes.
- Security logs must be reviewed regularly by the Information Security Department and as necessary by other interested parties specifically authorized by senior management. Any major findings identified as a result of the review shall be reported to Executive Management. Security logs may also be reviewed at any time by the Service Owner, the Information Security Department and the Internal Audit Department.
- The results of and recommendations arising from the review of logs shall be presented to the Company's Information Security governance body.

3.16 Operator Logs

Operator that includes **all users logs** recording internal and external **access** support activities must be maintained.

3.17 Fault Logging

- Faults, within this policy document, shall refer to problems with IT or communications systems including definite or suspected security breaches, system failures, program errors/bugs, viruses, and other undesirable information system operation. Faults must be reported and logged, using automated functions where available.
- Appropriate real-time monitoring and corrective actions must be taken promptly when a fault is reported. Clear rules must be established for handling reported faults including management reviews of:
 - a) Fault logs to ensure that faults have been satisfactorily resolved
 - b) Corrective measures to ensure that controls have not been compromised and that actions taken were fully authorized
 - c) Error logging configuration parameters



3.18 Clock Synchronization

All the system including the network and security appliances must be configured to synchronize clocks against the companies authorized time server.

3.19 Servers

- Operating systems must be configured in accordance with approved operating systems security baselines.
- Services and applications currently residing on servers that are not used must be disabled.
- Critical security patches must be installed on the development, test and production servers upon release unless the patch will interfere with service requirements and or service availability.
- Security-related events (such as access, change,) on critical servers must be logged and audit trails saved.
- Server information and baseline configuration of the hardened server must be captured in a Configuration Management Database (CMDB) and any changes to the server configuration must follow the appropriate Change Management Procedure. An approved documented hardware specification shall also be maintained.
- Functions that may be performed on a server shall follow standard security principles of least required access.

3.20 Network Segregation

- Internal AL-TIJARIA systems and networks shall be segregated according to the respective information security risks into separate categories, groups, partitions or domains as described below:
 - a) Systems owned or managed by third-party suppliers vs. AL-TIJARIA.
 - b) Systems holding data of classification 'Confidential' or above must be placed in the core network.
 - c) Development vs. test vs. production systems.
 - d) Wired vs. wireless networks.
- Information systems classified as 'Highly Confidential' shall have a dedicated computing environment.
- Segregation shall use appropriate control mechanisms such as firewalls/gateways, physical isolation, encryption (e.g. Virtual Private Networks (VPN) or Virtual LANs (VLAN)), reflecting the security requirements arising from business needs and assessed information security risks.
- Firewalls must be appropriately configured to protect customer data.
- The firewall at the boundary shall only allow connection from a network whose session status (such as Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)) can be verified.



- To protect internal information systems and information, Demilitarized Zones (DMZs) shall be created where publicly available information shall be placed.
- Unauthorized external requests to network devices shall be rejected.

3.21 Network Controls

- Networks shall be managed and controlled to be protected from external and internal security threats and to protect the systems, applications, and information processed on the network.
- Responsibilities for managing and securing AL-TIJARIA networks and the general IT infrastructure shall be assigned for IT Infrastructure & Operations. Network and computer management activities must be coordinated and monitored to minimize risks to the business and ensure that information security controls are applied consistently across the entire IT infrastructure.
- The network perimeter and, where relevant, discrete internal domains must use firewalls and/or router Access Control Lists (ACLs) to monitor and control access to and use of the networks and attached systems.
- Redundant network boundary mechanism shall be implemented to avoid leakage of information due to the failure of primary network boundary protection.
- Security features, service levels and management requirements of relevant network services (such as the provision of connections, private network services, and value-added networks and managed network security solutions such as firewalls and intrusion detection systems) shall be identified, documented and agreed in Network Services Agreements.
- When selecting an Intrusion Detection and Prevention Systems (IDPS), the IT environment and relevant information systems shall be considered. The IDPS shall be configured in such a way that their automatic response to attacks will not introduce more risks.
- For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted. Access control policies shall be implemented that can be based on the attribute, role of the identity.
- Firewalls and other traffic routing controls (such as source and destination address-checking mechanisms, designated internal IP address ranges and Network Address Translation) must be applied and monitored to govern information flowing within or between public and internal networks.
- The stable and secure version of Simple Network Management Protocol (SNMP) shall be enabled on devices that require it.
- The possibility of attacks on networking devices shall be reduced by hardening the networking devices. This might include disabling unnecessary protocols, services or ports and deploying tools to detect the possible attacks.



- Protection techniques (e.g. limiting Synchronize (SYN) packets and Internet Control Message Protocol (ICMP) packets) shall be used for protection against Denial of Service (DoS) attack.
- Switches shall only allow access to their ports on the basis of Media Access Control (MAC) addresses.
- AL-TIJARIA Security standard should be enforced on all the network & security devices. IT must periodically review the compliance with these standards and report to ISS in case of non-compliance.

3.22 Network Equipment Authentication

- The physical components of the company's network shall be identified to the system being accessed. Devices may include terminals, lines, communication nodes, network switches, controllers, remote processors and personal computers. The node authentication methods chosen to satisfy the business and security requirements must be professionally designed, documented, tested, implemented, operated, maintained and reviewed, with the frequency and extent of review reflecting the security risk level.
- Network components will be uniquely identifiable and restricted for their intended business function.

3.23 Remote Diagnostic and Configuration Port Protection

- Physical and logical access to diagnostic and configuration ports shall be controlled and only those ports, services and protocols shall be enabled that are required for performing the services.
- Access to remote diagnostics, configuration / management or console ports and modems permitting privileged access for technical support on devices such as telephone exchanges, servers, disk subsystems, routers, firewalls and gateways, must be restricted to authorized support staff and third-party suppliers using strong user authentication and access control mechanisms and should not be enabled by default. The access must be revoked once it is no longer required.
- Privileged ports will only be enabled as and when required for specific authorized remote support activities.
- Unnecessary ports shall be identified and closed through periodic scans of networking devices. Moreover, regular reviews (at least every 6 months) of services shall be conducted and only the services whose operations can be justified shall be enabled.



3.24 Wireless Network Security

- While designing and implementing wireless network security, the following shall be performed:
- A survey shall be performed so as to identify the appropriate places where the Access Points (AP) shall be deployed.
- The Service Set Identifiers (SSIDs) of the access points shall not reveal information about AL-TIJARIA to external network users.
- Creation of ad hoc wireless networks is prohibited.
- Inbound connection requests to mobile devices must be disabled.
- Strong encryption shall be configured on the wireless network.
- Unidentified APs must be restricted.
- While accessing the core network through wireless AP, similar authentication and access controls shall be applied as that of a wired network.
- Data traffic from the guest network shall not pass through the core network.
- Near-field wireless connectivity options shall be disabled, e.g. Bluetooth, Infrared.
- Connection to the wireless guest network shall only be allowed during a particularly defined timeframe as per the company's working hours.
- If information of classification 'Confidential' or above needs to be sent through the public wireless network, VPN shall be used.
- The Company shall implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

3.25 Mobile Computing Devices

- Appropriate security controls must be implemented when using mobile IT facilities such as laptops/notebooks and mobile phones supplied by AL-TIJARIA in order to safeguard the company information assets (hardware, software, and data).
- The IT Department shall be responsible for operating system and application software maintenance including prompt patching to correct significant security vulnerabilities, personal firewalls and malware protection on mobile devices.
- The Company's computing devices must only be assigned to authorized employees or third-party suppliers working under contract for the company and only for business purposes.
- Mobile devices and systems shall be pre-configured by the IT Department with appropriate logical access controls, encryption, networking, and data backup facilities and antivirus protection.



3.26 Use of Cryptographic Controls

- Cryptography must be used to protect information (either hosted in-house or at third-party) with high confidentiality and/or integrity requirements.
- The following requirements must be considered when implementing an encryption tool at AL-Tijaria:
 - a) The handling requirements for sensitive information when transported by mobile or removable media, devices or across communication lines.
 - b) The impact of using encrypted information on other security controls (e.g. virus detection).
 - c) The cryptographic key length shall be selected as per the information classification.
- For new or changed services, only the cryptographic controls which are approved shall be applied.
- Based on the classification of the information, information residing on desktops & laptop should be encrypted.
- Mobile devices must be encrypted where the information accessible on the device is classified as 'Confidential' and above.
- Cryptographic controls must ensure confidentiality, integrity, and non-repudiation of messages containing confidential business transaction data.

3.27 Public Key Infrastructure

- Information systems requesting direct access or through proxy shall be authenticated via public key certificate where technically feasible. The authenticity of public key certificates shall be verified before binding to it. Depending on the degree of protection/level of trust required by the business, digital signatures must be cryptographically verified using public keys intended for signing and published on valid digital certificates issued by verified and trusted certificate authorities.
- Cryptography shall be implemented in either hardware or software when applicable and approved by ISS prior to use of any encryption products, processes, and standards. The Information Security section will maintain a list of all approved algorithms and acceptable key lengths.
- The Company shall use certificates issued by a recognized Certificate Authority-CA, certificates with minimum assurance levels of the medium must be used. For internal purposes, the Company may use certificates issued by the company's internal Certificate Authority-CA.
- Digital certificates are required for all internet servers that provide services to AL-TIJARIA customers or partners.



- Certificates should also be used internally on systems that transmit confidential information considering performance overhead impacts and business continuity aspects.
- Any regulatory requirements shall also be adhered to in relation to the creation, usage, handling, and destruction of cryptographic keys.
- The use of cryptography in any business situation shall be analyzed, reviewed and approved by the Information Security section.
- IT must only use proven standard algorithms such as AES, RSA, and IDEA as the basis of their encryption technologies. Proprietary encryption algorithms that have not been through rigorous public scrutiny must not be used.
- Encryption keys shall be carefully protected by their owners/custodians and under no circumstances made available to third parties. Secret encryption keys shall be password protected.
- Public keys should be distributed by an appropriately secured directory service. Where this is not available users may distribute their own public keys.
- The validity period of the cryptographic key should be dependent on the algorithm and key length being used. The key should comply with published recommendations of relevant authorities and/ or independent experts.
- Keys may be revoked prior to the end of their validity period if they have been compromised or misused, or upon a user request.
- The user or administrator should be automatically notified of a pending key expiration prior to expiry.

3.28 Security Devices and Software

Appliances and software related to information security shall be implemented and maintained by authorized and trained personnel. Use of security software shall be restricted to only those personnel who require them for fulfilling their job responsibilities.

3.29 Devices Maintenance

- IT equipment and devices shall be correctly maintained in accordance with the supplier's recommended service intervals and specifications to ensure their continued availability and integrity. A plan for preventive and proactive maintenance shall be developed to improve information system availability.
- Only authorized maintenance personnel shall carry out repairs and service the equipment. AL-TIJARIA shall maintain a list of authorized maintenance organizations and their personnel.
- Previously applied security controls on the device or equipment shall be tested to confirm that they are operating properly after the maintenance. The configuration shall be confirmed to be the same as the hardening baseline. Suitable records shall be kept of suspected or actual faults and the preventative and corrective maintenance performed.



- IT devices being sent for offsite maintenance shall be sanitized to remove confidential information that may reside on the devices.
- Device and equipment maintenance activities shall be monitored and controlled whether offsite or onsite.
- Necessary equipment / spare parts that might be needed for system maintenance, shall be stored for immediate availability.

3.30 Cyber Security

- Security on the network and production server are to be maintained at the highest level. Those responsible for network and external communications are to receive proper training in risk assessment and how to build a secure system that minimizes the threats from cybercrime.
- In order to be prepared, maintained and regularly tested to ensure the damage done by possible external cyber-attack can be minimized and business service can be restored in the expected timeframe.
- It is a priority to minimize the risk related to cyber-attacks on company's systems and information through a combination of technical and robust procedural controls.
- Contingency and response plans for the different type of cyber-attacks are to be maintained and periodically tested to ensure adequacy.
- Fostering staff awareness, encouraging staff vigilance and deploying appropriate protective and detective controls to minimize the risk related cyber-attack.
- Without exception, the company has approved Anti-virus software is to be deployed across all the systems and regular malware definition and scanning must be enforced on all the systems.
- To minimize the impact related to malware infection, a formal incident procedure for responding to the malware related incident should be developed and tested regularly.



4. Logical Access Security Management

4.1. User Access Management

- Formal processes shall be established and implemented to control the provisioning of access rights to AL-TIJARIA information assets.
- Business requirements for access to specific information shall be defined and expressly approved by the relevant Service Owner before access to AL-TIJARIA's information assets is granted to users.
- A unique user ID shall be created on the required systems for each user, which shall link the employee to their user actions on AL-TIJARIA's information systems. User IDs must conform to naming standards and must not give any indication of the users' access rights e.g. contain words such as manager, supervisor or privileged.
- Where there is no alternative to using unique user IDs, a user ID may be shared by a specific group of users for a specific purpose and shall be explicitly approved by the IT Manager and the Information security officer. A single individual must be held personally accountable for the use of each shared user ID.
- IT shall coordinate with the HR Department to manage the records of users requiring access to multi-user information systems and services and other critical IT equipment.
- Service Owners (or their explicitly nominated delegates) shall determine normal users' access to application systems and authorize their user roles appropriate to the employee's job responsibilities.
- User accesses to the network and network services shall be granted, authorized and managed only on business need and need-to-know basis.
- Formal records shall be maintained on all access requests to evidence management authorizations and granted or revoked access rights.
- Service Owners, Department Managers, and HR Department shall be jointly responsible for promptly updating or revoking access rights if users change jobs or leave AL-TIJARIA and must periodically check for and remove redundant/invalid user IDs and access rights.

4.2. Secure Log-On

- The company systems must use the following secure logon processes, as applicable:
- Computers must be enabled with the (Control-Alt-Delete) and (Window Key +L) secure user login initiator sequence.
- Upon user logon, systems shall display a standard notice warning against access by unauthorized users.
- Passwords, Personal Identification Numbers (PIN), private keys and other access authorization codes must not be displayed on the screen, sent unencrypted over the network nor stored unencrypted.



- If invalid user credentials and passwords, PINs, token values and other access authorization codes are entered, systems shall not indicate which elements were incorrect.

4.3. Privilege Management

- The allocation of privileges must be controlled through a formal authorization process, which must:
- Identify the privileges associated with each system product (e.g. operating system, database management system) and the groups to which they need to be allocated.
- Allocate privileges to individuals on a 'need-to-use' basis and on an 'event-by-event' basis (i.e. the minimum requirement for their functional role only when needed).
- Privileged user management must follow the same procedure as normal users.
- Two-factor authentication shall be implemented for critical systems where appropriate.
- Local administrator privileges shall only be granted to specific IT Department employees for technical support tasks after seeking approval from the IT Manager and the Information security officer.
- Local administrator privileges must not be provided to non-IT end users except when required for specific business applications and if approved by the IT Manager and the Information security officer.
- Users must only be provided with access to the services that they have been specifically authorized to use.
- The users must be appropriately authenticated before granting access to these services.
- This applies to services such as Remote Desktop Protocol (RDP), SharePoint, Domain, Email, Files and Folders, Wireless, Web Access to Security devices, etc.



4.4. Password Settings & Management

- Systems containing information classified as 'Confidential' or higher shall require sufficient authentication (e.g. user names and strong passwords) to verify the identity of the users.
- A formal process must be followed to confirm the identity of the requesting user before a new password is delivered or a replacement password is issued.
- Passwords must be applied to allow system access (i.e. 'blank' passwords are not allowed).
- Default vendor account passwords must be changed for new implemented systems and devices.
- Copies of administrative passwords must be stored securely (in hashed form) with offsite backups for disaster recovery purposes.
- System administration staff must use personalized accounts and must not use administrative system accounts for normal day to day operations.
- Initial/temporary passwords must be changed after the first use.
- Passwords files must be stored in an encrypted form.
- Passwords complexity must be enabled for all systems:
 - At least one uppercase letter
 - At least one lowercase letter
 - At least one numeric digit
 - At least one non-alpha-numeric character
 - Passwords must be at least 8 characters in length.
 - Passwords must be complex
- A new password must not be the same as the last 6 previously used passwords.
- Passwords must be changed at least every 90 days.
- Passwords minimum age shall be 1 day.
- Passwords expiration alert must be 14 days prior to expiration.
- Account lockout duration must be at least 15 minutes.
- Account must be locked out after 5 invalid password trials.
- Logon must be restricted only to the users that are granted access.
- Systems for managing passwords shall be interactive and shall ensure quality passwords according to the policy.

4.5. Administrative Password Use

- Administrative privilege passwords for IT servers and network/security devices shall be maintained in a sealed envelope in a locked safe or in Privilege access Management System.
- Passwords (including pass-phrases, PINs) must be:
 - Kept confidential and not shared (except for specifically authorized shared / group user IDs).
 - Memorized rather than written down.
 - Easy to remember but hard to guess (e.g. no dictionary words, variants of AL-TIJARIA or the user's name, project or Departments' names, locations, simple keyboard sequences).



- Communicated to the user through a different channel to the method used to communicate the account ID.

4.6. Session Time-Out

- Inactive sessions must be ended after a defined period of time. The default time-out period is 15 minutes.
- Any variance is based on the risk categorization of applications which needs to be approved by the Information security officer and relevant Application Owner.

4.7. Directory Management

- To manage access to information assets and user accounts, a directory shall be produced and managed as described below:
- The directory shall be designed in such a way that the changes do not affect the already implemented access rights.
- Appropriate access policies shall be defined in the directory service.
- Directory servers shall be monitored periodically.
- The security classification of the directory service shall be the same as the highest classification of the information it accesses and shall be recorded.
- Only authenticated servers shall be allowed to join the directory service group.
- Communications involving authentication credentials or information system access permissions shall be performed using strong encryption.
- Only qualified and competent individuals shall be assigned responsibilities for managing directory.
- The Information security officer's approval shall be required for linking multiple directories.
- Only specific authorized individuals shall have access to directory service's technical details.

4.8. Review of User Access Rights

- The Information security officer shall ensure that Service Owners formally review user access rights on a semi-annual basis and after any significant organizational, systems or personnel changes, for users on their information systems.
- This will identify access rights that may no longer be required and any dormant accounts that can be removed from the information systems.



- The Information security officer shall ensure that privileged access rights granted on production systems are checked on an annual basis by the Service Owners against the approvals on file to ensure that unauthorized privileges have not been obtained.
-
- Ad hoc access rights reviews may be conducted at any time at the request of management, Service Owners, Information security officer or auditors.
-
- User access rights and privileges shall be reviewed and, if necessary, re-approved by managers when employees transfer internally, particularly in order to maintain appropriate access.
-
- Reviews of access rights and privileges must be documented and the documentation retained for at least a year in a form suitable for audit reviews.

4.9. Authentication of external connections

- Users seeking access to AL-TIJARIA networks must be authenticated at the initial point of entry into the network using unique user IDs and appropriate authentication (e.g. cryptographic security tokens or smart cards coupled with passwords, PINs and/or biometrics).
-
- Permitted forms of remote access shall be defined.
-
- VPNs shall be used for establishing and maintaining remote access connections and while connected through VPN to the core network, connection to other networks shall be restricted.
-
- Special control shall be established to safeguard the confidentiality and integrity of data passing over public networks and to protect the connected systems.
-
- Only one remote connection from a single account shall be allowed at any one time.
-
- The usage of internet-based remote desktop software like WebEx shall be prohibited unless authorized by the Information Security Department.

4.10. Information Access Restriction

- Application systems running across the organization must have an appropriate access control mechanism in place to ensure that data integrity and security are maintained and any unauthorized access to applications or a part thereof is prevented/restricted.



5. Human Resources Security

5.1. Enforcement of information Security Policies

- The Information security officer, Risk Management Department & System Owner in coordination with the HR Department, shall identify responsibilities towards maintaining the security of AL-TIJARIA's information assets and services for the current positions at AL-TIJARIA, including responsibilities of special individual roles or groups that are significantly involved in maintaining IT Policies at AL-TIJARIA. In coordination with HR, Risk Management Department and Information security officer, each line manager shall ensure that relevant Information Security Policies responsibilities are incorporated in the job descriptions of the subordinates.
- Information Security Policies responsibilities shall be included in the code of conduct and presented to potential candidates prior to employment.
- The code of conduct must clearly state the employee's obligation to comply with AL-TIJARIA's Information security policies and describe the disciplinary actions that shall be applied for non-compliance.
- Adequate segregation of duties shall be maintained in the designation of roles and responsibilities across the different roles at AL-TIJARIA, when circumstances allow and where the benefit of segregation of duties outweighs the operational risk of not having cross-trained employees as a backup.
- Employees shall sign the code of conduct document prior to being permitted access to AL-TIJARIA's information assets. A record of each employee's acceptance shall be maintained by the HR Department.
- All employees shall be required to read, sign and comply with the Code of Conduct.
- Every new Employee must attend and complete an information security awareness training within one month of the date when they began employment with AL-TIJARIA and all the subsequent security training complete in due date.
- Human Resources Department is to ensure that all employees are fully aware of their legal and information security responsibilities, which are to be included in key staff documentation (e.g, Terms and conditions of Employment and AL-TIJARIA Code of Conduct)



5.2. Personnel & Candidate Screening

- Candidates for employment and current employees, who have not been previously screened, shall be screened by the appropriate authorities according to the predefined screening criteria based on the security risk designation of the position.
- HR Department along with the relevant Business Departments shall determine the competence required for the role based on the role's specific characteristics and requirements, as per AL-TIJARIA's HR Policy. This shall include but not limited to: education, training, skills, and experience.
- Roles and responsibilities assigned to individuals shall be based on a comparison of the actual competence and the required competence of that role.
- New employees' education, professional qualifications, and employment background shall be checked for credibility and authenticity.

5.3. Disciplinary Process

- Disciplinary procedures shall be established to handle employees failing to comply with Information security policies. The disciplinary procedures shall be in compliance with applicable government requirements.
- Disciplinary actions shall be taken only where reliable evidence of a breach of obligations towards information security Policies is available. Only the individuals who have the need to be informed about the disciplinary activities shall be involved.
- The information obtained from disciplinary process activities shall be used for preventing similar cases in the future.
- Should an employee leave AL-TIJARIA or be terminated, the HR Department shall conduct an exit interview and notify the IT Department to coordinate the return of equipment assigned to the employee and ensure timely removal of the employee's physical access and logical access to AL-TIJARIA's applications.
- A record of the exit interview shall be maintained by the HR Department that captures the items in the employee's possession and the items returned.
- AL-TIJARIA shall define a retention period, where applicable, for disabled or inactive user accounts.
- Employee termination procedures must be followed with extreme conscientiousness particularly in regards to termination of access privileges.
- In every case where an employee is involuntarily terminated by The Company, the termination must take place in the presence of security personnel, who will escort them to the door after collecting their personal belongings.



6. Information Security Incident Management

6.1. Reporting Incidents & Events

AL-TIJARIA personnel must report information security events to the IT Service Desk as soon as practicable after they occur. Mechanisms (Service desk portal, telephone and email channels) shall be created through which these incidents can be reported. Information security events include, but are not limited to:

- Violation / non-compliance with AL-TIJARIA's IT policies, or with other applicable laws and regulations relating to risk, control, and governance of IT and AL-TIJARIA's services.
- Unusual IT system behavior such as malfunctions/bugs, error messages, viruses, alarms and alerts, delays and unanticipated results.
- Loss of IT services, equipment or facilities, including theft, damage, malfunctions, overloads, accidents, human errors or other situations that cause service outages.
- Phishing attack.
- Uncontrolled or unauthorized system changes.
- Discovery of inappropriate access rights.
- Misuse of systems.
- Confidentiality failures (e.g. unauthorized disclosure of or access to sensitive information).
- Violations of network, system or data access policies.
- The IT Service Desk shall notify to Information Security section after the initial validation of the reported event and ISS will initiate suitable incident response processes based on Incident Response framework

6.2. Reporting Security Weaknesses

Employees must not themselves attempt to explore, evaluate, confirm or prove suspected weaknesses which might

- (a) lead to serious security breaches,
- (b) interfere with forensic analysis and/or
- (c) be interpreted as a deliberate misuse of the system and result in disciplinary or legal action. Similarly, employees must not attempt to repair or deal with software malfunctions unless explicitly instructed to do so by the IT Service Desk.



6.3. Information Security Incident Management Planning

The planning for information security ISS – Risk Management shall include the following:

The information security ISS – Risk Management plan, shall be based on the predicted incident data and reviewed by the Risk Management Department.

- Checklists shall be created outlining the activities that need to be performed for containing predicted incidents, including notification obligations to internal and external stakeholders affected by the incident.
- Only authorized personnel shall be allowed to access the incident management framework and supporting tools.
- A central knowledge-base of information shall be developed which contains details about the identified incidents and the corresponding solutions.
- A diagnosis matrix shall be created to help IT staff in quickly detecting the type of incident occurring and what remedial measures can be taken.

Cooperative relationships shall be maintained with external providers of information system protection to remain updated about the latest information security incidents and their possible responses.

For possible major incidents, management shall give prior approval to the ISS – Risk Management team and agreed by the key stakeholders for taking the required action.



6.4. Responsibilities & Procedures

Incidents must be managed by an ISS – Risk Management team whose roles and responsibilities shall be clearly defined. Incident management responsibilities and procedures must ensure a quick, effective and orderly response to information security incidents. Monitoring of information systems and logging of events shall be integrated with incident management activities.

Incident response procedures shall cover:

- Classification and categorization of incidents based on their criticality and impact.
- Analysis of reported security events and weaknesses, monitoring of systems, alerts, and vulnerabilities in order to identify and prioritize security events that appear to indicate actual incidents or potential incidents if not prevented.
- Containment (e.g. disconnecting affected systems from the network pending further analysis).
- Analysis and identification of the causes of incidents (“What happened exactly? Who and which IT assets were involved? Which controls were missing or failed? What damage was caused to the Company?”).
- Applying the learning from incidents to achieve continuous improvement in AL-TIJARIA’s ability to manage information security risks.
- Log files, audit trails, and similar forensic evidence.

Major security incidents shall be reviewed and monitored as per incident response framework.

6.5. Information Security Incident Training & Simulation

- Designated personnel shall be trained to contain the incidents through simulation of incidents.
- The incident simulation shall be developed by a coordinator and a record shall be maintained of the outcomes of the training. Findings from the simulation and training shall be used for improving the Incident Management framework.
- The members of the ISS – Risk Management team (IT Infrastructure & Operations section) shall be switched without prior notice to determine how the incidents are managed if key roles are unavailable.
- Regular (at least annual) training shall be conducted so that the incident management team remains updated on the current trends in information security incident management.



6.6. Management of Security Incident Responses

- The ISS – Risk Management team shall be allowed to conduct an independent investigation. For major incidents, a single incident Co-ordinator shall be assigned to handle the incident with full authority.
- Supporting tools and checklists shall be established and used to manage incidents.
- Information security officer / IT Manager can conduct an independent investigation supported by third parties.

6.7. Management of Security Evidence

- A procedure shall be developed and used for the situations where an incident is escalated to a level that necessitates legal action to be taken. Adequate evidence shall be gathered and retained to adhere to the rules for evidence as stipulated by the relevant regulation/jurisdiction.
- The management of evidence shall comprise of four phases: a collection of data, examination, analysis, and reporting.
- The ISS – Risk Management team shall be competent to manage evidence.
- Evidence shall be stored in a secure area with properly defined access control policies.
- The logs related to the actions performed on evidence shall be maintained.
- External parties (lawyer or police) shall be involved, if required, for investigation.
- Digital evidence shall be obtained with write protected capabilities.

6.8. Post-Incident Analysis, Reporting, and Corrective Action

- Both, the ISS – Risk Management team and impacted parties shall be involved in the post-incident review. A report shall be generated following the review describing the significant findings.
- This report shall be approved by the Risk Management Unit, where suitable corrective actions shall be assigned to contain the incidents.
- The types, volumes, and costs (where appropriate) of security incidents shall be quantified and monitored to identify recurring or high impact incidents or malfunctions. This shall indicate the need for enhanced or additional controls and changes to AL-TIJARIA IT policies.
- Taking confidentiality into account (e.g. removing details of involved individuals or other sensitive information), information security incidents may be used for security awareness purposes

7. Asset Management

7.1. Inventory of Assets

An Inventory of the company's assets shall be recorded, reviewed, maintained and audited on a periodic basis.

7.2. Information Assets Classification

- Information in AL-TIJARIA's possession shall be classified as either public, internal, confidential or highly confidential, based upon their sensitivity.
- The default classification for assets shall be 'Confidential' until a specific classification is assigned to them.
- The classification of an information system shall correspond to the highest classification of data present on or passing through it.
- The classification of information assets shall be regularly reviewed by the information assets respective service owners in coordination with the information security officer & risk management department.
- An impact analysis must be undertaken whenever reclassification of an information asset is required, and the relevant stakeholders shall be informed about the reclassification.

7.3. Retention & Disposal of Information

- Effective file-keeping and data management are vital to allow AL-TIJARIA to carry out its business functions, the data retention and disposal policy provides clear guidance on the retention and disposal of the company's data, and ensures that the data is:
 - a. Retrievable and can be easily traced
 - b. Retained for only as long as necessary
 - c. Disposed of appropriately to prevent them from falling into the hands of unauthorized personnel.
 - d. Stored appropriately having regards to the sensitivity and confidentiality of the material recorded.
- Every information assets owner is responsible to consider security when using and disposing of information in all circumstances. Departments, units or vendors that are regarded as key information owners or custodians shall be responsible for defining and documenting the retention period of critical information.
- The legal requirements and responsible parties should also be specified.
- AL-TIJARIA shall define appropriate retention periods for certain kinds of information as stipulated from time to time by governing bodies and applicable guidelines. Every department, unit of vendor shall establish procedures appropriate to the information held and processed by them, and ensure that all relevant parties are aware of those procedures.
- Departments, units or vendors must retain records and information if:
 - a. They are likely to be needed in the future, unless a specific retention cycle has already been mandated by specific policy to ensure their timely availability.
 - b. Regulation or statute requires their retention.
 - c. They are likely to be needed for the investigation or prosecution of unauthorized, illegal, or abusive acts or to allow AL-TIJARIA to respond to discovery requests,



subpoenas, investigatory demands and other requests for information related to legal or regulatory proceedings.

- Sensitive information should be disposed of according to the respective disposal procedures for different classifications of information in order to ensure complete and secure removal of “Highly Confidential”, “Confidential” or “Internal” information, including both paper-based and electronic forms.
- Disposal procedures include shredding, low-level formatting, degaussing of hard disk drives, etc. Unauthorized destruction or disposal of the company’s sensitive information will subject the perpetrator to disciplinary action including termination and prosecution.

7.4. Management of Removal Media

The IT Shall develop, document, and implement procedures for the management of removable media.

8. Third-Party Supplier Management

8.1. Identification of Third-Party supplier Requirements

- Types of external parties and related information security risks shall be identified and documented. Subsequently, security requirements to address these risks shall be identified.
- Information security requirements must be included in the Requests for Proposal (RFP) and Requests for Quotation (RFQ). The third-party supplier must be required to include their commitment to the company’s information security requirements in the responses to the RFPs and/or RFQs, which shall be transferred to the agreement should the third-party supplier be awarded.
- Non-compliance with the agreed service levels by third-party suppliers shall be raised as a risk, recorded in the risk register and a plan to mitigate that risk shall be developed.



8.2. Security-Oriented Supplier Selection

- Third-party suppliers must be required to sign a Non-Disclosure Agreement (NDA) before any information about current information security status and future needs can be shared with them in RFPs and RFQs.
- Supplier proposals shall be reviewed and evaluated against the extent to which the third-party supplier meets the information security requirements defined in RFPs / RFQs. The contract shall not be awarded to third-party suppliers who do not meet the minimum information security requirements or are found to have other security-related issues.
- For the purposes of outsourcing data center hosting, the company's information of classification level 'Confidential' or above may be hosted outside of Kuwait.
- Discussions with, reviews and inspections/audits of potential third-party suppliers shall be conducted, where necessary, to evaluate if the third-party suppliers are capable of satisfying and maintaining security requirements prior to entering into contracts.

8.3. Managing Third-Party Suppliers Agreements

- The following must be considered when including information security requirements in an agreement with a third-party supplier (where applicable):
- The risks associated with the third-party supplier type and impact on AL-TIJARIA's overall security including legal and contractual requirements.
- Third-party supplier's obligations towards providing awareness of and ensuring compliance with AL-TIJARIA's relevant IT policies among the personnel deployed by the third party.
- The logical access requirements for user and administrator access.
- The logical access requirements for connections outside of AL-TIJARIA's network requiring details about the person approving interconnection, systems involved, communication paths used and protection of information being exchanged.
- The sensitivity of the information that the third-party supplier will access (requirements to comply with AL-TIJARIA's Information Labelling and Handling Standard requirements depending on information classification type must be identified and included in the contract).
- The target level for service and security and monitoring of the third-party supplier's performance against contractual security requirements for compliance at specific planned intervals.
- The change management process which will be followed by the third-party supplier.
- Physical access requirements.
- The impact of the agreement on service continuity requirements.
- The contract with the third-party supplier shall indicate the penalties or actions that can be imposed on the third-party supplier if they fail to comply with the information security requirements stated in the contract.
- The contract shall state that the third-party supplier shall indicate any possible risks that may arise from performing different activities on the information asset under focus.



- Third-party suppliers shall be required to agree, in the contract, that AL-TIJARIA's information is under agreed access control and is shared only among the relevant personnel.
- Security controls, service definitions, and delivery levels shall be included in third-party supplier service delivery agreements to be implemented, operated and maintained by the third-party supplier.
- Third-party suppliers' contracts shall incorporate a 'right of audit' clause giving AL-TIJARIA the ability to inspect and assess third-party suppliers' internal processes relating to the contract, including aspects such as documented security policies and procedures, change controls, audit trails and processes for identifying, managing, resolving and reporting security incidents.

8.4. Managing Third-Party Suppliers Access

- Access to AL-TIJARIA's information assets by third-party suppliers must be restricted to authorized organizations and people. Remote or onsite access for external parties to AL-TIJARIA's network or systems shall be based on the following requirements:
- Service Owners must explicitly pre-authorize third-party supplier remote access to their assets. Where direct access cannot be granted to the third-party supplier, the Service Owner shall designate a member of AL-TIJARIA's personnel to supervise the third-party personnel.
- The list of authorized third-party supplier logical access, maintained by IT, must be reviewed every six months and if requested by the Information security officer to confirm the continued requirement for the access.
- Logs shall be maintained for remote connections used by third-party suppliers and reviewed on a weekly basis.
- Remote access granted to third-party suppliers must be reconfigured and removed immediately if the contractual relationship with the third-party supplier ceases, the agreement/contract expires or if the Service Owner or Information security officer decides to terminate the arrangement for any other reason.
- The list of physical onsite third-party supplier access shall be maintained by the General Services Department in cooperation with the IT Department and the Administration Department – General Services who are responsible for third-party suppliers and reviewed every six months.

8.5. Third-Party Service Delivery

- Background checks shall be performed on third-party personnel that is exposed to AL-TIJARIA's information assets or information systems. AL-TIJARIA may perform these checks or request third-party suppliers to provide suitable evidence of clearance.
- Regular reports prepared by the third-party supplier describing the effectiveness and status of security controls implemented to protect AL-TIJARIA's information asset shall be shared with AL-TIJARIA where applicable. Monitoring data received from third-party suppliers must be verified for authenticity and integrity.



8.6. Monitoring & Review of Third-Party Services

- The services, reports, and records provided by the third-party supplier shall be reviewed, and audits shall be carried out where necessary on a regular basis.
- Services delivered by third-party suppliers must be monitored to ensure they are delivered and maintained in accordance with current information security requirements, business requirements and contractual obligations on a frequency appropriate to the contract duration and type of service.
- The performance of the third-party supplier shall be measured against service targets and other contractual obligations.
- An information security capability review shall be conducted at least annually for outsourced service suppliers to ensure that their capabilities to safeguard AL-TIJARIA's information are suitable and whether the business objectives for sourcing service or a service component remain valid according to the information security requirements.
- Responsibilities for managing supplier contracts and relationships must be assigned to specific roles or teams.
- The contract shall only be rewarded to a third-party supplier if the supplier's information security capabilities are as required by AL-TIJARIA. The contract with a third-party supplier shall be terminated if there are repeated violations of agreed information security requirements.

8.7. Managing changes to Third-Party Services

- Changes to the provision of services, including maintaining and improving existing IT policies, procedures, and controls, shall be managed and controlled against AL-TIJARIA Change Management process, taking account of the categorization of the supported service and classification of information systems and processes involved.
- AL-TIJARIA shall control changes to the third-party supplier's contracts by the Change Management process.

9. Data Protection and privacy

- The Legal Department shall identify all relevant laws and regulations for data privacy and protection of personally identifiable information and Information Security Department shall be responsible for complying with the identified laws and regulations.
- The Information Security Department shall identify specific controls required for safeguarding Customer information from unauthorized use, disclosure, destruction, and alteration, in line with applicable regulations.
- Users shall get Information Security's approval before collecting, processing, storing or disclosing confidential or customer information.
- All employee and/or customer data is to be treated as strictly confidential and made available to only properly authorized persons.
- Employees are discouraged from sharing personal salary details and other terms and conditions with other members of staff.
- All Users must treat passwords as private and highly confidential. Non-Compliance with this policy could result in disciplinary action.



9.1. Electronic Messaging

The information involved in electronic messaging such as the internet, email, and fax shall be protected from misuse of information, unauthorized access, modification or denial of service.

9.2. Protection of test data

Test data shall be selected carefully, protected and controlled to avoid the use of operational or any other confidential information.

9.3. Privacy and protection of personally identifiable information

The privacy and protection of personally identifiable information at AL-TIJARIA shall be followed in accordance with an AL-TIJARIA Privacy Policy, the related contractual clauses, and relevant global and local legislation.

10. Secure Design, Development & Testing of Services

10.1. Information System Design & Development

- Information systems design and planning shall be performed to include the definition of information security requirements prior to the selection/development, deployment and implementation of any new services or major changes to existing services. Information security must be taken into account early in the systems' development life cycle; within business cases, budget proposals, work requests, and similar initiation and planning documents.
- Once system development or system change projects are approved, Project Managers, working in conjunction with the Information security officer, shall be responsible for following AL-TIJARIA's approved software development life cycle and acquisition methods.
- Security requirements of the new service or changes to an existing service shall be formally outlined at the start of the project. The input of the Information security officer shall be sought to ensure that adequate security requirements are captured. Information security requirements shall be compatible with the operational requirements of the information system.
- A system design document shall be developed for new or changed services detailing the information security controls to be implemented to meet the identified security requirements. The design shall be approved by the Service Owner and the Information Security Department before the development of the service shall commence.
- Controls should be selected for implementation on multiple tiers, such as the user interface, application back-end, and database layer.
- A high-level information security risk assessment shall be conducted, if necessary, and complemented with detailed risk analysis to clarify the security control requirements,



reflecting the value of the information assets and the potential impacts of security incidents.

- Relevant Service Owners and the Information security officer shall be consulted in the design and development stages of a new information system or a significant change to an information system to ensure the efficiency of the proposed system when addressing the operational requirements in combination with implemented security controls.
- New or significantly changed information systems implementation planning shall include identification of IT capacity and availability requirements, error recovery and restart procedures and contingency plans.

10.2. Information Systems Testing & Implementation

- Information systems shall be tested prior to implementation.
- A testing plan shall be established and include test cases to evaluate the effectiveness of service/system controls against the security requirements specifications. Areas that failed security testing shall be amended to achieve compliance. Systems shall also be tested against possible malicious attacks. Security testing shall be conducted in accordance with AL-TIJARIA's approved system life cycle development and testing procedures.
- The results of security testing shall be documented within a testing report. If testing for a particular control fails, it shall be recorded in the report, alongside subsequent testing attempts. If the control corresponding to the failed test cannot be amended, a compensating control shall be applied and documented within the report. Known / inherent security vulnerabilities in the information systems must be addressed through suitable compensating controls as determined by the Service Owner, as advised by the Information security officer.
- Upon the successful completion of security testing, confirmation that the tested information system is compliant with the security requirements and does not have any unnecessary functionalities enabled shall be evidenced by the Service Owner's sign-off on the testing report prior to deployment on the production environment.
- Test data must be secured according to the data's classification. Production data must not be used for development or testing unless it is desensitized or scrambled. Test systems must be subject to the same access controls as applied to corresponding production systems.
- Configurations shall be applied on information systems and network devices according to the hardening baselines, using AL-TIJARIA security guidelines & Security Standard where applicable, before they are deployed on the production environment.
- An information system shall not be moved to the production environment unless all administrator, test, and development accounts have been removed from it. Testing data shall be removed from the information system once testing has been completed.
- Access to information systems shall be granted in accordance with the policy statements in Logical Access Security Management.
- New software and new sections of source code on existing software (e.g., Structured Query Language (SQL) queries and procedures), shall be reviewed for quality prior to deployment, wherever possible.
- Upon implementation of a new or significantly changed information system, the following shall be met:
 - An operations manual that covers start-up, shutdown, and recovery procedures shall be made available prior to the introduction of a new system.
 - System manuals and relevant training, where required, shall be provided to end users before the information system is to be used.



- Systems and data shall be backed up regularly and suitable resilience and disaster recovery arrangements must be made. 10.2.11 IT Infrastructure and Operations shall perform security testing on a quarterly basis which includes but not limited to:
 - a. Authenticated vulnerability scan.
 - b. Compliance scan based on AL-TIJARIA Security Standard.
 - c. Configuration review.

10.3. Control of Operational Software

- Details about approved and supported software shall be maintained including information about the previously approved software.
- Security software must be used only by authorized personnel and for authorized purposes.
- Implementation of software on production systems must be controlled to minimize the risk of corruption of operational systems. Only designated personnel shall be permitted to update production program libraries. Such updates must be authorized and logged.
- Operating system controls must prevent unauthorized software that can bypass the information security controls or have direct access to application program and data files (including application utilities/tools, application configuration/parameter files, application start-up/shutdown scripts, and application log files) by other users.
- Previous versions of software programs must be retained under configuration management as a contingency measure.
- Vendor supplied software used in production must be properly maintained, especially in the application of security patches.
- A plan shall be developed for Vulnerability and Patch Management. Patches shall only be applied to the production system after they are successfully tested on a separate test system.
- Direct read-only access to application programs and data files shall be authorized for routine systems management activities such as backups, performance, and capacity monitoring and security monitoring. Other direct access is only permitted when authorized through the change control procedures.

10.4. Security of Program Source Code

- Program source code and associated information (such as designs, specifications, program listings, test plans, and reports) shall be maintained in a controlled manner and changes shall be authorized by the Service Owner. Separate libraries shall be used for development, test and production environments, controlled by designated personnel.
- Software code shall be tested (using code analysis tools) and verified for completeness. The only code that has completed Production Acceptance Testing may be cataloged into production libraries.
- Code shall be stored in a central storage space in secure program libraries. Updates to code held in program source libraries must be authorized by the Service Owner. Issuance or compilation of code from libraries shall be performed by the designated personnel and must be logged.
- Old versions of source programs shall be archived.
- Third-party-owned source code shall be held in escrow if AL-TIJARIA is critically reliant on the ability to maintain/update the code, particularly if there is any doubt about the vendor's resilience or capabilities.



10.5. Software Packages

- The third-party supplier contract shall require the vendor to confirm that the applicable security testing has been performed and the software is free from known vulnerabilities.
- Wherever possible, third-party supplier software packages shall be used without significant modifications.
- Where it is deemed essential to modify a third-party supplier software package, the following rules must be respected:
 - The consent of the relevant Service Owner and vendor must be obtained in advance.
 - The associated risks and potential impacts must be assessed, especially if AL-TIJARIA will become responsible for the future maintenance of the software as a result of the change.
 - Changes must be fully tested and controlled.
 - Changes must be fully documented so that they can be re-applied if necessary following future software upgrades by the vendor.

10.6. Security of System Documentation

- Documentation describing system, network and application designs, security parameters, operating and management processes, data structures, user authorization processes, testing plans, test results must be classified according to AL-TIJARIA's information classification process and adequately protected against unauthorized access.
- Adequate security shall be applied to system documentation that is held on the intranet, which can be accessible by employees.



11. Service Continuity & Availability Management

- The policies in this section have been defined to describe AL-TIJARIA's services continuity and availability considerations. Business process contingency plans and information technology availability and recovery processes shall be established to maximize the ability to maintain a cost-effective and practical level of business continuity in the interim period between the interruption and recovery of information technology services.

11.1. Service Continuity & Availability Requirements

- AL-TIJARIA shall assess and document the risks to IT service continuity and availability.
- AL-TIJARIA shall identify with the different Departments IT service continuity and availability requirements, taking into consideration service requirements, SLAs, risks and business plans.
- Service continuity and availability requirements shall include:
 - a. Access rights to the services
 - b. Service response times
 - c. End-to-end availability of services

11.2. Service Continuity and Availability Plans

AL-TIJARIA shall document, implement and maintain plans and procedures for service continuity and availability.



11.3. Information Security in Business Continuity Management

- AL-TIJARIA shall consistently manage business continuity throughout the business departments. It shall address the dependency on critical business processes by ensuring the availability of supporting information systems.
- Components which are critical to the continuity of service shall be identified, and arrangements shall be provisioned to enable services to be resumed promptly in the event of their failure. Following measures, wherever practical shall be implemented at information processing facilities:
 - a. Provision of stand-by power supplies.
 - b. Redundant servers and hardware.
 - c. Duplication of processors and on-line storage.
 - d. Automatic re-routing of communications.
 - e. Fall-back capability to alternative internet carrier services.
 - f. Contract-based maintenance to ensure timely repair.

12. Security Training & Awareness

The policies in this section ensure that AL-TIJARIA employees receive the proper training and awareness in order to establish AL-TIJARIA's baseline expectations among the personnel for safeguarding AL-TIJARIA's information assets.

12.1. Information Security Induction

- A comprehensive information security induction process shall be established and shall outline and communicate information security responsibilities and expectations to the employees that should have access to AL-TIJARIA's information assets and systems, as per their job roles.
- Records shall be maintained showing the individuals who received the security induction. Attending the security induction session shall be a prerequisite for granting access to information assets or information systems for each new employee. Exceptions are not permitted.



12.2. General Information Security Awareness

- General information security awareness sessions, applicable to AL-TIJARIA's employees, shall be conducted at least once per year. Changes to IT processes, policies or organization shall be communicated to the users during the general awareness training sessions, in addition to other suitable communication to relevant parties within an appropriate time following a change.
- Communication of information security shall be planned, identifying the target audience, frequency, and modes of communication.

12.3. Information Security Education and training Curriculum

- An information security training curriculum shall be developed in coordination with HR with applicability to AL-TIJARIA employees handling AL-TIJARIA's information assets and systems, outlining the required information security training sessions that are tailored to roles involved in specific information systems use.
- The information security training curriculum shall be designed on the basis of required learning outcomes and objectives applicable to the different roles and categories of stakeholders. The Risk & Audit committee shall monitor the delivery and effectiveness of the training curriculum and information security related communication, such as e-mail campaigns or posters, reminding users of their information security obligations.
- The training curriculum shall be developed to ensure training sessions are conducted annually to reinforce the users' and other specific roles of their responsibilities towards information security management system.
- HR shall coordinate closely with Information Security to ensure that the training curriculum and training materials are updated to reflect new trends in information security, significant changes to AL-TIJARIA's environment, lessons learned from previous security incidents and based on attendees' feedback.
- Specialized information security training sessions shall be scheduled and conducted according to the training curriculum.
- Specialized training sessions shall enable AL-TIJARIA employees, end users, to effectively contribute to the implementation and improvement of AL-TIJARIA's information security management system, as well the implications of not complying with the Information security Policy requirements.
- In coordination with HR, a post-training evaluation shall be performed to assess if the objectives of the training have been achieved and that the attendees are equipped with sufficient knowledge to apply in practice.
- Records of the conducted training sessions and the attendees shall be maintained by the HR Department. Receiving the specialized information security training session on the protection/handling of a particular information system or asset shall be a prerequisite for granting access to that particular information asset or system to the role-holder in order to perform their assigned duties.