



INFORMATION SYSTEMS SECURITY POLICY

June 2026

CONTENTS

INFORMATION SYSTEMS SECURITY POLICY

1. Introduction	1
2. Scope	1
3. Principles	1
4. Responsibilities	2
5. Guidelines	2
6. Review and Update	2
7. Compliance	2
8. Approval	2

INFORMATION SYSTEMS SECURITY POLICY

1. INTRODUCTION

At Onizea (Onizea Tech, S.L.) we recognize that information system security is of vital importance to the ongoing success of our operations and to maintaining the trust of our customers, partners and stakeholders.

As an information technology service provider, we are committed to complying with the highest standards of information security such as ISO 27001, COBIT (Control Objectives for Information and Related Technologies) and ITIL (Information Technology Infrastructure Library), as well as other applicable regulations.

This Information Systems Security Policy sets out our commitment to protecting confidential and critical information relating to our operations, as well as guidelines for its secure and responsible management.

2. SCOPE

This policy applies to all employees, contractors, consultants and third parties who access or handle Onizea's information systems and data. This includes, but is not limited to, information digitally stored, or in printed form or transmitted by any means.

3. PRINCIPLES

Our Information Systems Security Policy is based on the following fundamental principles:

1. **Confidentiality:** Onizea protects the confidential information of its company, clients and stakeholders, preventing unauthorized access or disclosure.
2. **Integrity:** Onizea ensures the accuracy and integrity of information, preventing unauthorized modifications or corruption.
3. **Availability:** Onizea guarantees that information is available and accessible when required for business operations.
4. **Legal and regulatory compliance:** Onizea complies with all applicable laws, regulations and standards relating to information security, including ISO 27001, COBIT and ITIL.
5. **Commitment:** Onizea is committed to the continuous improvement of the management system by following a PDCA cycle that ensures the desired security levels are always maintained.
6. **Objectives:** Onizea periodically sets a set of objectives and indicators to enable the proper monitoring of security developments within the organisation.

4. RESPONSIBILITIES

It is the responsibility of all Onizea employees and stakeholders to comply with this policy and follow the guidelines set out to protect confidential information. The information security management team is charged with implementing and maintaining this policy, as well as providing the necessary guidance and support to ensure compliance.

5. GUIDELINES

1. **Access to information:** Access to confidential information will be restricted to those employees who require it to carry out their duties. Appropriate access controls will be put in place to ensure proper authentication and authorisation.
2. **Personal data protection:** We will comply with all applicable data protection laws and ensure the privacy and security of the personal data we process.
3. **Risk management:** We will carry out regular information security risk assessments and take measures to mitigate and manage the risks identified.
4. **Awareness and training:** We will provide information security training and awareness to all employees to ensure a proper understanding of security policies and procedures.
5. **Security incidents:** We will implement procedures for the reporting and management of information security incidents, including the investigation of security breaches and appropriate response.

6. REVIEW AND UPDATE

This policy will be reviewed and updates periodically to ensure its continued effectiveness and alignment with changes in the operating environment and best practice in information security.

7. COMPLIANCE

Failure to comply with this Information Systems Security Policy may result in disciplinary action, including termination of employment or termination of service contracts, as appropriate.

8. APPROVAL

This Information Systems Security Policy has been approved by Onizea's Executive Board and will come into full effect since the date of its publication.

ONIZEA's Executive Board
L'Hospitalet de Llobregat, July 08th 2026