ZIRA | ISO 27001

Information security policy statement

Our commitment to securing trust

At ZIRA Group, safeguarding information is foundational to our mission of building trust with clients, partners, and stakeholders. We are committed to protecting the confidentiality, integrity, and availability of all information assets, ensuring alignment with legal, regulatory, and contractual obligations while fostering a culture of accountability, transparency, and continuous improvement.

www.ziragroup.com

info@ziragroup.com

This policy is communicated to all employees, partners, and stakeholders and is reviewed annually or in response to significant changes to maintain relevance and effectiveness.

Core commitments

Protection of information assets

- Ensure the confidentiality of sensitive data by restricting access to authorized individuals, both internally and externally.
- Maintain the integrity of information through accuracy, completeness, and traceability in all processes.
- Guarantee the availability of critical information to support business operations, projects, and services.

Compliance & legal responsibility

- Adhere to all applicable laws, regulations, and contractual requirements, including ISO 27001 standards.
- Process, store, and destroy information lawfully, ethically, and transparently, retaining data only as long as necessary.

Risk management & mitigation

- Implement a robust risk management framework to identify, assess, and mitigate threats (internal/external, deliberate/accidental) to an acceptable level.
- Regularly evaluate vulnerabilities and deploy controls to minimize potential impacts on business continuity and stakeholder trust.

Accountability & governance

- Top Management commitment: Drive the Information Security Management System (ISMS) through leadership, resource allocation, and periodic reviews to align with strategic goals. Top Management assumes ultimate responsibility for ISMS governance, incident management, and policy adherence.
- Employee responsibility: All employees and stakeholders are accountable for complying with security policies, reporting incidents, and upholding best practices within their roles.

Strategic objectives

- Secure business operations: Integrate security into all administrative, commercial, and technical processes to protect client data, third-party information, and intellectual property.
- Incident management: Establish clear procedures to report, investigate, and resolve security breaches promptly, minimizing operational disruption.
- Business Continuity: Develop, test, and maintain continuity plans to ensure resilience against disruptions and rapid recovery of critical systems.
- Awareness & training: Foster a security-conscious culture through regular employee training, emphasizing the importance of safeguarding information assets.
- Continuous improvement: Enhance the ISMS through regular audits, stakeholder feedback, and technological advancements to address evolving threats.
- Implementation & enforcement
- Disciplinary actions: Enforce a formal disciplinary process for policy violations to uphold accountability.
- Resource allocation: Dedicate tools, technologies, and expertise to effectively implement, operate, and review the ISMS.
- Periodic reviews: Conduct systematic evaluations of the ISMS to ensure compliance with ISO 27001, stakeholder requirements, and emerging security challenges.

Our commitment

ZIRA Group is committed to protect information as a cornerstone of our ethical business practices. This policy underscores our dedication to operational excellence, stakeholder trust, and sustainable growth in an increasingly interconnected world.