serena

Information Security Policy

serena

1. Introduction

This policy defines standards and guidelines designed to ensure the confidentiality, integrity, and availability of data and information systems used by Omega. Adequate asset and data protection is fundamental to enable the identification, protection, detection, response to, and recovery from any event in case of a data breach. In addition, this Policy complements Section 13 of the Company's Code of Conduct which outlines the guidelines and expected conduct of employees, third parties, partners, suppliers, and service providers regarding the protection of assets and data to ensure confidentiality, integrity, and availability of information.

Approved by the Board of Directors on December 17, 2021, this Policy will be made available on the company website, Workplace (internal social network), andthe Microsoft Teams platform for all Omega employees. Whenever necessary, and with a minimum interval of two (2) years, the Policy will be analyzed by the Ethics Committee and may be revised. The Information Technology department will maintain a review/update program in place, which ensures that the technical and legal security requirements implemented are being met and in compliance with the current legislation, including the periodic review of action plans and their adherence initiatives to share information about cyber incidents.

Adherence to this Policy and any misconduct shall be addressed to Omega's Technology Board and, whenever necessary, reported to the Ethics Committee. Terms used in capital letters have the meanings defined in the glossary of the Code of Conduct or in this Information Security Policy.

2. Rules about Information Security

2.1 Information Security Principles:

Our commitment to the proper processing of Omega, customers, and general public information is based on the following principles:

Confidentiality

Ensure that the information will not be disclosed to individuals, entities, or applications without their owners' or Omega's prior authorization.

Integrity

Ensure that the contentof the information has not been altered and, therefore, is complete and authentic.

Availability

Allow confidential information to be used only when users and recipients need it.

2.2 Information Life Cycle:

For the purposes of this Policy, the information life cycle is as follows:

- Handling: the step when information is created and handled.
- Storage: the step when the information is stored, whether in a database, on paper, in external electronic media, among others.
- Transport: the step when the information is transported to a location, regardless of the medium in which it is stored.
- Disposal: the step when a printed (disposed in the trash and/or kept in a storage company) or electronic document is eliminated or when storage media (e.g., CDs, DVDs, floppy disks, flash drives) are fully destroyed.

2.3 Information Classification:

Information must be classified according to its content, external knowledge relevance, and specific document elements.

Access, disclosure, and processing of (paper or digital) documents, data, or information are restricted to employees who need to know them due to their duties within Omega, and this access is guided by the rules provided for in this Policy and other rules of the company. All information for corporate use must be classified according to their degree of secrecy regarding the company's business,considering three levels:

Confidential

It is the highest degree of secrecy, applied to strategic information which must be handled by a restricted group of users. Unauthorized access to this information can have critical consequences for the business, damaging the company's reputation.

Internal

It refers to specific information for internal use that is only disclosed within the company. This information may be available to all employees and contractors and should only be used for Omega activities. Despite being disclosed within the company, this information must not be disclosed to outsiders without due care, including, when necessary, the execution of non-disclosure agreements or formal authorizations previously evaluated by the department in charge of such information.

Public

It refers to information of free circulation and public domain. This type of information does not require security controls or restrictions for its access or storage.

2.4 Information Security Incidents:

For the purposes of this Policy, a security incident is defined as any harmful event resulting from the action or omission of employees and third parties, or even a threat to the principles of Information Security.

3. Information Security Management System

The Information Security Management System is a set of processes and best practices to establish, implement, operate, monitor, review, maintain, and improve information security with actions on four major fronts:

- Governance of information security policies and procedures;
- Information security features and components;
- Continuous monitoring of the information technology environment;
- Crisis management and business continuity.

4. Internal Information Security Controls and Cyber Security

4.1 Identifying and Assessing Threats and Vulnerabilities

Omega's Information Security department shall be responsible for identifying and assessing the risks to which processes and assets are subject and potential threat scenarios. Omega has revised or will revise the mandatory contractual clauses for contracting suppliers and service providers in order to adapt them to the current policies.

4.2 Proteção Prevention and Protection Actions

Standardized routines for the prevention and protection of processes and assets shall be adopted, as provided for in the internal standard, including vulnerability analyses, penetration tests, and other specific assessments that confirm compliance with the security requirements and previously established accountabilities. Attack and invasion tests must be carried out periodically to monitor the efficiency of the cyber security system. Omega carries out tests both in the internal environment (in the Gray Boxmode) and external environment (in the Black Box mode).

4.3 Monitoring and Testing

Effective internal controls must be implemented to protect Omega's Information and Communication Technology Resources (RTICs), guaranteeing their confidentiality, integrity, and availability, always observing the best market practices and current regulations.

The Information Security department can monitor or inspect the RTICs that are on its premises or that interact with Omega's environments whenever it deems necessary.

Critical applications must have audit trail generation/ maintenance, source code versioning control, and segregation between production and approval environments. Cyber threats must be analyzed alongside the vulnerabilities detected by the Information Security department in informationassets and must be actively monitored by said department.

4.4 Incident Action and Response Plan

Information Security incidents must be identified and recorded so that action plans can be monitored, and vulnerabilities can be analyzed, respecting the level of risk exposure defined by Omega.

4.4.1 Incident reporting

Users must immediately report any incidents to the person in charge of Information Security. Incidents must be evaluated and investigated for consistent analysis of cause, risks, persons involved, and responseplans. The assessment should be submitted to the Cyber Security Director, who will decide on the initial actions to be taken. Once the relevance of the incident has been classified, Omega must communication those involved, reporting the situation and the actions agreed, even if preliminarily, informing/notifying them about the actions that will be taken later. In addition, the person in charge of Information Security must prepare and disclose to the Board of Directors an annual report on action plans and incident response.

4.4.2 Violation attempt

The mere attempt to circumvent the guidelines and controls established by Omega shall be treated as a violation/incident.

4.4.3 Treatment of identified vulnerabilities

The treatment and active correction of major information asset weaknesses must be recorded. All residual risks must be assessed and the persons involved in the plan must provide adequate support.

4.4.4 Conflicts of interest

Omega must have a process for granting access that uses clear and objective criteria to identify conflicts of interest arising from technical limitations or duly authorized situations. Access activities and cyber threats must be monitored.

4.4.5 Preparing an action plan

An action plan must be prepared by the persons in charge of the Information Security department. Other departments may be involved if necessary to implement the solutions and to manage any contingencies. Such plan must outline the roles and responsibilities for

problem resolution, and the key employees or relevant external contacts, where applicable, must be notified. The threat scenarios provided for in the risk assessment must be taken into account, with criteria for classifying incidents as to their severity. The action plan should provide for situations that would require the use of contingency facilities (mostsevere cases), as well as the process of returning to the original facilitiesafter the incident has ended. All incident management documents must be filed for audit purposes.

4.4.6 Reporting to the Authorities

Omega will communicate the relevant incidents and service interruptions that constitute a crisis, as well as the measures taken for resuming these activities to the relevant authorities, when necessary, through the Legal and Communication Departments.

5. Training and Awareness Program

Omega uses its internal platforms to promote a recurring awareness plan onthe importance of Information Security aimed at all internal audiences, in addition to a security summary published on the company's portals.

Schedules

1. Access Management
2. Change Management
3. Operations Management
4. Terms of Use and Privacy Policy (omegaenergia.com.br) https:// omegaenergia.com.br/termosde-uso?Consumidor

Schedule 1 • Access Management

Purpose

The process of granting access to Omega's information assets must take into account the resources necessary to perform the tasks and one's position within the company, in addition tothe authenticity of the access credentials.

Process

1. Creating an Access Account

The account will usually be created during the Onboarding process, and may also result from job profile adjustments and role transfers. To open an account, the recruitment team and/or manager must file a request so that validations and approvals are obtained. This also helps ensure information security, data for audits, and service statistics. When hiring a new employee, the account creation request must include Payment, Facilities, Microcomputers, and Systems information. All the teams involved will be able to follow the progress and act accordingly on behalf of each team. Full name, Date of Birth, Start Date, Company, Cost Center, Manager, and Individual Taxpayer ID (CPF) are essential data that must be entered into the systems. The Systems team will only be able to register an employee when the network user has been created and the email approved. The Systems team must pay attention to the start date so that the access data that is sent by email by the systems analyst is cleared.

If the employee to be registered is a department manager, the recruitment and personnel management team must inform if the manager will own a cost center and if he/she should be included in some approval hierarchy. If so, this information should be provided when the request is made so that the correct configurations are set and the correct flows are defined in the systems. Access to the purchase and accountability modules is granted to all hired employees within the financial ERP. For other accesses, HR must be informed by the manager of the necessaryadditional systems and profiles.

As for hiring third parties, the department Manager is responsible for managing the resource but must communicate it to the personnel management team so that they can make a request for granting access and are able to control the third parties working in the company.

Within the information entered into the system, a differentiator must be created according to the type of employee to facilitate access control and auditing.

2. Changing an Access Account

An access account is usually changed when an employee is transferred. The change must be described in a request made by the recruitment and personnel management team, which must contain information on the new Business Unit, Cost Center, and/or Manager. The previous manager is responsible for verifying with the employee if there

is any pending issue and the future manager is responsible for validating employee access. If positions or business units are to be maintained, make a request detailing any revocations and/or inclusions.

If the employee is linked to some approval flow, i.e., is the owner of a cost center, it is necessary to describe in the request the new flow to be created, both in the destination and in the origin units. Third-party internalization is also important. In this case, registration is made to allow the traceability of operations across the different hiring steps. The update is made after an Onboarding request and the employee must be informed about the change of logins whenaccess changes are complete so that he/she can have plenty of time to complete all the workflows in the system before the user changes.

3. Blocking an Access Account

This happens when employment is terminated or the job role changes. In the event of a change, this must be carried out as outlined in item 2. In case of employment termination, the process should start with the personnel management team and the manager to validate any pendingissues and only then make a request to revoke access, thus ensuring process confidentiality.

The Information Technology will validate any pending issues and close access to the system. In the case of employment termination with security and/or confidentiality risks, a request for blocking access may be made directly to the Technology Board for immediate and exceptional action. The process shall be carried out by email and by a subsequent technical request.

4. Access Review and Process Error Mitigation

A review of the accesses granted to all Omega users and/or employees is carried out monthly, based on a spreadsheet provided by HR, making it possible to clear, block, and/or adjust whatever is necessary to comply with the Policy.

Every six months, access profiles are reviewed on two fronts. (i) Access Matrix (ii) Users by access profile, as shown in the example below. An access-per-user spreadsheet will be sent to department managers so that they can validate that the access accounts and the associated

profiles are in accordance with the management rules and controls. Profile Matrix X Reviewer

Access Profile	Reviewer
Oracle Accounts Payable	Financial department manager
Oracle Accounts Receivable	Financial department manager
Oracle Accounting	Accounting department manager
Oracle Fixed Asset	Accounting department manager
Oracle Requests	Immediate manager
Oracle Expense Report	Immediate manager
Oracle Level of Approvals	Financial department manager

Scheduale 02 • Change Management

Purpose

The progress and result of a change in a relevant technological system or infrastructure ensure the preservation of controls related to data availability, integrity, confidentiality, and authenticity, which are managed by the Information Technology Department in a planned, approved, and tested way, following the change management process.

Process

The account will usually be created during the Onboarding process and may also result from job profile adjustments and role transfers.

On-Premise and IaaS

For Omega's physical and internal environments, IaaS Cloud, and Corporate Systems (Oracle, GFT, XRT, etc.), we will follow the Change Management process that includes a change registration form, a weekly committee to present the objective, the tests carried out, and rollback methods,and approval or disapproval of the change. In addition, it is possible to request emergencychanges with the same form on Sharepoint, and such cases need immediate intervention andmust be approved by the leadership. Both cases have a record for future audits and lessons learned.

Software Engineering Cloud

For DevOps environments, we follow the CI/CD process, that is, automation of the release schedule, review of changes in the DEV environment, always by a developer other than the code creator, Merge from the DEV environment to the STAGING environment, Homologation by the QA team in a STAGING environment, Merge from a STAGING environment to a PROD environment. Only Tech Leads perform Merges. If any unplanned situation occurs, the Tech Lead is responsible for executing the rollback process, by merging the previous release into the PROD environment. The entire process has audit logs for future audits and lessons learned.

It is important to highlight that the MERGE step triggers CI/CD, that is, unit tests, end-to-end tests, component tests, security, checks, and deployment.

SaaS environments

For SaaS environments, we will follow the process determined by the contractor, that is, we are notified by the partners about the releases, which usually happen on a quarterly basis for the entire environment, in advance of tests and validations. The Tech team is responsible for managing pre-validation with key users when necessary and communicating with the company about these updates.

Every month, at the end of a GMUD Committee meeting, we report the number of regular, emergency, and canceled changes, as well as changes executed without due process and approval.

Scheduale 03 • Operations Management

Purpose

Carry out the life cycle management (acquisition, maintenance, update, support, and disposal) of the company's technology and telecommunications resources and guarantee the effective use of said resources to the company’s users, taking into account good market practices and the information security practices outlined in this Policy.

Process

Crisis support and management

The technology area responds to user requests, considering that they must make adequate use of technology resources, by recording incidents, questions, difficulties, or problems in the use of resources and technology.

The technology area provides and organizes communication channels to plan the daily operation:

• Groups on communication platforms
Some fixed groups are in place for monitoring operations and specific groups are created for specific crisis management.

• Ticket reporting system
The company has its own system, which is managed by the technology area, and the ticket systems by service providers, such as NOC and SOC.

Monitoring

The company has 24/7 monitoring on two fronts:

- NOC (Network Operations Center)
  A team that monitors the availability and performance of the technology environment.

  When alarms are set off and events occur, the NOC notifies the technical team of the company's technology department and takes action immediately (together with telecommunications providers, technology providers, and other service providers).

The NOC also acts reactively, when users report problems or have questions about the use of the company's communication resources.

  • SOC (Security Operations Center)
  By using tools such as SIEM and CAS, this team monitors the technology environment focusing on information security, constantly monitoring the events generated in the environment (alerts, alarms, and other data from the several older platforms used by the company, whether in the cloud or on-premise).

Each alarm or alert is properly analyzed and handled. Depending on the criticality levels of each event, more or less energetic actions can be taken.

Relevant events are notified by email.

Critical events require telephone contact with the company's technology area, usually after mitigation and containment measures have been taken for any risks, threats, or incidents.

A weekly meeting is held to monitor information security indicators.