CYBER SECURITY MANAGEMENT PROCEDURE (K25-FD 5.9)

Cyber risk management is the process of identifying, analyzing, evaluating, addressing, and monitoring cyber security threats to networked systems, data, and users. The goal is to minimize potential risks and help organizations protect their assets and business.
This Procedure is meant to protect the sensitive information and systems of Roiatti srl, outlining the necessary measures and best practices to safeguard our digital assets, ensure data integrity, and maintain the confidentiality of customer and company information.

Roiatti ensures effective cybersecurity is achieved by mitigating the risk of cyber-crime in our organization and addressing the following principles:

Risk Management	Roiatti includes a risk self-assessment about cyber risk in our file "*Struttura Sistema integrato*", on Sheet "*Analisi dei rischi*", enabling the company to prioritize the biggest threats and ensures appropriate responses. Risks and best practices are also included in our GDPR Manual.
Secure Configuration & user access	Roiatti mitigates the risk of data breach by Access Control of buildings and IT systems/software, we ensure that physical access to server and workstations and other critical infrastructure is restricted to authorized personnel only. • Multi-Factor Authentication (MFA) is implemented for all employees to access company systems and sensitive information. • Strong Passwords: we require employees to use strong, unique passwords and change them regularly. • Access Levels: We assign access levels based on job roles and responsibilities to ensure that employees only have access to the information necessary for their tasks

	• Wi-fi: we have set-up a separate wi-fi connection for Guests so that they cannot access or view Roiatti network
Home and Mobile Working	It is not applicable for now. This section will be reviewed, when necessary, as mobile working is not applied at Roiatti.
Incident management	Roiatti relies on a specialized third party IT company that prevents the impact of a possible cyber security incident by setting up a security system, that is monitored and updated regularly. In case of incidents, this IT Company works with Roiatti to identify the cause of the incidents and determine the extent of the damage. The IT Company has deeply studied Roiatti structure and prepared a detailed Disaster Recovery Plan that will restore affected systems and data to normal operations as quickly as possible.
Malware Prevention & Network Security	To mitigate the risks of malware that might damage and/or disrupt files or allow unauthorized access to our systems, Roiatti makes sure that our Antivirus systems work and are constantly updated. We also have a Firewall which is deployed to monitor and control incoming and outgoing network traffic based on predetermined security rules.
Monitoring	Our IT third-party vendor conducts regular audits to ensure ongoing compliance with cybersecurity standards. Also, we have a contract of monitoring and in case of faults, they immediately reach out to solve the problem.
Removable media controls	Training/information is regularly given to emphasize the need to digitally and physically protect removable device
Accountability, user education and awareness	• Roiatti will assign one clerk to work in cooperation with the Third-Party Vendor who is responsible for all updates.

	• Regular cybersecurity training sessions are given for all employees, covering topics such as phishing, password management, and safe internet practices. • Awareness Campaigns: we run ongoing awareness campaigns to keep cybersecurity top-of-mind for employees • Simulated Phishing Attacks: Conduct regular simulated phishing attacks to test employee readiness and improve their ability to recognize and respond to phishing attempts. • Employee Feedback: Encourage employees to provide feedback on cybersecurity policies and procedures to help identify areas for improvement. • Industry Best Practices: Stay informed about industry and GDPR best practices and emerging threats to continuously enhance the company's cybersecurity posture.

Cybersecurity risks are analyzed and self-assessed in our file *Struttura Sistema Integrato*, Sheet "Risks Analysis". Roiatti has identified the following threats/risks for cybersecurity:

- **Data access and confidentiality:** ensure only authorized employees have access to the needed data
- **Data integrity:** ensure data accuracy and completeness, complete back-up procedures, ensure data is not modified without authorization
- **Malware (malicious software):** software that has been specifically designed to perform malicious tasks on a device or network, such as corrupting data or taking control of a system
- **Spyware:** a form of malware that hides on a device providing real-time information sharing to its host, enabling them to steal data like bank details and passwords.

- **Phishing attack:** when a cybercriminal attempts to lure individuals into providing sensitive data such as personally identifiable information (PII), banking and credit card details, and passwords.
- **A supply chain attack:** when a cybercriminal hacks an organization by compromising a third-party vendor in its supply chain.
- **Trojan:** creates a backdoor in your system, allowing the attacker to gain control of your computer or access confidential information.
- **Theft of Money:** Cyber-attacks may gain access to credit card numbers or bank accounts to steal money.
- **Loss** of computer data or cyber-attack.
- **Data manipulation** (a form of cyber-attack that doesn't steal data but aims to change the data to make it harder for an organization to operate).
- **Data Destruction** when a cyber attacker attempts to delete data)
- **Ransomware attack:** a type of malware which prevents you from accessing your device and the data stored on it, usually by encrypting your files
- **Spoofing:** a type of cybercriminal activity where someone or something forges the sender's information and pretends to be a legitimate source, business, colleague, or other trusted contact for the purpose of gaining access to personal information, acquiring money, spreading malware, or stealing data.

Also, Roiatti ensures all IT equipment is listed on our assets list and properly maintained, kept updated (Annex 04).

Roiatti has decided to rely on a specialized IT Supplier to make sure our IT System is secure and always updates; our supplier also trains our staff on all aspects of cyber security and Data Protection. In addition, they prepared a Disaster Recovery Plan and Business Continuity Plan (Available in Italian) that is reviewed at least annually, to make sure the Company is ready and able to keep on all activities in case of need.

By adhering to these procedures, our company commits to maintaining a robust cybersecurity framework that protects our digital assets, ensures the integrity and confidentiality of data, and fosters trust with our customers and partners.

Roiatti will maintain comprehensive documentation of all cybersecurity policies and procedures and regularly review and update such policies (at least annually) to ensure they remain effective and compliant with current regulations and industry standards.

This procedure is given to all office employees / workers using the IT System as an integral part to the internal training provided by our IT supplier.