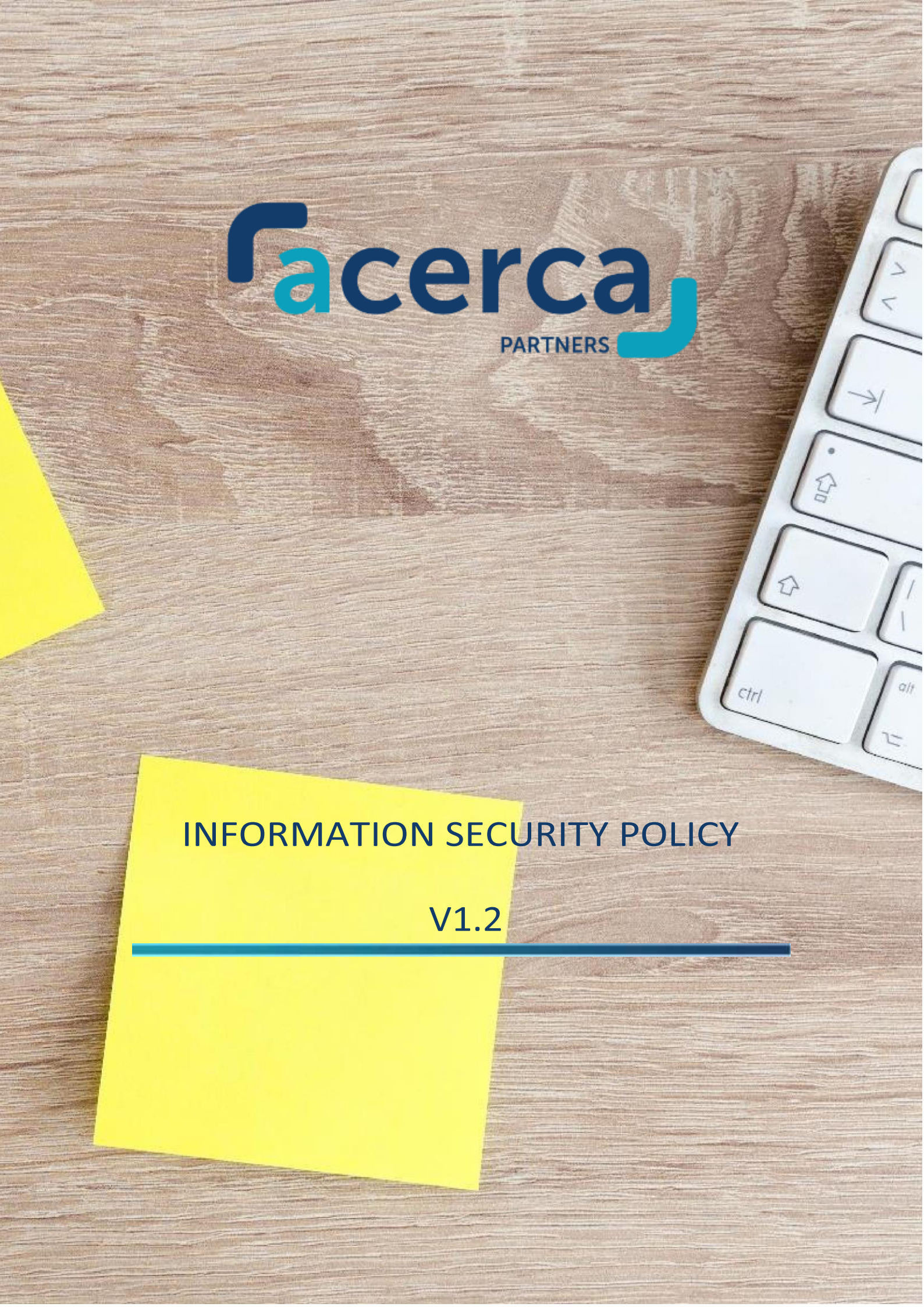

INFORMATION SECURITY POLICY

V1.2

INFORMATION SECURITY POLICY

V1.2

Table of Contents

1.- VERSION CONTROL

INFORMATION TECHNOLOGY POLICIES

CHANGE CONTROL BOX VERSION: 1.2

Version	Date	Description of the change	Remarks
0	01/02/2020	Creation	
1	25/04/2023	Sending new version	
1.1	18/05/2023	Updating the Document	
1.2	16/10/2023	Updating of the document following observations after audit	

2.- INTRODUCTION

ACERCA PARTNERS, S.L. has as a priority to safeguard the security of information, whether personal or not, and for this purpose it establishes an information security system.

The Information Security Policy is drawn up as a starting point for the information security management system implemented at ACERCA PATNERTS, S.L.

This policy must be known and adhered to by all staff.

3.- OBJECTIVES OF INFORMATION SECURITY MANAGEMENT

The general objectives of the policy are:

- Ensure access, integrity, confidentiality, availability, and the continued provision of our services, acting preventively, supervising daily activity and reacting quickly to incidents.
- Have the necessary control measures in place to comply with the legal requirements that are applicable as a result of the activity carried out, especially in relation to the protection of personal data and the provision of services through electronic means.
- Protect information resources and the technology used to process them from internal or external, deliberate or accidental threats, in order to ensure compliance with the confidentiality, integrity, availability, legality and reliability of the information.
- Describe in a general way the actions to be carried out for the classification of information assets.
- Describe in a general way the actions necessary for the risk analysis in accordance with the institution regulations compliance.
- Describe in a general way the actions to be carried out for the training of personnel.
- Describe the structure for the framework of information security policies, standards, and procedures to be developed in the institution.
- Compliance with legal requirements on information security, as well as any others that we subscribe to.
- Continuous improvement of the information security management system

4.- RISK MANAGEMENT

Risk analysis and management will be an essential part of the security process and must be kept permanently updated.

The risks to which we are exposed must be analysed. The results of these analyses should determine the most appropriate security management actions to minimize and prioritize them. To this end, the methodology that guarantees the reliability and repeatability of our risk assessments will be followed.

Risk analysis should be conducted on a regular basis to account for changes in security requirements, as well as changes in assets, threats, vulnerabilities, and impacts. Risk management, on the other hand, must be carried out in a methodical manner and capable of generating comparable and reproducible results.

Once the results have been obtained, it is necessary to decide when a risk is acceptable and when it is not, always according to the principles of service and information.

For each of the risks identified, the most appropriate treatment will be developed based on risk management.

Risk management will allow the maintenance of a controlled environment, minimizing risks to acceptable levels. The reduction of these levels will be achieved through the deployment of security measures, which will establish a balance between the nature of the data and the processing, the risks to which they are exposed and the security measures.

5.- ROLES AND RESPONSIBILITIES

The responsibilities in security are:

Security Officer

- Establish the technical measures, at a logical level, that guarantee security
- Carry out risk analysis and management, applied to information processing systems

Management

- Ensure the necessary resources
- Perform the system review

6.- REVIEW

This policy will be reviewed at least once a year and whenever there are relevant changes in the organization, in order to ensure that it is adapted to the strategy and needs of the organization.