1. Purpose of the document

This document presents the security policy adopted by Primatec. In this policy, Primatec will present rules and principles for Information Security Management.

The information Security Policy applies to the entire scope and domain of the Information Security Management System and must concern all employees of Primatec without exception and all other persons concerned by information security in their work activities (trainees, suppliers, etc.).

Each employee is required to be familiar with the security management system, to apply the information security documentation applicable to his/her business activity and to comply with all security requirements.

Non-compliance with rules and requirements will result to disciplinary measures.

2. Glossary

- **Confidentiality:** Property of an information that is accessible only to authorized persons or systems.
- **Integrity:** The property of an information that it is modified only by authorized persons or systems in a controlled manner.
- **Availability:** The property of an information that it is accessible only by authorized persons when necessary.
- **Information Security:** Preserving/protecting confidentiality, integrity and availability of the information.

3. Information Security Management

Primatec operates in a high-tech sector in which there is an intense competition.

Managing information security is no longer an option but a necessity. If information security incidents occur at Primatec, they can be fatal to the company's existence and future.

Any observed or suspected security incident must be reported and sent to the Information Security Responsible via email to the following email address: RSSI@primatec.tn

3.1 Information Security Objectives

The general objectives of the information security management system are the following:

- Guarantee to our partners, customers, employees and all interested parties that the availability, integrity and confidentiality of information will be appropriately maintained.
- Guarantee to our customers that we manage all information security risks related to their assets that are hosted by our company.
- Guarantee the continuity of the company's activity in order to be able to meet its commitments with its customers.
- Guarantee to our partners, customers, employees and all interested parties that we comply with the applicable laws and regulations related to information security and respect of personal data.
- Implement necessary and adequate measures for the management of the company's assets in order to minimize the impact of threats that may affect the continuity of the company's activities and its commitment with its customers.
- Ensure meticulous monitoring of all risks related to information security that may affect all company's assets.
- Win new business with customers who have high requirements in terms of information security

The management is engaged to offer all the technical, financial and human resources to achieve its objectives and to support all the actions that are part of the implementation of ISMS in order to minimize risks and to ensure a good management of information security.

3.2 Information Security Requirements

This policy and the entire information security management system are compliant with the ISO 27001 standard Version 2013, the applicable laws and regulations and the requirements of the company's customers.

3.3 Information Security Planification

Risk analyses are conducted regularly to ensure that the ISMS is properly adapted to the context (stakes, requirements of internal and external stakeholders, etc...) to identify and protect from undesirable effects that may affect it. These analyses carried out under the responsibility of the

Information Security Responsible are also an opportunity to highlight possible areas for improvement.

At the end of the risk analyses, a treatment plan is proposed which describes when and how the identified actions will be carried out (correction, prevention, improvement, etc.) as well as how their effectiveness can be evaluated.

The risk treatment options selected by Primatec comply with the acceptance criteria defined with Management, depending on the selected option, measures may be implemented as proposed in Annex A, in accordance with the declaration of applicability, or based on proposals from the IT team.

3.4 Information Security Responsibilities

Position	Responsibility
Information Security Responsible	Responsible of Information Security
Physical Security Responsible	Responsible of Physical Security
IT administrator	Responsible of Networks Security
Information Security Responsible	Responsible of Personal Data Security
Information Security Responsible	Responsible of Information Security Incidents treatment
Project/Test manager Or Team Leader	Responsible of Projects Information Security
Test Equipment Team Leader	Responsible of Test Equipment Security
IT administrator	Responsible of Applications Security
Logistics manager	Responsible of Suppliers Information Security
All Employees	Respect and follow all Information Security policies

The company's information security policy is reviewed yearly by the executive management as part of the management review. Changes and updates to this policy in this context are part of the continuous improvement process of the information security system.

This policy will be communicated to interested parties if necessary.