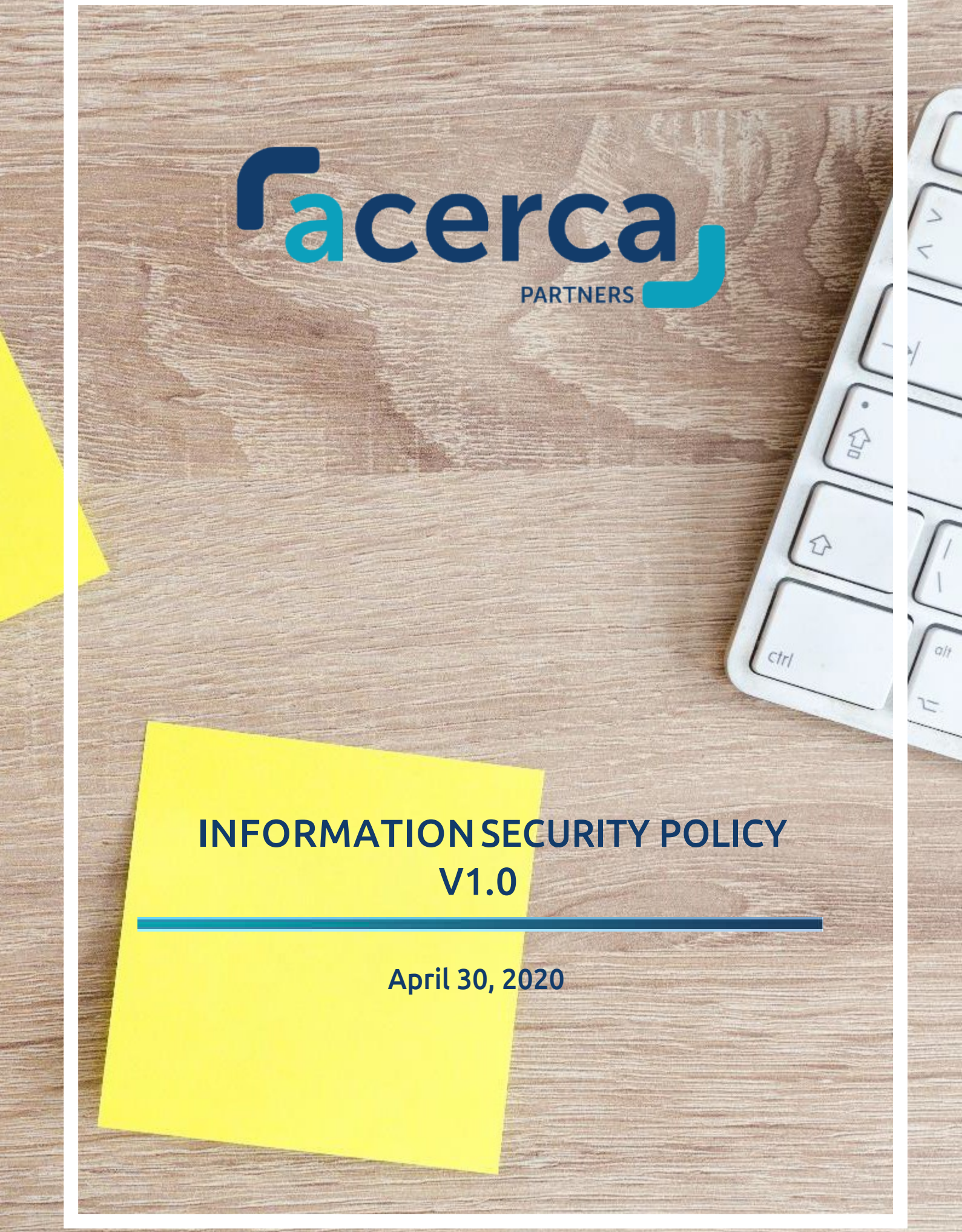

INFORMATION SECURITY POLICY V1.0

April 30, 2020

INFORMATION SECURITY POLICY V1.0

Table of Contents

1.- VERSION CONTROL

	INFORMATION TECHNOLOGY POLICIES	
		VERSION: 1.0

CHANGE CONTROL BOX		
Version	**Date**	**Description of change**
0	01/02/2020	Creation

2.- INTRODUCTION

Acerca Fits has as a priority to safeguard the security of information, whether personal or not, and for this it establishes an information security system.

This policy must be known and complied with by all staff.

3.- OBJECTIVES OF INFORMATION SECURITY MANAGEMENT

The general objectives of the policy are:

- Ensure access, integrity, confidentiality, availability, authenticity, traceability of information and the continued provision of our services, acting preventively, supervising daily activity and reacting quickly to incidents.
- Have the necessary control measures to comply with the legal requirements that are applicable as a result of the activity carried out, especially with regard to the protection of personal data and the provision of services through electronic means
- Protect information resources and the technology used for their processing, against threats, internal or external, deliberate or accidental, 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 and cadastre of information assets.
- Describe in a general way the actions necessary for the Risk analysis in accordance with the regulations in force in the institution.
- Describe in a general way the actions to be carried out for the training of personnel.
- Describe the structure for the framework of policies, standards and procedures on information security to be developed in the institution.

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 analyzed. The results of these analyses should determine the most appropriate security management actions to minimize them and prioritize them. To this end, the methodology that guarantees the reliability and repeatability of our risk evaluations will be followed.

Risk analysis should be performed periodically to account for changes in security requirements, as well as changesinassets, threats, vulnerabilities and impacts. For its part, risk management must be carried out in a methodical manner and capable of generating comparable and reproducible results.

After obtaining the results, it must be decided when a risk is acceptable and when it is not, always according to the principles of service and information.

For each of the identified risks, the most successful 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 carried out through the

deployment of security measures, which will establish an equalibrio between the nature of the data and the treatments, the risks to which they are exposed and the security measures.

5.- ROLES AND RESPONSIBILITIES

The responsibilities in security are:

Security Officer

- Establish technical measures, at a logical level, to guarantee safety
- Perform risk analysis and management, applied to information processing systems

Address

- 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 the needs of the organization itself.

The Management