Public Information Security Management Policy

Policy

MULTICERT_PJ.ISMS_699_en

Rating: Public

Version: 7.0

Date: 16/03/2023

MULTICERT, Serviços de Certificação Electrónica, S.A.,
Estr. Casal do Canas, Lote 3 e Lote 6 Edf. SIBS Alf I e II 2720-092 Amadora – Portugal
Phone: +351 217 123 010

Summary

1 Introduction

1.1 Objectives

This document aims to disclose the Information Security Management Policy and the commitments assumed by MULTICERT.

1.2 Target

This document should be read by the general public.

1.3 Document Structure

This document is structured into 7 chapters:

- Security policy;
- Organizational commitments;
- Scope of Protection;
- Risk Management;
- Incident Management and Business Continuity;
- Compliance with Legal Requirements;
- Maintenance and Continuous Improvement

2 Security Policy

MULTICERT, as an entity concerned with its credibility and image, is committed to reinforcing the reliability of what its business also represents: information security, not only internally, but also in its relationships with its partners and customers.

2.1 Organizational commitments

The Information Security Management Policy aims to present commitments to protect information resources. In this context, the following are the commitments assumed by MULTICERT.

The **confidentiality** of information within the ISMS scope and all information under legal compliance will be ensured.

The **integrity** of the information will be maintained;

The **availability** of information will be ensured;

The **authenticity** of the information will be guaranteed;

Non-repudiation in information flows will be guaranteed.

MULTICERT has created an ISMS framework that guarantees compliance with the objectives described above.

2.2 Scope of Protection

The Scope of Protection defined for the ISMS (Information Security Management System) is made up of processes and activities associated with the Management and Operation of the PKI (Public Key Infrastructure) and the Registration Authority service.

2.3 Risk Management

MULTICERT guarantees the management and analysis of risk to its information resources.

As a result of the respective risk analysis, a Risk Treatment Plan is drawn up to ensure effective management of the risks.

2.4 Incident Management and Business Continuity

Being aware of the risks that may occur, and having an attitude of absolute transparency towards its partners and customers, MULTICERT maintains a Business Continuity Plan implemented in order to guarantee the commitments assumed in this policy, thus ensuring that all situations that may occur will be handled by incident management and business continuity, applying measures to control the impact on information resources.

2.5 Compliance with Legal Requirements

MULTICERT, aware of its commitments to customers and partners, provides services that comply with legal, regulatory, normative and contractual requirements, which protect its activity. As such, a compliance management process has been implemented, assumed to be one of the most relevant tools for complying with information security requirements.

2.6 Maintenance and Continuous Improvement

MULTICERT guarantees the existence of conditions for your ISMS (Information Security Management System) to be audited, maintained and continuously improved, through the operationalization of the Plan – Do - Check - Act method, in accordance with the requirements set out in the ISO/IEC 27001 standard.