

Information Security Policy

Code	ICT-POL-001
Control	5.1 Policies for Information Security 5.2 Information Security roles and responsibilities
Version	5.0
Date of Version	1/16/2023
Created by	Corina Guardado
Approved by	Saied Avash
Confidentiality level	In-Confidence
Authorized users	All EMAYA Employees

Version Control

Date	Version	Change/reviewed by	Description of the change/review by
6/20/2019	1.0	Corina Guardado	Document Creation
09/2/2019	1.0	Corina Guardado	Added Org Chart and Process Map for the Organization
09/24/2019	1.5	Saied Avash	Review and Approve document, added core values, mission vision.
10/23/2019	1.5	Corina Guardado	Added Pestel chart, and documentation
11/07/2019	1.5	Executive Team	Review changes: Pestel and SWOT analysis
6/25/2020	2.0	Corina Guardado	Update Organization Chart and Core values, Design.
8/25/2020	2.1	Executive Team	Revision of PESTEL and Swot analysis for 2020-2021
8/28/2020	2.2	Executive Team	Update Strategic Objectives
05/14/2021	2.3	Corina Guardado	Update Organization Chart
03/08/2022	3.0	Jorge Huezo	Update Structure and Content
3/21/2022	3.1	Jorge Huezo	Addressed comments and updated Organization Chart
9/1/2022	4.0	Saied Avash	Review and Approval
1/16/2023	5.0	Jorge Huezo	Addressed the suggestions from the audits and updated the document to the new format.

Contents

Version Control.....	2
Introduction.....	5
Purpose.....	5
Scope.....	5
Emaya.....	6
Mission	6
Core Values	6
Vision.....	7
Strategic Objectives.....	7
Stakeholders	7
Organizational Chart.....	8
Process Map	8
Interested Parties.....	9
Pestel Analysis	10
Political	10
Regional Political Stability	10
Government Support	10
Economic	10
Economic Growth in LATAM	10
Financial Stability.....	10
Social.....	10
Talent Pool Development	10
Technological.....	11
Tech Integration in BPO	11
Cybersecurity Advances.....	11
Environmental	11
Sustainability Practices.....	11
Legal.....	11
Local Regulatory Landscape.....	11
ISO 27001 Certification Adherence.....	12
External Influences	12
Competitive Landscape.....	12
Industry Standards and Trends.....	12
SWOT Analysis.....	12



Information Security Policy.....	14
Information Security Objectives.....	14
Roles & Responsibilities	15
Information Security Supporting Policies & Documentation.....	15

Introduction

This information security policy serves as an overview of the internal organization, procedures and strategic analysis that supports the Information Security Management System of EMAYA. Topic specific policies can be found as separate documents that expand on the allowed behaviors and the use of information assets within the organization.

Purpose

This policy gives an overview of EMAYA's operations, its context, procedures and rules that have been established in order to have an ISMS that is compliant with the ISO 27001:2022 norm.

The purpose of this policy is to minimize the risk of security information by implementing an Information Security Management system. Effective implementation of this policy will minimize potential threats to the business continuity of EMAYA.

Scope

EMAYA provides outsourced services for international clients from different industries. The protection of all the information and data assets that EMAYA receives for the delivery of the functions, services, and activities that EMAYA performs. Protected assets are physical locations, printed data, electronic data, employee records, commercial and contractual agreements, software and licenses, and physical IT hardware. The limits of the Information Security Management System are the virtual platforms authorized by our clients and managed by them.

Every user in the organization shall be aware of this document, understand its contents and respect the policies and procedures established on it or risk disciplinary actions being taken.



Emaya

EMAYA was founded in 2015 and it started operations with a small team focused primarily on Contact Center services. As time advanced and opportunities unfolded, EMAYA evolved from a small Contact Center into a true People organization, focusing on the importance of attracting talented professionals who are forces for good for our company and our clients. EMAYA has grown steadily from 12 employees to over 200.

EMAYA seeks to establish a partnership for growth by helping to bring together the best and brightest professionals to our clients. EMAYA spares no resources when it comes to ensuring a client's success, the company strives to provide the best tools, facilities, and quality professionals to ensure that we are producing great results. We are not only a service provider but a business partner. OUR success rests in the success of our CLIENTS.

Mission

To provide our clients with the ability to safely and securely unlock potential talent in any labor market and provide life-changing work opportunities to people around the world.

Core Values

Trust: We work hard to preserve and improve the bonds with our stakeholders through transparency and open communication. The trust that our clients, employees, and investors have in us is very important and key to our operations

People-focus: The way a company treats its employees is a statement of its merit. EMAYA recognizes that to be the best, you need the best people. We strive to create a workplace where our employees can thrive and where everyone loves to come to work.

Security: EMAYA understands that all data has value and that any data our clients choose to share with us is a testament to their trust in our company's ability to safeguard it. Although we don't store client data, EMAYA is dedicated to keeping all our information assets secure through constant oversight and a focus on continuous improvement.

Integrity: We always keep our word to our clients, employees, and investors. We pride ourselves on always doing the right thing, even when no one is watching.

Empathy: We believe this to be one of our greatest virtues and is a strength of our company. Mindfulness of how EMAYA's decisions as a company affect all our stakeholders drives us to make better decisions that improve the experience of all our employees, clients, and stakeholders.

Performance: We have a duty to perform to the expectations of our clients and to never be complacent about our results. We work closely with our clients to continuously improve our performance and processes

Adaptation: We recognize our company is a Complex Adaptive System that must evolve to keep up with an ever-changing business climate while always staying true to our core values.

Vision

To become one of the world's best companies by connecting great clients with great people.

Strategic Objectives

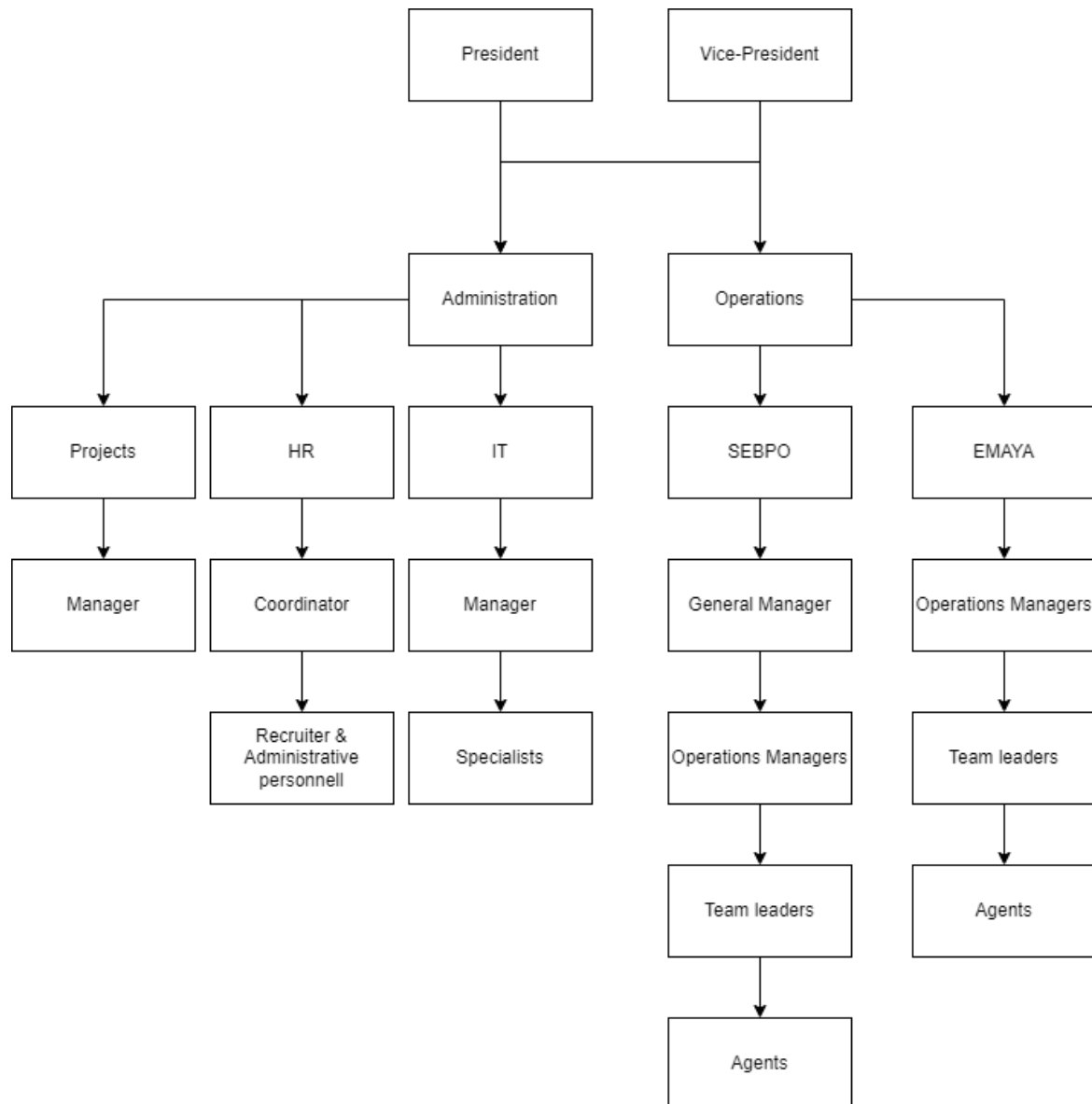
- To be one of the most desirable places to work in El Salvador.
- To leverage other markets within Latin America.
- To attract new clients at an international level by being at the forefront of Information Security.
- To diversify our client list while continuing to grow organically by leverage of our existing partnerships.

Stakeholders

Emaya provides outsourcing services for international clients. Much of the information and data that is handled is generated by the delivery of these services, this data's confidentiality, integrity, and availability is of the highest importance.

EMAYA works to ensure that this information is protected all the time. Information assets are managed through a risk assessment process, the risk of the information assets is recorded and managed through a risk matrix and a risk management procedure. Stakeholders of the system are clients, employees, shareholders, and the government.

Organizational Chart



Process Map

Emaya's main business processes are the Recruitment, Hiring and provisioning of outsourced agents, this is supported by the IT infrastructure, service providers, Human Resources and all the policies and procedures defined to be compliant and certified with the ISO 27001:2022 norm.



The support processes function as business processes in most cases since the service provided to clients is the provision of these support processes for the purpose of hiring outsourced agents.

This is done through providing agents with the infrastructure to work with clients, i.e., a computer, secure working environment, and ensuring the integrity, availability and confidentiality of customers data through the implementation of security procedures and policies and maintenance of an ISMS that is certified to be compliant with the ISO 27001:2022 norm.

Interested Parties

Interested Party	Needs & Expectations	Addressed by the ISMS
Employees	Good work environment, job security, safe working environment, quality work, necessary tools, resources to work.	Safe working environment
Shareholders	Sustained Growth, Profitability, Business Continuity	Business Continuity
Suppliers & Partners	Reliability in products and services. Good delivery times, responsive customer service.	
Clients	Quality of our services Confidentiality and Integrity of their Data	
Competitors	Ethical Behavior, fair competition zero ethical faults	
Government	Compliance with statutory and regulatory requirements. Compliance with work laws and tax laws.	

Pestel Analysis

Political

Regional Political Stability

Political volatility or unrest in El Salvador and other operational regions might impact business continuity. EMAYA must monitor geopolitical dynamics and establish contingency plans to mitigate potential disruptions.

Analyzing diplomatic relations between El Salvador and other nations could influence cross-border data transfer regulations, impacting EMAYA's information security protocols.

Government Support

Investigating the extent of governmental support, including tax incentives and industry-specific regulations, offers insights into EMAYA's compliance requirements and strategic growth opportunities.

Understanding lobbying efforts or industry associations within the political landscape might aid EMAYA in shaping favorable regulatory environments.

Economic

Economic Growth in LATAM

Examining economic growth trends, trade agreements, and GDP forecasts in LATAM countries identifies potential markets for EMAYA's expansion and tailoring services to emerging market demands.

Evaluating currency exchange rates and inflation rates is crucial for pricing strategies, especially when considering client budgets and cost-effective service delivery.

Financial Stability

Assessing the financial stability of clients and market trends in the BPO sector helps EMAYA predict demand fluctuations and adjust service offerings or pricing models accordingly.

Analyzing credit availability and interest rates impacts EMAYA's investment decisions in technological upgrades and infrastructure development.

Social

Talent Pool Development

Collaborating with local educational institutions or vocational programs to cultivate specialized skills aligns with EMAYA's goal of unlocking talent. Developing partnerships may ensure a steady stream of skilled professionals.

Addressing societal perceptions of outsourcing and ensuring positive social impacts, such as job creation and skill enhancement, fosters community acceptance and support for EMAYA's operations.

Client-Centric Approach:

Recognizing evolving client preferences and expectations in BPO services allows EMAYA to tailor service offerings and engagement models. Conducting regular client feedback surveys helps in enhancing the client-provider relationship.

Technological

Tech Integration in BPO

Exploring emerging technologies, such as machine learning or chatbots, offers opportunities to streamline operations and improve service delivery. EMAYA can evaluate these tools' potential impact on efficiency and client satisfaction. Assessing the scalability and compatibility of new technologies with existing systems ensures smooth integration and minimizes disruptions in service provision.

Cybersecurity Advances

Investing in cutting-edge cybersecurity measures beyond standard protocols demonstrates EMAYA's commitment to safeguarding client data. Continual updates in encryption technologies and threat detection systems enhance resilience against evolving cyber threats.

Collaborating with cybersecurity experts or participating in industry forums allows EMAYA to stay ahead of emerging threats and adopt proactive security measures.

Environmental

Sustainability Practices

Implementing energy-efficient technologies and eco-friendly infrastructure aligns with global sustainability goals while optimizing operational costs. EMAYA can leverage renewable energy sources and efficient cooling systems in data centers to reduce environmental impact.

Adopting green practices in office facilities and promoting recycling or waste reduction initiatives reflects EMAYA's commitment to environmental responsibility and corporate citizenship.

Legal

Local Regulatory Landscape

Understanding El Salvador's data protection laws and compliance standards enables EMAYA to establish robust policies aligned with local regulations. Regular audits and legal consultations ensure adherence to evolving legal requirements.

Assessing liability clauses and legal implications in service contracts safeguards EMAYA's interests and mitigates legal risks associated with client engagements.

ISO 27001 Certification Adherence

Constantly aligning EMAYA's practices with ISO 27001 standards ensures a systematic approach to managing sensitive information. Regular audits and certifications demonstrate commitment to international best practices in information security management.

Engaging legal counsel to interpret ISO standards within the context of local laws and regulations ensures comprehensive compliance.

External Influences

Competitive Landscape

Analyzing competitors' strategies and market positioning allows EMAYA to identify unique value propositions and maintain a competitive edge. Understanding their approaches to information security aids in benchmarking EMAYA's security practices.

Monitoring market entrants and disruptive technologies enables EMAYA to proactively adapt and innovate, staying ahead in the competitive BPO landscape.

Industry Standards and Trends

Keeping abreast of evolving industry standards, certifications, and technological advancements in BPO services ensures EMAYA's services remain relevant and at the forefront of industry innovation.

Analyzing industry trends in data privacy, client expectations, and service delivery models guides EMAYA's strategic decisions and service enhancements.

SWOT Analysis

Emaya has identified the following Strengths, Weaknesses, Opportunities, and threats that for EMAYA are important:

Strengths	Weaknesses
<ul style="list-style-type: none">• Extensive Founders' Experience• Client-Centric Approach• Innovative Service Offerings	<ul style="list-style-type: none">• Potential Security Vulnerabilities• Dependency on Specific Markets
Opportunities	Threats
<ul style="list-style-type: none">• Market Expansion in LATAM• Technological Advancements	<ul style="list-style-type: none">• Cybersecurity Risks and Data Breaches• Intensifying Market Competition

More details can be found on: EMS-DOC-10 Strategic Planning

Information Security Policy

Information security is the preservation of confidentiality, integrity and availability of information. The confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes; integrity is the property of accuracy and completeness, and availability is the property of being accessible and usable on demand by an authorized entity. For EMAYA to meet this standard we have defined the following:

Information Security Objectives

1. Mitigate and prevent information security incidents through the establishment of policies and standardized procedures.
2. Maintain a work environment oriented to the protection of information and the assets that support it.
3. Maintain all security risk and threats controlled through a risk management plan; ensuring they are all at acceptable levels of risk
4. Comply with all regulations and policies. Maintain good information security practices.

EMAYA is committed to compliance with legislation of security information, regulations, best practices, and legal obligations along with client's service levels agreements.

EMAYA has introduced various methods to ensure that effectiveness and continual improvement of processes and procedures takes place; this is further registered in the continuous improvement matrix.

EMAYA shall follow a formal disciplinary process for employees who have violated the information security policies and procedures; this is executed through the disciplinary matrix that EMAYA has established together with its clients.

EMAYA shall ensure that the review of the Information Security Policy and related documents is performed at least on an annual basis or when significant changes occur to ensure suitability, adequacy, and effectiveness of the ISMS framework.

Roles & Responsibilities

Owners of the Assets	Responsibilities
President HR Director	Responsible for Human resources system, employee documents, medical files, incidents files, and corporate learning and development.
Vice-President of Operations	Responsible for all the financial documents and system.
Account Manager	Responsible for the daily activities of an account Responsible for the agents working on that account and their security practices
IT Manager	Responsible for the technical infrastructure, equipment, and their configurations, as well as maintenance of the operative equipment.
Information Security Officer	Responsible for the implementation and maintenance of the information security management system. Responsible for the development of continuous improvement plans within the company.
Supervisors / Operation Managers	Responsible for the management of employees, information, direct contact with the client.
Agents	Responsible for the client's information they use. Responsible for maintaining the integrity, confidentiality, and availability of client's data.
Vendors/subcontractors/External Auditors	All external visitors that have access to EMAYA's information are responsible for maintaining confidentiality and integrity of the information shared with them.

Information Security Supporting Policies & Documentation

At a lower level, the information security policy is supported by topic-specific policies that mandate the implementation of information security controls. Topic-specific policies are typically structured to address the needs of certain target groups within an organization or to cover certain security areas. Topic-specific policies should be aligned with and complementary to the information security policy of the organization.



A more detailed view of these documents and their location can be found on EMS-CTRL-001 Document Catalog in the DMS.