Information Security Policy

Version	4
Approval Date	2024-05-01
Author	Michael Skolarikis (CIO)
Reviewed by	Maria Siapka (CQO)
Approved by	Spyridon Skolarikis (CEO)
Owner	Chief Information Officer

Contents

Revision History

Version	Date	Author(s)	Summary of Changes
4.0	2024-05-01	Michael Skolarikis	Changed format
3.0	2016-09-01	Michael Skolarikis	BCP/DR changes
2.0	2015-12-02	Michael Skolarikis	Classification Changes
1.0	2015-03-27	Michael Skolarikis	Document creation

Introduction

Mission

Comidor S.A (the Company), responding to changes in the business environment and aiming at the protection and management of its information systems in terms of exemplary customer service, has designed and implemented an Information Security Management System, in line with the International Standardization, ISO 27001:2022 and General Data Protection Regulation (EU) 2016/679 ("GDPR"). The Management team demonstrates a commitment to the provision of the required facilities and equipment necessary to conform with duties and delivery of the services provided.

Purpose

The Company's Information Security Policies cover Software Design, Development, Implementation and Support and have been designed upon its needs and goals, as well as upon the laws and regulations of European Legislation. The purpose of the Information Security Policies is to guarantee that Management, Internal and External Audits and Regulators are satisfied with the level of security awareness and implementation of controls. Additionally, to ensure that clients and business partners are assured their data is safe.

Objectives

The main objectives of the Information Security Management which support the Company's Information Security Management System are as follows:

- Continuous process improvement aiming at continuous sustainable customers' satisfaction in terms of their needs and expectations to the highest possible level
- The minimization of incidents and near-misses, to the minimum level, as well as of their effects that might affect business continuity
- Processing and control of any information distributed in any way, via its electronic or non-electronic systems, in a way that ensures their safety regarding their confidentiality, integrity and availability.
- The compliance with the laws and regulations that the Company is subjected to

Regarding personal and sensitive data protection, Senior Management defines security policies and enforces the rules to comply with General Data Protection Regulation. Some of the principles being adopted but not limited to are the following:

- Data processing in an appropriate and legitimate way
- Data storage for clearly predefined goals

- Data restrictions in use for the achievement of those goals
- Data protection through the adoption of adequate security measures

Time limitations in data storage (minimization)Scope

All Management and staff are fully informed and obliged to comply with the Company's business policies regarding the information security program. The above must act on specific security and confidentiality rules and guidelines, at all times, especially while interacting with information or information systems. Those include: Clouds systems developed or commissioned by the Company, systems managed by the Company, data over which the Company holds intellectual property rights, data over which the Company is the data controller or data processor or any electronic communications sent from or on behalf of the Company.

Management Commitment

Senior Management is committed to supporting and enabling the information security program, for reviewing and approving security practices and measures, as recommended by the Chief Information Security Officer.

Senior Management emphasizes the need for the company to comply with the relevant legislation and the applicable regulations, in every communication with the Company's Executives.

All Managers and Department Heads are responsible for protecting information resources from internal and external threats pertaining to their confidentiality, integrity and availability. It is on their responsibility to:

- ensure that the approved protection policies, standards, and procedures are followed.
- recognize and report security vulnerabilities and ensure that appropriate measures are taken to address them.
- keep Auditors and Regulators satisfied with the implemented security controls.
- ensure that products and services being used by the Company conform to the Information Security Policies.
- ensure that products and services produced and offered by the Company conform to the Information Security Policies.
- train personnel adequately to clearly understand the information security concepts so that they are able to react to incidents promptly.

Continuous Improvement

Senior Management provides all the resources needed to carry out internal inspections and corrective actions in order to continuously improve the system and adapt to the constantly changing needs of the company.

Human Resources and Personnel Security

Our process of personnel onboarding is governed by a plethora of security practices in order to ensure that the data of our clients remain safe at all times. Specifically, during the hiring process of a new employee the following practices are applied:

- Background screening before the employee is given access to any sort of critical infrastructure, data, or system
- Documented process of system and data access that is reviewed regularly
- Documented disciplinary process for non-compliance with corporate policy
- Authorization and access revocation procedures for system and data access
- Documented termination or change of status policy with appropriate accompanying process

Physical and Environment Security

Digitally securing our company assets would be useless without robust security mechanisms that restrict physical access to any unauthorized entity. The company makes the greatest possible efforts to ensure that data and systems are only accessed from authorized parties, at any given time.

In order to ensure physical security we are taking certain measures:

- Enforcing a Physical Security policy that must be followed by all our employees and contractors
- Physical access to the building is monitored via a CCTV and an alarm system
- A Clear Desk policy is enforced and must be followed by all employees
- Access to the "Server Room" area is restricted to authorized personnel only
- Controlled entry point for everyone entering premises
- All visitors must be escorted at all times
- The building is regularly inspected by a safety technician
- The "Server Room" is equipped with Uninterrupted Power Supply units
- Fire suspension systems are installed on the office and server spaces
- Sensors for live humidity and temperature statistics are installed in the "Server Room"

Information Systems Security

The security of our clients' data is of utmost importance for each and everyone that is working in Comidor. In order to ensure that these data remain confidential whatever the circumstances we are taking certain steps:

- Enforcing an information security policy which includes information classification & handling
- A standardized information risk management plan is in place
- All employees are subject to the following list of security related company wide policies:

    1. Acceptable use of equipment
    2. Access and Control management
    3. Incident Management
    4. Internal and External Network Security
    5. Remote Access
    6. Data Encryption
    7. Business Continuity
    8. Data Destruction and Disposal
    9. Clean Desk
    10. Personnel Security
    11. Physical and Environment Security
    12. Non-Compliance frame
    13. Security Training and Awareness Program
    14. Third Party Security
    15. Security Event Management
    16. Password Policies and Management
    17. Vulnerability Scanning and Management
    18. Penetration Testing Process
    19. Change and Patch Management
    20. Server - Mobile - Cloud Security
- Sensitive data is always in an encrypted state, either in transit or at rest

Technology Management

Managing our technology assets is a crucial aspect of having a proper defence mechanism against cyber criminal activity. We ensure that in the entire lifecycle of our infrastructure and software there is always a security line of defense against possible data leaks or corruption. Also, our IT team is high-maintenance ensuring that there are always available logs for anything that happens in our environments.

Specifically:

- Our Software Development Life Cycle contains secure development / coding practices
- Enforcing a security based testing approach for cloud-based applications
- Secure code reviews against the entire codebase during the development phase
- Vulnerability Scanning and penetration testing processes after a piece of software has reached the testing phase
- Test data masking
- Test accounts and passwords are removed prior to software reaching the production environment
- Remediation of QA findings
- Formal Security training for developers
- Process for code migration to production environment
- The “Development”, "Staging" and "Production" environments are segregated
- Monitoring access and acquiring logs for source code access
- Application security vulnerability assessments and application penetration testing conducted prior to any product release
- Infrastructure and application monitoring
- Asset Management Policy

Business Continuity Plan and Disaster Recovery (BCP/DR)

Disaster strikes even the most secure and well organized entities in the technology world. We have developed an intricate BCP/DR plan to ensure that we can continue operation in a matter of hours while ensuring that all of our clients' data remain accessible and secure at all times.

In order to achieve this level of operational excellence we are taking the following measures:

- Documented Business Continuity Plan that is regularly reviewed and tested
- Crisis and Incident Management Policy
- Disaster Recovery, Data Backup and Restore process
- Backed by leading IaaS Cloud providers.

Approval and Review

Review Process

The Information Security Policy will undergo a formal review process to ensure its ongoing relevance and effectiveness. Reviews will be conducted annually or whenever significant changes occur within the organization, such as updates to the ISMS, introduction of new technologies, or changes in regulatory requirements.

- **Review Frequency:** Annually
- **Responsible Party:** Chief Information Officer

Any amendments to this document will be documented and approved through the same process to maintain the integrity and accuracy of the Information Security Policy.

Approval

This Information Security Policy has been reviewed and approved by the senior management of Comidor. The approval signifies the organization's commitment to maintaining and continuously improving the ISMS in alignment with ISO/IEC 27001:2022 standards.

Approved By:
Michael Skolarikis, Chief Information Officer
Spiros Skolarikis, Chief Executive Officer

Date:
May 01, 2024