

INFORMATION SECURITY MANAGEMENT POLICIES MANUAL

EPL House

manual code: EPL House -ISMSM-policies

Table of contents

|  |  |  |
| --- | --- | --- |
| # | Contents | Page Number |
|  | The objective of the information security system | 2 |
|  | Application scope of the ISO 27001 | 2 |
|  | Concepts & Shortcuts | 2 |
|  | Competencies | 4 |
|  | Responsibilities and Powers | 7 |
|  | Controls in accordance with the international standard ISO 27001 Information Security | 10 |
|  | Reference | 38 |
|  | Forms | 38 |
|  | Key Performance Indectors (KPI’s) | 39 |
|  | Versions & Revisions | 39 |
|  | Approvals | 39 |

1. **Information security system objectives:**

* Establishing responsibility and accountability for information security at the Al Qarib Company
* Employees awareness by clarifying the powers and responsibilities related to information security.
* The ability to deal with and reduce the occurrence of information security breakthroughs.
* Providing important services continuously in the event of information security incidents.
* Ensuring company compliance with applicable laws and regulations, including ISO 27001:2022.
* Ensure the implementation of the laws & regulations necessary to provide appropriate protection for the confidentiality, integrity and availability of company information assets.

1. **Application scope of the ISO 27001**

* Scope of application of the system: “At the level of all departments in the Al Qarib Company & under the supervision of IT Department, which includes: networks, technical support, systems and database, systems development, electronic services in accordance with the issued information security policy.

1. **Concepts & Shortcuts:**

|  |  |
| --- | --- |
| Concepts | Defenitions |
| Accountability | The security principle states that individuals should be able to identify themselves and be responsible for their actions |
| Access rights / privileges | User access rights (or access privileges) Know what actions the user is allowed to do when accessing information assets |
| Assets | Assets are anything that can be useful to the company |
| Asset owner | The person or entity authorized to make decisions related to the asset |
| Authentication \ Reliability | Confirmation that the person who impersonates a specific trait is actually the owner of that trait |
| Availability | The accessible property is usable on demand |
| Privacy | Ownership of information that is not available or disclosed to unreliable parties or entities |
| Control | It is a means of managing risks, including policies, procedures, guidelines, etc., which can be of a managerial, technical or legal nature. |
| Encryption | Convert readable text to unreadable form |
| The incident | Any event (or activity) that has the potential to damage the security of one or more of the company's assets |
| Information Security | Protecting information and information systems from illegal access, use, disclosure, modification and destruction in order to ensure the confidentiality, validity and availability of (the information) |
| logging (event logging) | Create and store specific information about the activities that occurred on the system |
| Malware (malicious code) | Software used to disable a computer, collect sensitive information, or gain unauthorized access to computer systems. |
| Penetration test | Attempting to gain control and intrusion into a computer system, simulating the methods and techniques of malicious attackers, to determine how a real attacker could hack the system; And what harm can it cause? |
| Danger | Risk is the combination of the probability of an event occurring and the consequences of its occurrence |
| Third side | That person or body recognized as being independent of the parties concerned, in relation to the concerned matter |
| Threat | The threat has the potential for an unwanted event that could damage the system |
| Vulnerability | Vulnerability is defined as a weakness associated with the company's assets |

|  |  |
| --- | --- |
| Shortcuts | Defenitions |
| Company | Al Qarib |
| CCTV | Closed circuit television |
| IPS | Intrusion prevention system |
| IRT | Incident Response Team |
| ISO | International Standards Organization |
| ISSC | Information Security Steering Committee |
| ISMS | Information Security Management System |
| RA | Risk assessment |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| SAT | Security Awareness Training |
| SLA | Service level agreement |
| SoD | Separation of duties |
| UPS | Uninterruptible power supply |

1. **Competencies:**

* To determine the necessary competency of those responsible for managing information security and to ensure that these persons are qualified on the basis of appropriate education, training, or experience. Those responsible for innovation activities are evaluated according to the required competencies on an annual basis, identifying gaps and working to meet the requirements according to the following competency assessment matrix model:

**IT Team Leader**

**Major Task**

* Manage the schedule of the technical team in terms of project deliveries
* Divide & assign task to the IT team
* Attends meetings as per client’s request
* Looking for new technologies to implement

**Minor Task**

* Same as the senior web developer tasks

**Years of Experience**

* Minimum of 5 years + of experience

**Education**

* Bachelor of Computer Science
* Project Management Certification

**Sr. Web Developer**

**Major Tasks**

* Web Development using .NET C#, MVC framework and all related technologies
* Front-end development – slicing PSD design into valid HTML5 mark-up and providing rich user interaction using JavaScript and modern CSS animations, Responsive designs developments
* Application Development based on customer’s requirements
* Analyze business requirements and transform them into technical design
* Web Services/ API’s development and backend integration
* Proactively provide creative ideas and solutions towards the improvement of the company products and interact with business development and marketing team to understand the business requirements
* Assess risk and impact on the existing systems that may arise due to any requirement or functional change
* Look after improving the current CMS functionalities, and security
* Provide Second level supports to clients
* SharePoint implementation
* Be able to support and coach junior developers in solving development issue

**Minor Tasks**

* Managing & securing the servers
* Handling firewalls & anti-virus
* Monitoring & giving access to users on demand
* Maintaining the offices pcs, servers & peripherals

**Years of Experience**

* Minimum of 5 years + of experience

**Education**

* Bachelor of Computer Science

**Digital Communication Officer**

**Major Task**

* Website CMS Update
* SharePoint CMS Updates
* HTML Development
* Design Restyling
* Images & Banners editing & Resizing
* Clients Communications
* Ability to train users on the systems implemented by us
* Ability to provide benchmark reports based on requests.

**Minor Task**

* Maintaining website updates & reports
* Maintaining testing reports
* Maintaining & documentation of enhancements requirements

**Years of Experience**

* Minimum of 3 years + of experience

**Education**

* Bachelor of Computer Science Or Business

**Computer Engineer**

**Major Task**

* System Analyst
* Technical Documentation
* HTML Development
* Content Management System Operation
* Technical Support
* Training
* Systems Development

**Minor Task**

* Training Documentations
* Data Gathering
* Testing

**Years of Experience**

* Minimum of 3 years + of experience

**Education**

* Bachelor of Computer Science

1. **Responsibilties & Powers:**

|  |  |  |  |
| --- | --- | --- | --- |
| # | **Job** | **Responsiblities** | **Powers** |
|  | **Network Administrator** | * Defining network and server processing systems and supplies. * Continuous updating of the network and server and ensure their readiness. * Install, check and operate operating systems, network supplies and systems. * Control access to the network, information and other operational systems and their uses with the competent authorities in coordination with the concerned parties. * Updating the work of the main network, the internal network, all computers, technology and the various support systems used. * Implementation of electronic interconnection programs between all software sub-systems in the company. * Ensure information security, prepare alternative software in case of emergency, monitor network traffic, prioritize blocking operations, general monitoring, control and deal with intrusions. * Periodic and preventive maintenance of devices and auxiliary operating systems to ensure their readiness and follow-up performance, modification and updating to ensure the achievement of the required efficiency. * Perform any other tasks assigned to him related to the nature of work | * Comprehensive power to control and manage servers and network devices * The authority to manage the firewall . * The authority to create email accounts for employees and departments |
|  | **Master Programmer** | * Suggesting mechanisms for the continuous development of the programs and applications used in the Company. * Monitoring and developing standards and policies for IT operations and controlling their quality. * Contribute to determining the software needs of the systems needed by the company. * Contribute in designing modern systems and applications and their adaptation to serve business objectives and requirements. * Contribute analysising programs performance and the necessary corrective actions to be taken in cases of programs deficiencies. * Communicate with users to gather information about their needs for the necessary information systems and applications. * Selecting the software and hardware to be purchased and evaluating their quality, compatibility and prices. * Perform any other tasks assigned by the direct manager. | * Access to software servers * Access to the main servers * Authority to amend and update management policies and procedures * Authority to issue purchase orders for software and systems * The authority to approve technical reports for programs and systems |
|  | **Infrastructure Administrator** | * Follow up system backup * Follow the antivirus system * Follow servers * Monitor network devices * Follow up on phones * Research new technologies * Technical support * Follow up on the company's website * Perform any other tasks assigned by the direct manager. | * Comprehensive power to control and manage servers and network devices * Ability to generate reports for servers and network devices * Ability to scan network and servers for vulnerabilities * Validity of experiments and studies to research and develop new systems compatible with the company's operating systems * The authority to monitor, verify and amend employee permissions * Create, modify and copy databases. (database management) * Access to software servers. (Manage Software Servers) |
|  | Heads of Departments | * Ensure that management personnel adhere to relevant information security controls, procedures, standards and guidelines. * Ensuring that the department's employees receive appropriate training in the field of information security awareness. * Understand and adopt information security manuals, policies, procedures, standards and guidelines and perform their duties in accordance with them. | * Monitor and evaluate the performance of employees within the department * Define performance indicators for each employee |
|  | Asset User | * Adhere to all security policies, manuals, procedures and standards relevant to his role. * Attending security awareness sessions. * Understand and adopt information security manuals, policies, procedures, standards and guidelines and perform his duties in accordance with them. | * Use information assets responsibly, in accordance with the appropriate usage policy. * Report suspected security incidents, poor security and policy violations |
|  | Asset Owner | * Adhere to all security policies, manuals, procedures and standards relevant to his role. * Attending security awareness sessions. * Understand and adopt information security manuals, policies, procedures, standards and guidelines and perform his duties in accordance with them. | * Use information assets responsibly, in accordance with the appropriate usage policy. * Report suspected security incidents, poor security and policy violations |

1. **Controls in accordance with the international standard ISO 27001 Information Security:**

|  |
| --- |
| **Information security incident management policy and procedures** |
| **1 Policy Statement**   * Incident Management policy shall enable the response to a major incident or disaster by implementing a plan to restore the critical business functions of Al Qarib. The number of computer security incidents and the resulting cost of business disruption and service restoration rise with the increase in dependence on IT-enabled processes. Implementation of sound security policies, blocking of unnecessary access to networks and computers, improvement in user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce such risks and decrease the cost of security incidents.   **2 Purpose**   * The purpose of the incident management policy is to provide company-wide guidance to employees on the proper response to, and efficient and timely reporting of, computer security-related incidents, such as computer viruses, unauthorized user activity, and suspected compromise of data. It also addresses non-IT incidents such as power failure. Further, this policy provides guidance regarding the need for developing and maintaining an incident management process within Al Qarib.   **3 Scope**  **3.1 Employees**   * This policy applies to all Employees, Contractors, and Third-Party Employees, who use, process, and manage information from individual systems or servers.   **3.2 Documentation**   * The documentation shall consist of Incident Management Policy, and related procedures.   **3.3 Document Control**   * The Incident Management Policy document and all other referenced documents shall be controlled. Version control shall be to preserve the latest release and the previous version of any document. However, the previous version of the documents shall be retained only for a period of two years for legal and knowledge preservation purposes.   **3.4 Records**   * Records being generated as part of the Incident Management Policy shall be retained for a period of two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year.   **3.5 Distribution and Maintenance**   * The Incident Management Policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned. The maintenance responsibility of the document shall be with the system administrators.   **4 Privacy**   * **The Incident Management Policy document shall be considered as “confidential” and shall be made available to the concerned persons with proper access control. Subsequent changes and versions of this document shall be controlled.**   **5 Responsibility**   * The Incident Management Policy shall be implemented by the designated personnel. The primary responsibilities associated with incident management are to identify and respond to suspected or known security incidents, contain or limit the exposure to loss, and mitigate (to the extent practical) the harmful effects of security incidents. The IT department will manage incidents at the company level, an IT department security representative shall be assigned to facilitate the handling of security incidents. The nature of the incident may require the assignment of staff from other divisions/offices. In all cases, top management shall be informed of the incident and the steps recommended or taken to mitigate the incident.   **6 Policy**   * The top management shall ensure that:  1. Incidents are detected as soon as possible and properly reported. 2. Incidents are handled by appropriate authorized personnel with ‘skilled’ backup as required. 3. Incidents are properly recorded and documented. 4. All evidence is gathered, recorded and maintained in the Security Incident Reporting form that 5. will withstand internal and external scrutiny. 6. The full extent and implications relating to an incident are understood. 7. Incidents are dealt with in a timely manner and service(s) restored as soon as possible. 8. Similar incidents will not recur. 9. Any weaknesses in procedures or policies are identified and addressed. 10. All incidents shall be analyzed and reported to the designated officer. 11. Learning from the incidents are recorded.  * The policy shall apply throughout the company, including information resources, data stored and processed on those systems, data communication and transmission media, and personnel who use information resources.   **7. Implementation**   * This shall develop, maintain and implement an incident management and response plan that addresses information technology security incidents. The following paragraphs specify the incident management plan requirements. These requirements shall be in compliance with relevant State and policies and standards.  1. **Incident Management Training:**  * This shall provide incident management training to the Divisions/Offices on how to identify and report security incidents.  1. **Identifying and Prioritizing Types of Incidents:**  * This will develop and maintain guidelines for identifying and prioritizing security incidents. The Divisions/Offices or their affiliated staff designated by agreement or assignment shall evaluate the potential for the occurrence of certain types of incidents. All security incidents shall be classified by severity level and type. The following five event severity levels as defined in the ITS Incident Response Standard shall be used for classification purposes. In addition, each incident shall be identified as to type: email, hacking, virus/worm, inappropriate use, social engineering and other.  1. **Incident Monitoring:**  * The Al Qarib shall develop and maintain guidelines on how to monitor for security incidents. The Divisions/Offices or their affiliated staff designated by agreement or assignment, as part of their risk management program, shall continuously monitor for security incidents (both physical and Technical – related incidents) according to the guidelines listed above.  1. **Incident Detection:**  * The IT department shall develop and maintain enterprise-wide procedures for collecting, analyzing, and reporting data. The integrity of all data relating to criminal acts must be preserved as possible evidence and collected.  1. **Incident Reporting:**  * The IT department shall define the basic procedure to be followed for reporting incidents. The procedure shall be expanded upon by the Divisions/Offices as necessary to include the internal communications and escalation procedures that will be used. Security incidents classified as level 3, 4, or 5 shall be reported to the top management and the related department within a period of 24 hours from the time the incident was discovered and Submit an incident report to take the suitable action.  1. **Organization Protocols:**  * Security incidents may occur across network boundaries. The IT department shall define the protocols for handling these incidents and the contacts between Divisions/Offices, state agencies and outsourced entities.  1. **Impact Assessment:**  * The IT department shall evaluate the impact of security incidents. Assessments may be required at various stages of the incident life cycle to assist management in deploying the proper risk management procedure.  1. **Documentation**:  * All security incidents shall be thoroughly documented by the Divisions/Offices with as much detail as possible to describe the incident, time discovered and impacted area for subsequent investigation. The incident report shall indicate who was notified and what actions were taken.  1. **Record Retention:**  * Divisions/Offices shall maintain the incident logs and corresponding documentation for a minimum of one year following the discovery of an incident or until an investigation is completed. Incident logs should be stored in a secure location.  1. **Post-Incident Analysis:**  * It is necessary to amend the risk register, assess the risk that occurred, and put preventive procedures to avoid such risks. * **Related forms \ documents:**  1. Incident Reporting Form for breaches of security or confidentiality 2. Risk Register |
| **Business Continuity and Disaster Recovery Policy** |
| * It how to recover quickly from service interruption or disaster, whether natural or man-made. This policy contains the set of best practices, standards, and guidelines to ensure proper risk management, which enables the Al Qarib to continue to deliver its services during a disaster. * Some of the key elements of this policy include the following: * It’s important to define what a disaster is for Al Qarib . This can vary widely, depending on the organization and industry. * There must be some ready-made plan for predictable disasters such as fire, earthquakes, or breakdown of products. * Team responsibilities must be identified in order to reduce the response to the incident, which may help resolve the incident in the minimum amount of time. * The recovery plan for the data backup and storage of the device must be defined. |
| **Remotely Work** |
| * Remotely Work means that information and communication equipment is used to enable employees to perform their work outside the company. * Remote work must be authorized by the [direct manager] by sending the attached form indicating the permitted period and the method of entering the company's systems. * The [Network Administrator] is responsible for preparing plans and procedures to ensure the following: * Protection of mobile computing equipment as defined in the previous clause. * Prevent unauthorized access to persons who live or work in the location where the remote work activity is carried out. * The appropriate arrangement of the local network used to connect with the Internet * Protect the Company's intellectual property rights, either to software or other materials that may be protected by intellectual property rights. * A process for recovering data and equipment in the event of termination of service (employment).   Forms used:   1. Remote work permit |
| **Acceptable Use Policy** |
| Purpose and scope:  The purpose of this document is to define clear rules for the use of the information system and other information assets in the company  This document applies to the entire scope of the information security management system, ie to all information systems and other information assets used within the scope of the information security management system.  The users of this policy are all employees of the company |
| **Controls regarding the acceptable use of information assets** |
| Prohibited Activities:   * Prohibit the use of information assets in an unnecessary manner that consumes their capacity, undermines the performance of the information system, or poses a security threat. It is also prohibited: * Downloading image or video files that have no commercial purpose, sending email and chain messages, playing games, etc. * Installing software on the local computer without the express permission indicated by [Software and Systems Administrator]. * Use of Java applications, active EXE controls, and other mobile codes, unless authorized by [Software and Systems Administrator]. * Use encryption (encryption) tools on the local computer, except for the cases described (specified) in the Information Classification Policy. * Download the program code from external media. * Installing or using external devices such as modems, memory cards, or other devices to store and read data (such as flash drives) without the express permission and explanation of [Infrastructure Administrator], use is permitted in accordance with the Information Classification Policy * Taking the assets outside the company * Equipment, information or software, regardless of its shape or storage way, may not be transferred off-site without the prior written permission of the (Management Director). * As long as the above assets are outside the Company, they must be monitored by the person who gave permission to take them out. * Returning assets upon expiry of the contract  1. Upon termination of the employment contract or any other contract on the basis of which various equipment, software or information is used in electronic or paper form, the user must (return) all such information assets to the [infrastructure administrator].  * Backup procedure  1. The user should back up as per the backup procedure of all sensitive information stored on his computer at least once a day.  * Antivirus protection  1. Security and antivirus software must be installed by [Infrastructure Administrator] on each computer with automatic updates enabled.  * Permits (licenses) to use the information system  1. Information system users can only access information system assets that have been authorized to them by the asset owner 2. Users can use the information system only for the purposes for which they have been authorized, that is, for which they have been granted access rights. 3. Users should not engage in activities that could be used to bypass information system security controls.  * User Account Responsibilities  1. The user must, directly or indirectly, not allow another person to use his access rights, i.e. the username, and must not use the username (and/or) password of another person. The use of a user group (group user names) is prohibited. 2. The owner of the User Account is its User, who is responsible for its use, and all operations performed through this User Account.  * Software installation restrictions  1. It is prohibited to install the software on a local computer without the express and indicated permission of [Program and Systems Administrator]. 2. When installing new software, it must be included in the asset inventory. 3. The list of installed programs should be reviewed periodically every six months and uninstalled unwanted programs.  * Password Responsibilities  1. Users should implement good security practices when selecting and using passwords: 2. You must not disclose passwords to other people, including administrators and system administrators. 3. Passwords should not be typed, unless a secure method is approved by the [Information Security Officer] 4. Passwords provided to users must not be distributed through any channel (verbal use, written or electronic distribution, etc.). 5. Passwords should be changed if there are indications that passwords or the system have been compromised - in which case a security incident should be reported. 6. Strong passwords should be chosen, as follows:  * Use at least 8 characters. * Use at least one numeric character. * Use at least one uppercase letter and at least one lowercase letter of the alphabet. * Use at least one special character. * The password must not be a dictionary word, dialect, or dialect of any language, or any of these words spelled backwards. * Passwords should not be based on personal data (such as date of birth, address, names of family members, etc.). * You should not reuse the last three passwords.  1. Passwords must be changed every 3 months. 2. The password must be changed at the beginning of logging in to the system. 3. Passwords should not be stored in an automated login system (such as a macro or browser). 4. Passwords used for private purposes should not be used for commercial purposes. |
| **Disposal & Destruction Policy** |
| * Purpose and scope: * The purpose of this document is to ensure that information stored on equipment and media is safely destroyed or erased. This document applies to the entire scope of the information security management system, ie to all information technology as well as documents within the scope. * The users of this document are all employees of the company. |
| **Controls related to the policy of disposal and destruction** |
| 1. Disposal and destruction of equipment and media  * All licensed data and software stored on portable storage media (such as CDs, DVDs, data memory drive, memory stick, papers , etc.) and on all equipment containing storage media (such as computers, mobile phones, etc.) Erase or destroy media before disposal or reuse. * The person responsible for the data erasure/destruction of the media shall inform the responsible asset owner regarding the data erasure/destruction, and the asset owner shall inform the asset owner   1. **Equipment:** * [Infrastructure Administrator] is responsible for checking and erasing data from equipment, unless the information classification policy describes it differently. The data must be erased but if the process of erasing the data is not secure enough due to the sensitivity of the data, then the media storage must be destroyed.   1. **Portable Storage Media:** * [Network Administrator] is responsible for erasing data from portable storage media, unless the information classification policy is described differently. The data must be erased but if the erasure process is not secure enough due to the sensitivity of the data, then the storage media must be destroyed.   1. **Paper Media:** * Employees of the company who deal with individual documents are responsible for the destruction of paper documents unless the information classification policy is described differently. Paper documents are destroyed in paper shredders.   1. **Erase and destroy records; Information Destruction Committee:** * Deletion/destruction records must be kept for all data classified as "restricted" and "confidential". Records should include the following information: media information, erasure/destroy data, erasure/destroy method and the person who performed the operation. * All information classified as “confidential” must be erased/destroyed in the presence of a committee consisting of persons authorized to access the said information. Forms used: [Records erase/destroy] |
| **Asset Disposal** |
| * Asset disposal is the act of obsoleting unwanted equipment or assets in a safe manner. A large volume of data is being transferred and stored on computer systems and the security of this information is essential, even when the data is being removed. If the information is not properly removed before the disposal of asset, it could be accessed and viewed by unauthorized personnel. * Hence, organizations need to write an organizational policy that covers the disposal of information assets. A few key points that need to be covered in this asset disposable policy are the following: * Media sanitization procedures: All the electronic media must be properly sanitized before it is transferred from the custody of its current owner. The proper sanitization method depends on the type of media and the intended disposal process of the media. * **Such as ,** if you are sharing the hard drive from one department to another, it must be formatted before being reused to ensure security of the data. * Destruction of electronic media: Destruction of electronic media is the process of physically damaging the medium so that it cannot be reused by any device that may normally be used to read electronic information, such as computers, hard drives, pen drives, etc. * Repairing hard drives under warranty: In a special situation where a hard drive under warranty has failed and the manufacturer requires that the failed disk drive be returned, an appropriate Business Associate Agreement between the manufacturer and organization must be in place before the drive can be shipped to the manufacturer. If the manufacturer will not sign a Business Associate Agreement, the old drive must be properly destroyed. * Disposal of damaged media: The first attempt should be to overwrite the hard drive or other media device. If it cannot be overwritten, the hard drive must be disassembled and mechanically destroyed so that it is not usable. * External party: You can choose from many companies that will remove your media, but you need to make sure that the provider you select agrees to the non-disclosure agreement (NDA) and follows it. |
| **Asset Management Policy** |
| * This document describes the asset management policy for all IT and non-IT assets of the organization. The policy covers all information assets, such as hardware, software, and data. As the name suggests, the key component of this policy is management and it should cover: * Identification and inventory of all the assets and relevant information about their location, backup, business value, criticality, etc. For example, these assets can be: * Information assets such as databases, contracts, agreements, manuals, policies, plans, etc. * Software assets such as system software, application software, utilities, etc. * Hardware assets such as computer hardware, servers, communication services, removable media devices, etc. * Personnel assets such as people, their qualifications, and the skills, etc. * Every asset should have a designated owner, which could be a person, a business process, an application. * This covers the monitoring and tracking of all the assets during their lifespan with the organization. |
| **Work In Safe Areas** |
| * **Purpose and scope:** * The purpose of this document is to define basic rules of conduct in safe areas. * This document applies to all secure areas of the Information Security Management System. * The users of this document are all employees of the company |
| **Incident Management Policy** |
| * This purpose of this policy is to define how the incident can be managed and reported in the organization. It should cover: * Security Incident Management Practice Standard. Such as : * Whenever a security incident occurs in the organization, report it to the information security team or IT team with the corrective and preventive actions. * Define who is responsible for initiating, completing, and documenting the incident investigation. * Define the incident reporting flow. * Store the incident information for learning and for future |
| **Controls Related To Working In Safe Areas** |
| Rules for safe areas  * 1. **List of safe areas :** Existing safe areas that require special rules are the following: * Network server rooms. * The safe for storing the storage media and the master passwords, which is located in the (IT Department Store) * The persons responsible for each safe zone are recorded as asset owners in the asset holdings.   1. **Right to access safe areas:** Access to safe areas is approved according to the Access Control Policy   2. **Access Controls:** Access to secure areas is protected by the following access controls:   3. **Visitor access:** * Persons who are not working in the company (add: visitors) must obtain access permission according to the access control policy. * Visitors can enter the safe areas and stay in those areas only in the presence of the competent employee - this employee must accompany the visitor throughout his stay in the safe area. * The exact time of entry and exit of visitors from the safe areas will be recorded by [Network Officer Specialist].   1. **Prohibited activities (banned)**   + It is not allowed in safe areas to: * Perform any kind of photography, audio or video recording. * Connect any electrical device to a power source unless it has been given special permission to do so. * Touching or in any other way tampering with any equipment installed in safe areas unless he has been given special permission to do so. * Connect any device to a network unless it has been given special permission to do so. * Archiving a large amount of paper material. * Storage of flammable materials or equipment. * • Use any type of heating device. * Smoking, eating or drinking |
| [ IC Card Reader Records ] - [ Recordings from CCTV Cameras] - [ Name of Visitor Records ] |
| Forms: [List of persons authorized to access document] |
| Information Classification Policy |
| Purpose, Scope and Users:The purpose of this document is to ensure that information is protected at an appropriate level.This document applies to the entire scope of the information security management system, that is, to all types of information, regardless of format - paper or electronic documents, applications and databases, employee knowledge, etc. |
| Controls related to the classification of information |
| 1. **Classified information**    1. Steps and Responsibilities   The steps and responsibilities for managing information are as follows:   |  |  | | --- | --- | | **Step Name** | **Responsibility** | | 1. Entering the information asset in the (assets inventory). | Asset owner | | 2. Classification of information | Asset owner | | 3. Description (Paste tag) Information | Asset owner | | 4. Information handling | Persons with access rights |   If confidential information is received from outside the company, [Senior Operations and Information Security Administrator] is responsible for classifying it according to the rules set forth in this policy, and this person becomes the owner of the information origin.   * 1. **information classification**      1. **Classification criteria**   + The level of confidentiality is determined based on the following criteria:  1. The value of the information - based on the effects assessed during the risk assessment. 2. Sensitivity and importance of information - based on the highest degree of risk calculated for each information item during the risk assessment. 3. Legal and Contractual Obligations - Based on [List of Legal, Regulatory, Contractual and Other Obligations]    * 1. **Confidentiality levels**   All information must be classified into confidentiality levels.   |  |  |  |  | | --- | --- | --- | --- | | **Access Restriction** | **Classification criteria** | **Description (Paste Tag)** | **Confidentiality levels** | | Information is publicly available | Making information public can not harm the company in any way and data provided by government or private sector data to individuals, provided that it is freely or subject to a minimum, or used or exchanged with third parties. | (no tag) | Open | | Information available to select employees and partners | Unauthorized access to information may cause minor damage and/or inconvenience to the company and unrestricted disclosure or exchange data may cause limited harm to organizations and individuals in the public or private sector such as:   * Limited damage to assets, or limited financial loss to an entity, company or individual * It reduces the competitiveness of companies and negatively affects the principle of equal opportunities | Private | Private | | The information is only available to a certain group of employees and partners who are authorized to view | Unauthorized access to information may substantially harm the business and/or its reputation and unrestricted disclosure or exchange data may cause significant harm to government agencies, companies or individuals such as:   * Breach of privacy by disclosing sensitive personal information, such as records to employees. * A significant decrease in the ability of organization to perform its functions, or significant damage to its assets. * or a large financial loss that causes great harm to companies that can lead to a loss of competitiveness * Or losing some of its basic cognitive and intellectual advantages, or incurring huge financial losses in the operational effectiveness of the relevant organization. * Significant damage to relations with clients leading to the imposition of official sanctions. | Sensitive | Sensitive | | The information is only available to specific individuals in the company | Unauthorized access to information may cause irreparable disaster for the company and its reputation and disclosure data or unrestricted exchange that may cause very significant harm to government agencies, companies or individuals, such as:   * Disclosure of any VIP personal information (very important) * Violation of any intellectual property rights of VIPs has a significant or noticeable negative impact on the higher interests of the state. * - A sharp decline in the company's ability to carry out its functions, or very large damage to its assets, severe financial loss, and loss of customers' confidence. | Confidential | Confidential |  * + The basic rule is to use the lowest level of confidentiality ensures an adequate level of protection, so as to avoid the protection of unnecessary costs.     1. **List of authorized persons**   Information classified as "sensitive" and "confidential" must be accompanied by a list of authorized persons so that the the department manager determines the names or job functions of the persons who have the right to access that information.  The same rule applies to the level of confidentiality "internal use" if people outside the company will have access to such a document.   * + 1. **Reclassification**   Asset owners should review the confidentiality level of their information assets every [two years] and assess whether the level of confidentiality can be changed. If possible, the level of confidentiality should be reduced.   * 1. **Description (Paste Card) Information**   The levels of confidentiality are described as follows:   * **Paper documents** - The level of confidentiality is indicated in the upper left corner of each document page. Also indicated on the front of a cover or envelope holding such a document is the filing folder in which the document is stored. * **Electronic documents** - the level of confidentiality is indicated in the upper left corner of each document page. * **Information systems** - the level of confidentiality in applications and databases must be indicated on the access screen of the system, as well as in the upper left corner (in the case of the Arabic version) of each successive screen that displays confidential information. * **Email** - The level of confidentiality is indicated in the first line of the email body. * **Electronic storage media** (disks, memory cards, etc.) – The level of confidentiality must be indicated on the upper surface of this media. * **Information Sent Orally** - Level of Confidentiality For confidential information to be sent in face-to-face contact, by phone or some other means of communication, the information itself must be reported.   1. **Handling classified information** * All persons who access confidential information must follow the rules listed in the following table. The [Department Manager ] must initiate disciplinary action every time the rules are broken or if information is given to unauthorized persons. Every incident related to the handling of confidential information must be reported in accordance with Incident Management Procedures. Information assets may only be taken off the premises after authorization in accordance with the Acceptable Use Policy. The method for security erasure and destruction (destruction) of the media is specified in the document [ IT Operating Procedures ] / [ Disposal and Destruction Policy ].  |  |  |  |  | | --- | --- | --- | --- | |  | **Internal use** | **Restricted (selected)\*** | **Confidential (private)\*** | | **Paper documents** | * Only authorized persons have access * If sent outside the company, the document must be sent as registered mail * Documents can only be kept in rooms without public access * Documents must be removed from printers and fax machines at short intervals | * The document must be stored in a locked safe * Documents can only be transferred inside and outside the company in a sealed envelope * If sent outside the company, the document must be mailed with an acknowledgment of receipt service * Documents must be immediately removed from printers and fax machines * Only the owner of the document can copy the document * Only the owner of the document can destroy (destroy) the document | * The document must be stored in a safe place * The document can only be transferred inside and outside the company by a trustworthy person in a sealed and sealed envelope * Faxing the document is not allowed * The document can only be printed if the authorized person while standing next to the printer | |  | |  | | |  | |  | | **Electronic documents** | * Only authorized persons have access * When files are exchanged via services such as FTP, instant messaging, etc.., they must be password protected. * Access to the information system where the document is stored must be protected by a strong password * The screen on which the document is displayed should automatically turn off after a minute of inactivity | * Only persons authorized for this document can access the part of the information system where this document is stored * When files are exchanged via services such as FTP, instant messaging, etc., they must be encrypted * Only the owner of the document can erase the document | * The document must be stored in encrypted form * The document can only be stored on servers controlled by the company * The document must not be exchanged by services such as FTP, instant messaging, etc. |  | |  | |  | |  | | **Information systems** | * Only authorized persons have access * Access to the information system must be protected by a strong password * The screen should turn off automatically after a minute of inactivity * The information system is located only in rooms with physical access control | * Users must log out of the information system if they have temporarily or permanently left the workplace * Data should only be erased with an algorithm that ensures secure deletion | * Access to the information system must be controlled through the authentication process (proof of authenticity) using smart cards or biometric readers. * The information system can only be installed on servers controlled by the company * The information system is located only in rooms with physical access control and the identity of persons to access the room |  | |  | |  | |  | | **E-mail** | * Only authorized persons have access The sender must carefully verify the recipient * All rules stipulated under the heading “Information Systems” apply | * Email must be encrypted if sent outside the company | * All emails must be encrypted |  | |  | |  | | **Electronic storage media** | * Only authorized persons have access * Media or files must be password protected * If sent outside the company, the media must be sent as a registered mail * Media are only kept in rooms with physical access control | * Media and files must be encrypted Media must be stored in a locked cabinet * If sent outside the company, it must be mailed with acknowledgment of receipt service * Only the owner of the media can delete or destroy (destroy) the media | * The media must be stored in a safe place * Media can be moved inside and outside the company only by a trustworthy person in a closed and sealed envelope |  | |  | |  | |  | |
| Forms: [List of persons authorized to access documents [ |
| Access control |
| * The purpose of this document is to define rules for access to various systems, facilities and equipment, based on business and security requirements for access. * This document applies to the entire scope of the Information Security Management System, ie to all systems, equipment, facilities and information used within the scope.  The users of this document are all employees of the company . |
| **Data Retention and Disposal Policy** |
| * This policy tells you how securely the data is retained and how you dispose of data when it’s no longer needed. This policy should document the lifespan of data. Such as how long is the log file data kept for record purposes. * This policy should cover the following points: * How the data is collected and kept securely in compliance with the law and with organizational policy. * The business should capture the minimum user data required for the business operation after getting consent from their users/employees. * How stored data access is managed in the organization. * An organization must have the guidelines and statutory procedures for records retention. Such as :   + The organizational records containing sensitive information that are not being used for active business should be archived until retention requirements have been met.   + If relevant, only primary records should be archived. The duplicate records maintained elsewhere multiple times may be considered for archival.   + Similarly, organizations have guidelines for the disposal of records and data. For example:   + When retention requirements have been met, records must be either immediately destroyed or placed in secure locations.   + Before disposing of the data or any other assets, get the required approvals to avoid any miscommunication. |
| Controls related to access control policy |
| 1. **Introduction**   The basic principle is that access to all systems, networks, services and information is prohibited, unless expressly permitted by individual users or user groups. There must be a user registration procedure for each system and service.  Access to all physical areas of the company is permitted, except for areas that must be franchised by an authorized person (" privilege management" clause).  This policy specifies rules for accessing systems, services and facilities, while the Information Classification policy specifies rules for accessing individual documents and recordings.   1. **User Profile**   The user's access permissions are defined by the user profile form in the access control policy   1. **Privilege Management**   The privileges and rights in relation to the personal files of the users mentioned above are allocated so that the head of each department is responsible for granting and revoking rights and powers to the special systems of his department, and must take into account the business and security requirements for access (defined in the risk assessment), as well as the classification of information that It is accessed with access rights, in accordance with the Information Classification Policy.   1. **Regular review of access rights**   The (Information Security Officer) shall review every six months whether the granted access rights are in line with business and security requirements and shall be placed in a special register for regular review.   1. **Change of status or termination of a contract**   Upon a change of employment or dismissal, the responsible persons who have approved benefits for the employee concerned must be immediately notified.  When changing contractual relationships with third parties who have access to systems, services, and facilities, or upon the termination of the contract, the contract holder must immediately inform the responsible persons who have approved the benefits for the relevant third parties.  The access rights of all persons whose employment status or contracting relationship has changed shall be immediately removed or changed by the persons responsible as defined in the following clause.   1. **Technical implementation**  * The technical implementation of allocating or removing access rights is carried out by persons proposed by the of the concerned department manager through an e-mail sent to him. * Persons listed in this table may not freely grant or remove access rights, but only based on the user profiles specified in this policy, and requests by authorized (authorized) persons to assign privileges.  1. **User password management**   When assigning and using user passwords, the following rules must be complied with:   * By signing a Statement of Acceptance of Information Security Management System Documents, Users also accept the obligation to maintain the confidentiality of passwords, as stipulated in this document. * The user can only use his or her own unique username. * Each user should have the option to choose his or her own password, wherever the application is accepted. * The temporary password used for the first login to the system must be unique and strong, as stipulated above. * Temporary passwords must be given to the user in a secure manner, and the identity of the user must be verified in advance. * The password management system should ask the user to change the temporary password on the first login - entering the system. * The password management system should ask the user to choose (set) strong passwords. * The password management system should require users to change their passwords every 3 months. * If the user requests a new password, the identity of the user must be determined by the password management system * The user must confirm receipt of the password * The password should not be visible on the screen during login. * If the user enters an incorrect password three times in a row, the system must block the account of the user in question. * Passwords generated by the software or hardware manufacturer must be changed during the initial installation. * Files containing passwords must be stored separately from application system data. |
| Forms: [Records of the regular review for access rights] |
| Email Usage Policy |
| * The purpose of this policy is to ensure acceptable use of email services provided by the Alqarib to its users/employees to conduct business in an ethical, legal, and lawful manner. It should cover the following points: * All components of the email system, including any messages created, sent, received, or stored locally on the user system or on the mail server in any form, are considered organizational property. * The company email system should not be used under any circumstances for the creation or distribution of any disruptive or offensive messages, including ones about race, gender, hair color, disabilities, age, sexual orientation, pornography, vulgar jokes, religious beliefs and practice, and political beliefs or national origin. * The employee should not forward any viruses or hoax email messages to company email addresses and groups that they receive through their company or personal email address. These messages must be immediately reported to the IT Helpdesk. * The employee should not use company email to infringe on the copyright or other intellectual property rights of others. * The employee should not distribute abusive, fraudulent, or harassing messages and avoid writing messages in any unethical, illegal, or wrongful manner. |
| Password Policy |
| * The purpose of this document is to describe (set) rules to ensure secure password management and the secure use of passwords (passwords). * This document applies to the entire scope of the information security management system, ie to all workplaces and systems within the scope of the system.  Users of this document are all employees of the company. |
| Password policy controls |
| 1. **User Obligations**   Users should implement good security practices when selecting and using passwords:   * Passwords must not be disclosed to other people, including administrators and system administrators. * Passwords should not be typed, unless a secure method has been approved by the [Information Security Officer]. * Passwords provided to users must not be distributed through any channel (verbal, written or electronic distribution, etc.); * Passwords must be changed if there are indications that passwords or the system may be in risk (disclosure) – in those Case a security incident must be reported. * Strong passwords must be chosen, as follows: * Use at least eight characters. * Use at least one numeric character. * Use at least one uppercase letter and at least one lowercase alphabet letter. * Use at least one special character. * The password must not be a dictionary word, dialect or idiom of any language, or any of these words written backwards. * Passwords should not be based on personal data (eg date of birth, address, names of family members, etc.). * You must not reuse the past three passwords.   + - Passwords must be changed every 3 months.     - The password must be changed at the beginning of logging in to the system.     - Passwords should not be stored in an automated login system (eg a macro or a browser).     - Passwords used for private purposes must not be used for business purposes.  1. **User password management**   When assigning and using user passwords, the following rules must be followed:   * + - By signing a Statement of Acceptance of Information Security Management System Documents, Users also accept the obligation to maintain the confidentiality of passwords, as stipulated in this document.     - The user can only use his or her own unique username.     - Each user should have the option to choose his or her own password, wherever the application is accepted.     - The temporary password used for the first login to the system must be unique and strong, as stipulated above.     - Temporary passwords must be given to the user in a secure manner, and the identity of the user must be verified in advance.     - The password management system should ask the user to change the temporary password on the first login - entering the system.     - The password management system should ask the user to choose (set) strong passwords.     - The password management system should require users to change their passwords every 3 months.     - If the user requests a new password, the password management system must specify an identity     - The user must confirm receipt of the password     - The password should not be visible on the screen during login.     - If the user enters an incorrect password three times in a row, the system must block the account of the user in question.     - Passwords generated by the software or hardware manufacturer must be changed during the initial installation.     - Files containing passwords must be stored separately from application system data.  1. **Master passwords**    * + Master passwords are kept in a closed, sealed file that is kept in the special safe located in the office of the department manager.      + In the event of a need to use it, a request must be submitted explaining the reasons for it, and the file is opened in the presence of the department manager.      + When changing the person responsible for the master passwords, a change of passwords must be done      + The persons responsible for the master passwords are the department manager [Information Security Officer]      + Strong passwords must be chosen, as follows:      + Use at least 14 characters.      + Use at least one numeric character.      + Use at least one uppercase letter and at least one lowercase alphabet letter.      + Use at least one special character.      + The password must not be a dictionary word, dialect or idiom of any language, or any of these words written backwards.      + Passwords should not be based on personal data (eg date of birth, address, names of family members, etc.).      + You must not reuse the past 3 passwords |
| Office and Computer Screen Empty (Cleanliness) Policy |
| * **Purpose, Scope and Users** * The purpose of this document is to define rules to prevent unauthorized access to information on premises as well as common facilities and equipment. * This document is applied to the entire scope of the information security management system, ie to all workplaces, facilities, and equipment within the scope of the system.  The users of this document are all employees of the company |
| Controls regarding desk and computer screen cleanliness policy |
| 1. **Office and computer screen clearance policy**  * All classified information as defined in the Information Classification Policy is considered sensitive in this Office and Computer Screen Clearance Policy.   1. **workplace protection**      1. **Office cleanliness policy**   If the authorized person is not at his workplace, all paper documents, as well the data storage media classified as sensitive, must be removed from the office or other places (printers, fax machines, copiers, etc.) to prevent unauthorized access.  These documents and media must be stored in a secure manner in accordance with the Information Classification Policy.   * + 1. **Computer Screen Empty ( cleanliness ) Policy**   If the authorized person is not at his workplace, all sensitive information must be removed from the screen, and access to all systems for which the person has authorization must be denied.   * In case of short absences (up to 30 minutes), the screen-Empty policy is implemented by logging out of all systems or locking the screen with a password. If the person is absent for a longer period of time (more than 30 minutes), the screen-free policy is implemented by logging out of all systems and locking the workstation (device). |
| Operational (work) policy of the Information Technology Department |
| * Purpose, Scope and Users * The purpose of this document is to ensure the proper and secure functioning of information technology.  This document applies to the entire scope of the Information Security Management System, ie to all IT functions, as well as related documents within the scope. |
| Controls related to the operation (work) of the Information Technology Department |
| 1. **Every change to operating or production systems must be made in the following manner:**    1. The change can be introduced by the person who needs the change required for operational purposes    2. The change request is made through the Change Management System (Manage Engine).    3. The change request is distributed to the departments Managers, and then the request is accepted by the department responsible for the change request    4. The change request is reviewed by the department manger which concerned with the change, who must evaluate his justification for action    5. The change must be authorized by the [Information Technology Department manager and Information Security Officer], who must evaluate its rationale for action and potential negative security implications.    6. The change must be carried out by the person authorized by the department manager which concerned with the change    7. The concerned department manager is responsible for verifying that the change has been implemented as per the requirements.    8. The concerned department manager is responsible for testing and checking the stability of the system - the system should not be put into production before a comprehensive test has been carried out.    9. The implementation of changes must be reported to the following persons: [ Information Technology Department manager and Information Security Officer].    10. Change records are maintained by the change management system. 2. **Network Security Management**  * [Network Administrator] is responsible for managing and monitoring computer networks, to ensure the security of information in networks, and to protect services connected to networks from unauthorized access. Therefore it is necessary:   1. To separate operational responsibility for the networks of responsibility for sensitive applications and other systems.   2. Protect sensitive data passing through the public network   3. Protect sensitive data passing through wireless networks   4. Protection of equipment connected to the network from remote sites   5. Separation of traffic coming from mobile devices, setting unique firewall policies, static routes, workable local networks, etc.   6. Ensure availability of network services   7. [Network Administrator] Must regularly monitor and test the implemented controls.  1. **Network Services**  * [Infrastructure Administrator] have to determine the expected security and service level characteristics of all network services, whether these services are provided internally or from external sources – these requirements must be documented with service providers. * If the network services are outsourced, then the requirements must be specified in the agreement as specified in the supplier's security policy.  1. **Disposal and destruction of equipment and media**  * All licensed data and software stored on portable storage media (eg CD, DVD, data memory drive, memory stick, etc.; also on paper) and on all equipment containing storage media (eg computers, mobile phones, etc.). Media must be erased or destroyed before disposal or reuse. * The person responsible for data erasure/destruction of media shall inform the responsible asset owner regarding the data erasure/destruction, and the asset owner shall inform the asset owner.   1. **Equipment** * [Network Administrator] is responsible for checking and erasing data from equipment, unless the information classification policy is described differently. The data must be erased but if the process is not secure enough due to the sensitivity of the data, then the storage media must be destroyed.   1. **portable storage media** * [Network Administrator] is responsible for erasing data from portable storage media, unless the information classification policy is described differently. The data must be erased but if the erasure process is not secure enough due to the sensitivity of the data, then the storage media must be destroyed.   1. **paper media** * Company personnel who handle individual documents are responsible for destroying paper documents, unless the information classification policy is described differently. Paper documents are destroyed in paper shredders.   1. **erasure and destruction of records; Committee for information destruction** * Deletion/destruction records must be kept of all data classified as "restricted" and "confidential". Records must include the following information: media information, erasure/destroy date, erasure/destroy method, and the person who performed the operation. * All information classified as “confidential” shall be erased/destroyed in the presence of a committee consisting of persons authorized to access the said information.  1. **System Monitor**  * Based on the results of the risk assessment, [Operating System Administrator] decides which recordings will be saved on which systems and which systems, and how long they will be stored. Recordings must be saved for all administrators (supervisors) and system operators on sensitive systems. * [Operational System Administrator] is responsible for monitoring the automatic error report logs on a daily basis, as well as for recording errors reported by users, to analyze the cause of errors and take appropriate corrective actions. [Special permissions can be specified to take action in the event of an error, as well as how to keep error logs]. * [Operating System Administrator] is responsible for regularly reviewing the registry in order to monitor the activities of users, administrators and system operators. The review is held (performed) at specified intervals by the [Operating System Administrator], who specifie and select the recordings to be reviewed, and how the performed review will be recorded. [Operating System Administrator] Should be notified of the results of the review. |
| Forms: [Records Erase / Destroy ] |
| Change Management Policy |
| * **Purpose, Scope and Users** * The purpose of this document is to specify how to control changes to information systems. * This document applies to the entire scope of the information security management system, ie to all information technology within the scope.  The users of this document are the employees of the Information Technology Department. |
| Antivirus Policy |
| * The purpose of this policy is to help prevent the infection by computers and other malicious code and to provide a virus-free environment. The goal is to prevent the Alqarib data from damage due to a virus/Trojan attack. * This policy should cover the following issues as a best practice: * Antivirus software and virus pattern files must be kept up-to-date. * Virus-infected computers must be removed from the network until they are verified as virus free or the machine has been reformatted, if possible. * Do open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. It’s best to delete these attachments immediately and remove them from the trash. * Delete spam, chain, and other junk emails without forwarding them. Never download files from unknown or suspicious sources. * Do not directly share reading/writing access to the disk unless there is a compelling business requirement to do so. * USB ports should be blocked on all the machines. If there is a business need to use pen drives, it is highly recommended that this external media be scanned before use. * No files should be excluded from being scanned by anti-virus software. |
|  |
|  |
| Controls related to the change management policy |
| 1. **Every change to operating or work systems must be made in the following manner:**    1. The change can be introduced by the person who needs the change required for operational purposes    2. The change request is made through the Change Management System (Manage Engine).    3. The change request is distributed to the departments Managers, and then the request is accepted by the department responsible for the change request    4. The change request is reviewed by the department manger which concerned with the change, who must evaluate his justification for action    5. The change must be authorized by the [Information Technology Department manager and Information Security Officer], who must evaluate its rationale for action and potential negative security implications.    6. The change must be carried out by the person authorized by the department manager which concerned with the change    7. The concerned department manager is responsible for verifying that the change has been implemented as per the requirements.    8. The concerned department manager is responsible for testing and checking the stability of the system - the system should not be put into production before a comprehensive test has been carried out.    9. The implementation of changes must be reported to the following persons: [ Information Technology Department manager and Information Security Officer].    10. Change records are maintained by the change management system. |
| Information Transfer Policy |
| * Purpose, Scope and Users * The purpose of this document is to ensure the security of information and software when it is exchanged within or outside the Company. * This document applies to the entire scope of the information security management system, ie to all information technology and information within the scope.  The users of this document are the employees of the Information Technology Department. |
| Controls related to the transfer of information inside and outside the company |
| 1. **Information transmission**    1. **Electronic communication channels**  * Company information can be exchanged through the following electronic communication channels: e-mail, downloading files from the external network, transferring data via [file server .... etc.], telephones, fax machines, SMS messages, mobile media, forums and social networks. * [Network Administrator and Operating System Administrator] Specifies the communication channel that can be used for each type of information, and possible limitations regarding the permissions to use the communication channels, ie which activities are prohibited. * In addition to the controls defined by the Information Classification Policy, [Operating System Administrator] identifies (describes) additional controls for each type of data and communication channel, based on the results of the risk assessment.   1. **Relationships with external parties** * Third parties include various service providers (providers), equipment and programming maintenance companies, transaction or data processing companies, customers, etc. * Before exchanging information and/or software with any third party, an agreement must be signed, which is the responsibility of the [Information Security Officer]. The agreement can be in paper or electronic form (eg agreement on general terms and conditions), and it should contain clauses consistent with the risk assessment, including at least the following:   + The method of determining the other party.   + Permits to access information.   + Non-repudiation guarantee.   + Technical standards for data transmission.   + Respond to the incident.   + Labeling and handling of sensitive information.   + copy right. * Agreements with third parties must be drawn up in accordance with the supplier's security policy. |
| Security Development Policy |
| **Purpose, Scope and Users**The purpose of this document is to define the basic rules for the security development of programs and systems.This document is applied to the development and maintenance of all services, design, programs and systems that are part of the Information Security Management System.Users of this document are all employees who work on development and maintenance in the company. |
| 1. **Security development and maintenance**    1. **Risk assessment for the development process**   In addition to the risk assessment carried out in accordance with the risk assessment and treatment methodology, the [Operating System Administrator] shall periodically perform an assessment of the following:   * Risks related to (related to) unauthorized access to the development environment * Risks related to (related to) unauthorized changes to the development environment * Technical weaknesses of the information technology systems used in the company * The risks that a new technology may bring if it is used in the company   1. **Secure development environment**   [Identification of internal and external requirements]   * 1. **. Principles of safe engineering**   [Infrastructure Officer] will issue procedures for security information system engineering, to develop new systems and to maintain existing systems, as well as to establish minimum security standards that must be complied with.  The same security engineering principles will be applied to outsourced development, defined through contracts as defined in the Supplier Security Policy.   * 1. **Security requirements**   When acquiring new information systems, developing or changing existing ones, [Information Security Officer] security requirements must be documented in the security requirements specification.   * 1. **Security requirements related to public networks**   [Operation Systems Administrator] is responsible for defining security controls related to information in application services that pass over public networks:   * Describe the user character verification systems to be used * Describe how confidentiality and safety of information is ensured * Describe how non-repudiation of the procedures is ensured   [Operating System Administrator] is responsible for defining controls for networked processes, which should include the following:   * How will wrong orientation be prevented? * How will incomplete data transfer be prevented * How will unauthorized message change be prevented * How will unauthorized repetition of the message be prevented * How will unauthorized disclosure of data be prevented   1. **Check and test the implementation of security requirements**   [Information Technology Department Manager and Information Security Officer] is responsible for defining the methodology, responsibilities and timing of checking whether all security requirements from the security requirements specifications have been complied with, and whether the system is acceptable for production.   * 1. **Storage**   The code and all other development-related files are maintained by the Team foundation so that they are protected from unauthorized access and unauthorized change of version control.   * 1. **change control**   Changes in development and during systems maintenance should be made in accordance with [Change Management Policy] / [Information Technology Operating Procedures]   * 1. **Test data protection**   Confidential data, as well as data that may be related to individual persons, should not be used as test data. Exceptions can only be approved by the [administrator], in this case the [administrator] must specify how such test data is protected.   * 1. **Required security training**   [Department Manager ] determines the level of security skills and knowledge required for the development process and suggests training courses for the company's employees. It also includes appropriate training courses in the training and awareness plan. |
| Resource Security Policy |
| **Purpose, Scope and Users**The purpose of this document is to define the rules for the relationship with suppliers and partners.This document applies to all suppliers and partners who have the ability to affect the confidentiality, integrity and availability of sensitive information of the company.Users of this document are senior management and persons responsible for suppliers and partners in the company. |
| Legal Compliance Policy |
| The purpose of this policy is to address the legal, statutory, regulatory, and contractual obligations arising from the security and privacy requirements of an organization. Itshould cover the following points:All relevant statutory, regulatory, and contractual requirements should be documented and kept updated by HR and the legal team.Relevant standards and procedures should be defined and implemented by the information security team in consultation with HR and the legal team to ensure compliance with legal/contractual obligations on the use of information with respect to intellectual property rights.Any guidance on essential legal requirements should be taken from management.If any incidents relating to legal compliance occur, define how they will be handled and managed. |
|  |
|  |
| Relationship with suppliers and partnersIdentifying the risksSecurity risks related to suppliers and partners are identified during the risk assessment process, as defined in the risk assessment and treatment methodology. During the risk assessment, special care must be taken to identify risks related to information technology, as well as risks associated with the product supply chain.[Information Security Officer] Decides whether it is necessary in addition to assessing risks related to individual suppliers or partners.examination[Infrastructure Administrator] Decides whether it is necessary to carry out background checks for individual suppliers and partners, and if yes - which methods to use.ContractsThe [Department Manager] is responsible for deciding which security clauses will be included in the contract with the supplier or partner. This decision should be based on the results of risk assessment and treatment; however, clauses providing for confidentiality and asset recovery after the termination of the agreement are mandatory. Furthermore, contracts must ensure reliable delivery of products and services, which is especially important with computer service providers over the information network.A list of the proposed items is given in the apendex to the security clauses for suppliers and partners.[Department Manager] will decide whether individual employees of the supplier/partner will have to sign confidential data when working for (for) the company.[Department Manager] decides who will be the contract holder for each contract - ie who will be responsible for a particular supplier or partner.Training and AwarenessThe contract holder decides which supplier and partner employees need security awareness and training.The [Department Manager] is responsible for providing all training and awareness raising for these employees.Monitoring and reviewThe contract holder shall regularly check and monitor the level of service and fulfillment of security clauses by suppliers or partners, reports and records generated by the supplier/partner, as well as auditing the supplier or partner at least once a year.All security incidents related to the work of the partner/supplier must be immediately referred to the [Director of Administration].Changes or termination of supplier servicesThe contract holder proposes changes or termination of the contract, and the [Department manager] makes the final decision. If necessary, the [Information Security Officer] will conduct a new risk assessment before the changes are accepted.Removal of access rights / asset recoveryWhen the contract is changed or terminated, access rights for employees of partners/suppliers shall be removed in accordance with the access control policy.Furthermore, when the contract is changed or terminated, the contract holder must ensure that all equipment, software or information is recovered in electronic or paper form.Security clauses for suppliers and partnersWhen drafting an agreement with a supplier or partner, you must specify which of the following items will be included in the agreement (the legal form of the agreement must be prepared by the person responsible for legal matters.):Details of the service provided, specifying what information should be provided for this purpose and how the information is classified.Whether the supplier has the right to use sub-contractors If yes, then the written consent of the company must be obtained, describing the controls that must be complied with by the sub-contractors.Define confidential information and how secrets are organizedDuration of the agreement and the obligation to maintain confidentiality and confidential information / trade secrets after the termination of the agreement (when writing this article, it must be considered how business continuity will be ensured in the company.The right of the company to access the information stored or processed by the supplier / partner.The right to audit or monitor the use of confidential information, monitor the implementation of the agreement at the supplier/partner facility, and whether audits can be performed by third parties; determine the rights of auditors.Actions required after the termination of the agreement (recovery, destruction or erasure of confidential information, return of equipment, etc.) to ensure the protection of confidential information and to ensure business continuity in the company.Define and use key controls to ensure the protection of organizational assets – for example, physical controls, controls to protect against malicious code, physical security controls, controls to protect the Safety, availability and confidentiality of information, controls to ensure that information assets are recovered or destroyed after their use, controls to prevent copying and distribution of information .Ensure access to financial reports, to reports by internal and external auditors, and other reports relating to suppliers/partners' business operations, that may be relevant to the organization.Responsibilities and actions of the parties to the agreement in order to prevent access to the agreement by unauthorized persons (eg only need-to-know persons may have access rights to information, etc.)Determining the owner of the information and how to organize intellectual property rights.Permitted use of confidential information, i.e. the prescribed manner for dealing with such information.A process for notifying the other party to the agreement of unauthorized access to information, breaches of confidentiality or any other incidents.Determine the incident response time, and establish an escalation process for the problem and incident resolution.Procedures to ensure that the agreement is breached The supplier/partner's liability for unfinished (fulfilled) contracted operations and other activities, not on time or incorrect.The supplier / partner's knowledge of the main security policies and company procedures.A commitment to train supplier/partner staff in all activities in which they participate.Ensure that suppliers/partners are aware of the need for security.Prevent company employees from moving to suppliers/partners.The target service level and the unacceptable level of service.Defining service performance standards, monitoring them and preparing their reports.An accurate definition of the reporting system and the form of reports.Exactly defined change management process.Access control system – determination of the reasons for third-party access rights, allowed login and password process, process of authorizing individual user access and assigning privileges, obligation to keep a record of all users and their access rights, process of removing access rights.A clause that clearly states that all unauthorized access rights are expressly prohibited.The right to monitor and cancel any activity related to the company's assets.Controls to ensure business continuity, according to the company's priorities - ie services that need to be restored within any deadline.Liability for damage in case of breach (breach) of contractual relations, including material liability in case of breach of confidentiality of information or in case of non-performance of services.The responsibility of the supplier/partner to store the data in accordance with the regulations.Conditions for extension or termination of the agreement.The language of the agreement and future communication between the company and suppliers/partners |
| Incident Management Procedures |
| * **Purpose, Scope and Users** * The purpose of this document is to ensure rapid detection of security events and vulnerabilities, and rapid response and response to security incidents. * This document is applied to the entire scope of the Information Security Management System, that is, to all employees and other assets used within the scope of the system, as well as to suppliers and other persons outside the company who deal with systems and information within the scope.  The users of this document are all employees of the company as well as all the persons mentioned above. |
| Incident ManagementAn information security incident is “a series of undesirable or unexpected security or individual events with a high probability of exposing or compromising business operations and threatening information security” (International Standard ISO/IEC 27000:2022).Receiving and classifying accidents, vulnerabilities and eventsEvery employee, supplier or other third party in contact with the company's information and/or systems must report any system weakness, accident or event that could lead to a potential accident as follows:All IT related incidents must be reported to [all IT staff].All other events must be reported to [all IT staff].Accidents, vulnerabilities and events should be reported as soon as possible, by phone or in person.The person receiving the information should categorize it as follows:A security vulnerability or event - not an accident, but the event related to a system, process or institution that may lead to an accident in the near or near future.Minor incident - An incident that cannot significantly affect the confidentiality or integrity of information, and cannot cause long-term unavailability of information.Major Incident (Major) – An incident that could cause significant damage due to loss of confidentiality or integrity of information, or that could cause an interruption in the availability of information and/or operations for an unacceptable period of time.Weaknesses or security events treatment processThe person receiving the information about a security vulnerability or event analyzes the information, identifies the cause and, if necessary, suggests preventive and corrective action.Minor accident treatmentIf a minor incident is recorded (reported), the person receiving the information must take the following steps:Take measures to contain the accident.Analysis of the cause of the accident.Take corrective measures to remove the cause of the accident.Inform the persons involved in the accident, as well as the [Infermation security representative], about the process of handling the accident.The person who received information about a minor accident must register the accident [description of the method of registration for it - manual, electronic or automatic (for example through the Company’s online portal)].Major Accident TreatmentIn the event of major (major) incidents that could disrupt activities for an unacceptable period of time, the [Incident Response Plan as part of the Business Continuity Plan] is called.Learning from accidentsThe Information Security Officer must review all minor incidents every 3 months, and enter the recurring ones, or those that may turn into major incidents on a future occasion, in the incident log.[Information Security Officer] Each incident recorded in the Incident Log shall be analyzed (identifying the type, relevance and cost of the incident) and, if necessary, proposing a preventive or corrective actiondisciplinary action[Department Manager] A disciplinary process should be called for each breach of security rules.Evidence gathering[Information Security Officer] will set rules on how to identify, collect and preserve evidence that will be admissible as evidence in legal and other proceedings. |
| Encryption Controls Use Policy |
| * **Purpose, Scope and Users** * The purpose of this document is to define rules for the use of encryption controls, as well as rules for the use of encryption keys, in order to protect the confidentiality, integrity, authenticity and non-repudiation of information.  This document applies to the entire scope of the information security management system, ie to all systems and information used within the scope. |
| * **Encryption controls**   In accordance with the Information Classification Policy, as well as legal and contractual obligations, the Company shall protect individual systems or information by means of the following encryption controls:   |  |  | | --- | --- | | **Key size** | **Encryption algorithm** | | 128-bit, 192-bit, and 256-bit | AES | | 128-bit, 192-bit, and 256-bit | SHA1 | | 2048-bit to 5012-bit | Diffie-Hellman | | 2048-bit to 5012-bit | Elliptic-Curve Diffie-Hellman | | 2048-bit | DSA | | P-192، P-224 ، P-256، P-384 ،P-521 ،B-163 ،B-233 ،B-283 ،B-409 ،B-571 ،K-163 ،K-233 ،K-283 ،K-409 ،K-571 | ECC | | 224-bit to 512-bit | HMAC SHA2 | | 2048-bit key length and longer, with SHA1, and SHA2 with 256-bit to 512-bit key lengths | RSA | | 224-bit to 512-bit | SHA2 |      * **Encryption keys**   The [Information Security Officer] is responsible for describing the following rules regarding key management:   * Generate private and public encryption keys. * Activation and distribution of encryption keys. * Determine the time period for using the keys and update them regularly (according to the risk assessment). * Archiving passive keys that are necessary for archiving encrypted electronic (records). * Destroy the keys.  The keys are managed by their owners in line with the above rules. |
| Backup Policy |
| **Purpose, Scope and Users**The purpose of this document is to ensure that backups are created at specified intervals and tested regularly.This document applies to the entire scope of the information security management system, ie to all information technology within the scope.The users of this document are the employees of the [Information Technology Department]. |
| **The goal of the policy:**   1. Establishing a clear and sound framework for backup copies and information recovery in order to ensure the availability of information for the company in the event of file loss. 2. Ensure that the company develops and implements adequate controls for backup critical data and systems 3. Determining the duration of the company’s retention of backup copies and rewriting on tapes   Backup management items in the company:   1. Preparing a central infrastructure for backups that takes backup copies to protect company data and ensure its recovery 2. Adopting the method of full weekly and monthly copies and daily updates during backup operations and providing copies of critical systems in the disaster recovery site 3. The system for the backup process will copy the data weekly on Friday and Saturday **completely**, and the working days are from Sunday to Thursday, it copies **the updates** from the data only 4. Make backup copies of the following systems (databases, e-mail system, internal website, shared file system, company website system, virtual systems, attendance system) 5. The company is obligated to keep the backup copies for a period of 20 days, after which it is allowed to copy and keep the data again for the same last period 6. Transferring backup tapes for critical systems outside the company on a weekly basis after the success of the copying process, and the tapes sent in advance are returned weekly to ensure that there are backup copies outside the company building, with daily copies taken and kept in the fireproof information technology department safe 7. Encrypting the backup tapes before sending them outside the company’s building and placing them in the Information Technology department’s vault with AES 128 bit encryption 8. Document all tape transfers outside the company premises and in the backup log 9. Experiment with validating Oracle database backups in a trial environment every month 10. Document copy recovery operations in the re-application log  The Information Technology Department is responsible for the implementation of the copying procedures. |
| Vulnerability Management Policy and Security Updates |
| * **Purpose, Scope and Users** * The purpose of this document is to determine the way to deal with security vulnerabilities on various assets and how to manage them and implement the necessary steps to fill these gaps and ensure that they are not used by any attacks that may target assets that contain these vulnerabilities. And to ensure the implementation of the latest security updates. * Scope: All of the company's assets, including hardware, servers, software, and operating systems  The users of this document are the employees of the Information Technology Department. |
| Controls related to the vulnerability management policy and security updates |
| All assets within the scope should be scanned and updated according to the following method:   * All security settings must be in accordance with the recommendations followed by the Manufacturer. * The process of searching for vulnerabilities and updating systems should be as follows:  1. Define the scope of the search 2. Conducting a vulnerability check periodically every six months 3. Assessing operational risks related to the discovered vulnerabilities and setting priorities for dealing with them 4. Determining the responsibilities and tasks of the technical team to deal with the discovered gaps according to priorities. 5. Take the necessary corrective measures to fill these gaps 6. i. The tasks of the technical team are as follows: 7. Check the latest security updates for the department's assets 8. Implement the latest security updates according to the manufacturer's recommendations 9. The update process should be done as soon as it is released 10. In the absence of a suitable update for one of the discovered vulnerabilities, the information security officer must study his options to deal with it until the appropriate update is available, for example. 11. Filter requests through firewall or IPS devices 12. Putting systems under surveillance to detect any suspicious activity related to the discovered vulnerability 13. Virtual patcing 14. Disable the services or features related to the vulnerability until the appropriate update is available 15. All updates must undergo an Acceptable Security Test (UAT) to ensure that the updates do not cause any crashes or affect the performance of the assets  The change management policy should be considered in implementing updates |

* + 1. **References:**
* International Standard (ISO 27001) - Requirements and Guidelines of Use
* International Standard (ISO 9001) - Requirements and Guidelines of Use
* International Standard for Quality Management System ISO 9001:2015
* International Standard for Risk Management 31001
* International Standard for Business Continuity System
* Risk Management Manual
* ISO procedures for quality management, health and occupational safety
  + 1. **The Used Forms:**
* Information Security System Legal Requirements Form No.:
* Risk Register Form No.:
* Information Security System Objectives Model No.:
* Records form for erasing and destroying records classified as restricted or confidential No.:
* Remote Entry Form No.:
* List form of persons authorized to access information classified as restricted or sensitive No.:
* User Profile Form in Access Control Policy No.:
* Accident records No.
* Access Rights Regular Review Record No.:
* Accident Reporting Form No.
* Product Receipt Request Form - Hardware
* Product Receipt Request Form – Software
  + 1. **Performance indicators:**
* The percentage of achieving the objectives of the information security system
* Number of breakouts
* The rate of reduction in the number of security incidents
* Percentage of security incidents that have been addressed
* The level of awareness of human resources about information security and its risks
  + 1. **Version and revision history**

| **Next revision date** | **The Change** | **Methodology mode** | **revision number** | **Date** |
| --- | --- | --- | --- | --- |
| **01-02-2025** | **Origional** | **-** | **1** | **01-02-2025** |
|  |  |  |  |  |

* + 1. **Accreditation / Aprovals**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **signature** | **01/02/2025** | **Date** |  | **Information Technology Manager Review** |
|  |  | **01/02/2025** |  |  | **Managing Director Review** |
|  | **signature** | **01/02/2025** | **Date** |  | **Accreditation / Aprovals** |