RISK MANAGEMENT

POLICY

[Soggetto]

1 Document version control

	Last modified	Last modified by	Changes to the document
0.1	[DATE]		Document created for the first time

2 Index

3 Risk Management Policy

3.1 Purpose

The purpose of this policy is to define the company's risk management policy for information security

3.2 Recipients

All employees and third-party users.

Risk and risk management applied to information security and the confidentiality, integrity and availability of information owned, processed, stored and transmitted by the organisation.

3.3 Principle

Information security management for the company is based on appropriate and adequate risk management.

3.4 What is risk management

Risk can be defined as the threat or possibility that an action or event will negatively or positively affect an organisation's ability to achieve its objectives.

Risk management can be defined as the systematic application of principles and approaches and a process by which a company identifies and evaluates the risks associated with its activities and then plans and implements risk responses.

3.5 Risk appetite

Overall, the company has a moderate risk appetite, which means that risks are mitigated in a cost-effective and risk-proportionate manner and a certain risk acceptance is acceptable according to business needs.

3.5.1 Low-risk propensity

The company has a low appetite for risk, which means that risks will not be accepted and that it will have resources allocated to mitigate risk in a proportionate and cost-effective manner:

- Unauthorised access, use or release of personally identifiable information or sensitive data.
- Non-compliance with laws, regulations, policies or procedures concerning technology.
- Lack of resilience against cyber security threats.

3.6 Risk identification and assessment

Risk assessments are carried out at regular intervals or at least every 12 months and where significant changes have occurred or may occur.

Risks are identified and assessed at least for

- The processing, storage or transmission of confidential, personal or cardholder information
- Third-party providers that process, store or transmit confidential, personal or cardholder information
- New systems
- Significant changes

3.7 Risk Register

All risks are recorded in the company risk register.

3.8 Risk Signalling

The risk register is reviewed during the review team meeting.

Risks are reported to the Review Team

Significant risks, identified as risks requiring senior management attention or risks with a score above 20 or risks classified as serious, are reported to senior management and form part of the company's corporate risk management reporting.

3.9 Risk Review

Risks are regularly reviewed and monitored during the Review Team meeting to ensure:

- Advancement of Risk Action
- Effectiveness of risk action
- Residual risk management

3.10 Risk treatment

A risk manager is assigned to all risks

3.10.1 Risk acceptance

The decision to accept risks is taken by the head of the relevant department and/or senior management.

The criterion for accepting the risk is based on these criteria

- The risk is classified as low and it is not convenient to treat it.
- There is a business or commercial opportunity that justifies the threat and impact.
- There is no risk treatment
- The impact of the risk occurring is acceptable to the company

3.10.2 Risk mitigation

Where a risk must be mitigated

- An action plan is approved by the relevant departmental manager and/or the Review Team and/or Senior Management.
- Responsibility for the implementation and management of the plan is assigned.
- Risks are reported and reviewed during the management review team meeting and recorded in the risk register.

3.11 Risk assessment

Risk impact assessment is considered as a function of:

- Compliance and law
- Reputation
- Customers
- Corporate goals and objectives
- Financial performance

Compliance with standards

3.12 Measuring Compliance

The information security management team will monitor compliance with this policy through various methods, including, but not limited to, company tool reports, internal and external audits, and feedback to the information security policy manager.

3.13 Exceptions

Any exception to the policy must be approved and recorded by the information security officer in advance and reported to the management review team.

3.14 Non-compliance

An employee found to have violated this policy may be subject to disciplinary action, up to .

3.15 Continuous improvement

The policy is updated and revised as part of the continuous improvement process.