COSTAISA GROUP

Security Policy

11/07/2019

Reviews

Reviews				
Status	**Review**	**Change Description**	**Authors**	**Effective date**
Published	0	Initial publication.	Antonio Serra Francisco Araujo	06/15/2018
Published	1	ISO22301 standard elements update, minor modifications.	Antonio Serra	01/22/2019
Published	2	• Minimum security requirements related to article 11 of Royal Decree 3/2010 are added. • Reference to Services affected by the Continuity Plan is added. • Reference to the LOPDPGDD is added, and reference to the LOPD is eliminated.	Antonio Serra	05/16/2019

TABLE OF CONTENTS

1. APPROVAL AND ENTRY INTO FORCE

Text approved on 15 June 2018 by the General Management and Security Committee. This Information Security Policy becomes effective as of the date hereof and it's valid until such time, as it is replaced by a new Policy. This text supersedes the previous one, which was approved on 30 June 2011 by the management.

2. INTRODUCTION

The fulfilment of the objectives of Costaisa Group depends on ICT (Information and Communication Technologies) systems. These systems must be administered with caution by taking suitable measures to protect them in light of any accidental or deliberate damage that may affect the availability, integrity or confidentiality of the information processed or services provided. The objective of the information security is to guarantee the quality of the information and continued provision of the services, while acting in a preventive capacity, supervising daily activity and reacting promptly to any incidents. The ICT systems must be protected against rapidly evolving threats with a potential to impact on confidentiality, integrity, availability, intended use and value of information and services. To defend against these threats, it is necessary to adopt a strategy suited to changes under the conditions of the environment with a view to guaranteeing the continuous provision of the services. This means that departments must apply the minimum security measures required by the National Security Framework (NSF), and provide continuous monitoring of the service provision levels, monitor and analyse reported vulnerabilities, and prepare an effective response to any incidents with a view to guaranteeing the continuity of services. The various departments must verify that CIT security is an integral part of each stage of the life cycle of the system, from its design up to its withdrawal from service, not to mention development or acquisition decisions and operation activities. Security requirements and financing requirements must be identified and included in the planning, in the request for proposals, and in any bid terms for CIT projects. Departments must be prepared to prevent, detect, react to and recover from incidents, in accordance with Article 7 of the NSF.

3. PREVENTION

Departments must avoid, or at least prevent, where possible, the information or services from being compromised by security incidents. With that in mind, departments must implement the minimum security measures determined by the NSF, as well as any additional control identified on the basis of a threat and risk assessment. These controls, and the security roles and responsibilities of all staff members, must be clearly defined and documented.
To guarantee compliance with the policy, departments must:

1. Authorise systems before they become operational.
2. Regularly assess security, including assessments of any configuration changes implemented on a routine basis.
3. Request a regular third-party review with the aim to obtain an independent assessment.

4. DETECTION

In view of the fact that services may degrade quickly due to incidents (which range from a mere slowdown to a complete shutdown of activity) services must monitor operations on a continuous basis, in order to detect anomalies in the provision of services and act accordingly pursuant to the provisions established in Article 9 of the NSF. Monitoring is especially relevant when layers of safety are established in accordance with Article 8 of the NSF. Mechanisms related to detection, analysis and reporting will be established; information will be reported to managers on a regular basis and whenever there is a significant deviation from any parameters which have previously been designated as normal.

5. RESPONSE

Departments must:

1. Establish mechanisms to effectively respond to any security incidents.
2. Designate a point of contact for communications regarding to any incidents detected in other departments or in other agencies.

3. Establish protocols to interchange information related to the incident. This includes communications, in both directions, with Emergency Response Teams (CERT).

6. RECOVERY

To guarantee the availability of critical services, departments must develop continuity plans for CIT systems as part of their general business continuity plan and recovery activities.

7. REACH

This policy applies to all the CIT systems of Costaisa Group and to all members of the organization, with no exceptions.

Concerning ISO27001 standard, the scope of the SGSI extends to underlying processes in the field of Operations, while focusing on some of the most important processes with which services are offered to clients: Chaman Service, Administrative Client Management, Intranet Service, E-mail Service, Public Web Storage and Maintenance Service, IPS (Integrated Prevention Service), User Desktop Service, Client Staff and Payroll Management and Hosting services for SAP Services.

8. MISSION, VISION AND VALUES

8.1 Mission

Costaisa Group intends to develop a continuity business to help to improve the industrial and productive fabric.

- On the basis of organisational and technological consultancy, client companies are able to achieve greater success in their businesses.
- Guarantees the recruitment processes of professionals with employment quality and continuity in the workplace.
- Provides benefits to shareholders.
- Helps to improve the industrial network on the basis of design, development and introduction of organisational and technological solutions.

8.2 Vision

Costaisa Group intends to become the benchmark consultant in the fields in which it is active, and would like its clients to regard it as its organisational and technological partner for its strategic business projects.

8.3 Values

- Proximity and confidence: Its main asset is the professionals who make up the work teams, together with its clients, performing services and consulting in close proximity and strengthening trustworthy relationships.
- Willingness to improve day by day: Competitiveness is won by working towards continual improvement; that is why a Quality Management System has been created to adjust our processes to market demands.
- A daring attitude: The goal is to achieve its clients' objectives.

9. REGULATORY FRAMEWORK

9.1 Information Systems

9.1.1 Organic Law 3/2018, of December 5, Protection of Personal Data and guarantee of digital rights

Party responsible: Technical Management
Legal Advisor: Across Legal

9.1.2 EU Regulation 2016/679 of the European Parliament and of the Council, of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

Party responsible: Technical Management
Legal Advisor: Across Legal

9.1.3 L 34/2002 of July 11 (Information society and electronic trade services)

Party responsible: Technical Management
Legal Advisor: Across Legal

9.1.4 Telecommunication Act 9/2014, of 9 May

Party responsible: Technical Management
Legal Advisor: Across Legal

9.1.5 OM PRE/2740/2007 of 19 Sep. (Regulation on Assessment and Certification of Information Technology Security)

Party responsible: Technical Management
Legal Advisor: Across Legal

9.1.6 National Security Framework

- Royal Decree 951/2015, of 23 October, amending Royal Decree 3/2010, of 8 January, regulating the National Security Framework in the field of Electronic Administration.
- Royal Decree 3/2010, of 8 January, regulating the National Security Framework in the field of Electronic Administration.

Party responsible: Technical Management
Legal Advisor: Across Legal

9.1.7 Standard ISO27001 on Information Systems Security

Party responsible: Technical Management
Legal Advisor: Across Legal

9.1.8 Standard ISO20000 of IT Services Management

Party responsible: Technical Management
Legal Advisor: Across Legal

9.1.9 Standard ISO22301 of Business Continuity

Party responsible: Technical Management
Legal Advisor: Across Legal

9.2 Intellectual Property

9.2.1 Royal Legislative Decree 1/1996, of 12 April, approving the consolidated text of the Intellectual Property Act

Party responsible: Administration
Legal Advisor: Brugueras, García-Bragado, Molinero & Asociados

9.3 Human Resources

9.3.1 Royal Legislative Decree 2/2015, of 23 October, approving the consolidated text of the Worker's Statute Act

Party responsible: Human Resources
Legal Advisor: Brugueras, García-Bragado, Molinero & Asociados

9.3.2 Act 3/2012, of 6 July, on urgent measures for labour market reform

Party responsible: Human Resources
Legal Advisor: Brugueras, García-Bragado, Molinero & Asociados

9.3.3 Collective Bargaining Agreement of Business Premises

Party responsible: Human Resources
Legal Advisor: Brugueras, García-Bragado, Molinero & Asociados

9.3.4 Workplace Risk Prevention Act (Act 31/1995, of 8 November)

Party responsible: Human Resources Legal Advisor: Brugueras, García-Bragado, Molinero & Asociados

10. DESIGNATION PROCEDURES

The full list of committees and functions can be found in the Security Regulations. The Information Security Manager will be appointed by the Management at the proposal of the Security Committee. The appointment will be reviewed every 2 years or whenever the position becomes vacant. Any Department that is responsible for a service that is provided electronically in accordance with Act 11/2007 will appoint the System Manager and specify the corresponding roles and responsibilities within the framework established by this Policy.

11. INFORMATION SECURITY POLICY

The security committee will be responsible for the annual review of this Information Security Policy and its proposed review or maintenance. The Policy will be approved by the Security Committee and distributed for the information of all the parties concerned.

12. PERSONAL DATA

Costaisa Group processes personal data. The Security Document to which only authorised parties will have access includes the files affected and the corresponding controllers. All the information systems of Costaisa Group will be adjusted to the security levels required by the regulations for the nature and purpose of the personal data included in the aforementioned Security Document.

13. RISK MANAGEMENT

All the systems subject to this Policy must undergo a risk analysis, which assesses the threats and risks to which they are exposed. This analysis will be repeated on a regular basis, at least once a year or when:

1. The managed information changes
2. The services change
3. A serious security incident takes place
4. Serious vulnerabilities are reported

In order to harmonise risk analyses, the Security Committee will establish a benchmark assessment for the various kinds of information managed and the various services. The

Security Committee will stimulate the availability of resources with a view to responding to the security needs of the various systems, by promoting horizontal investments.

14. INFORMATION SECURITY POLICY DEVELOPMENT

This Information Security Policy complements Costaisa Group's security policies in several subjects:

- Standard ISO27001 of Information Security
- National Security Scheme (ENS) (In process of certification)
- Standard ISO22301 of Business Continuity (In process of certification)
- Standard ISO20000 of IT Service Management (In the process of certification)
- General Data Protection Regulations (RGPD)

This Policy will be developed through security regulations that address specific aspects. The Security Policy will be available to all the members of the organization that need to know it, particularly for those who use, operate or manage the information and communications systems. The documentation will be available in the Notes BBDD of Instructions and Manuals.

Basic principles include:

a) Organization and implementation of the security process.
It will be developed in the current Security Regulations published in Instman.

b) Risk analysis and management.
It will be developed in the risk analysis carried out each year for review by the management of the ISMS. The applied methodology is explained in the instruction.

c) Personnel management.
It will be developed in the current Security Regulations published in Instman.

d) Professionalism.
It will be developed in the current Safety Regulations published in Instman and in the manuals of relevant functions of each area / department.

e) Authorization and access control.
It will be developed in the current Security Regulations published in Instman.

f) Protection of facilities.
It will be developed in the current Security Regulations published in Instman.

g) Acquisition of products.
It is developed in the manual CS_MNPR_Procedure of acquisition of components.

h) Security by default.
It is included in various manuals of Systems enforcement and in the Safety Regulations.

i) Integrity and system updating.
It is included in the manual SIMNPR01_20180219_QVM_Remediación_Vulnerabilidades, and in various manuals and procedures of Systems Division.

j) Protection of stored and in transit information.
It will be developed in the current Security Regulations published in Instman. When dealing with information related to the health of people, it will always be encrypted, according to the relevant Exploitation and Systems manuals.

k) Preventative measures of other interconnected information systems.
It will be managed following the Systems Division manuals.

l) Activity record.
The QRadar corporate tool collects and manages all records, according to the relevant Systems manuals.

m) Security incidents.
It will be developed in the current Security Regulations published in Instman.

n) Continuity of the activity.
It will be developed in the Continuity Plan, ME_MNPR_Business Impact Analysis BIA and in the current Safety Regulations published in Instman. The list of services included within its scope as services that can be managed by the organization business continuity can be found in the manual M-2198 CS_MNPR_AlcanceSGSI / SGCN.

o) Continuous improvement of the security process.
As part of the ISMS and the SGCN, the System is reviewed in its entirety at least once a year following the Deming cycle (Plan, Do, Check, Act).

15. STAFF OBLIGATIONS

All the Costaisa Group members are obliged to know and comply with this Information Security Policy and Security Regulation; the Security Committee is responsible for providing the necessary means to ensure that the information reaches the parties concerned. All the members of Costaisa Group will attend a CIT security awareness session at least once a year. A continuous awareness programme will be produced for all members, especially new recruits. Those responsible for the use, operation or administration of CIT systems will receive training in the safe management of the systems to the extent they need it, to perform their tasks.
The training will be compulsory before any responsibility is assumed, both in the event that this is the first deployment or a change of job or responsibility.

16. THIRD PARTIES

When Costaisa Group provides services to other bodies or manages the information of other bodies this Information Security Policy will be passed on to them, and channels will be established for reporting and coordination purposes between the respective CIT Security Committees; response procedures will be established for any security incidents. When Costaisa Group uses third-party services or transfers information to third parties, this Security Policy and the Security Regulation pertaining to these services or information will be passed on to them. This third party will be subject to the obligations established in this regulation, and may develop their own operating procedures to ensure compliance with the same. Specific reporting and incident resolution procedures will be established. Steps will be taken to ensure that the third parties staffs are suitably aware of security aspects, at least according to the level established in this Policy. When any aspect of the Policy is unable to be respected by a third party according to the provisions of the paragraph above, the Security Manager will be required to produce a report specifying the risks involved and the manner in which they are processed. This report must be approved by the information and services affected managers before moving on.
The tracking of the supplier's service is treated in CS_MNPR_Procedimiento of SLAs tracking with suppliers.