

# Information Security Policy Statement

CODIX acknowledges that the principles of Confidentiality, Integrity, and Availability in Information Security Management are integral to its overall management function. CODIX's management considers these principles as core responsibilities and essential to the best business practices in implementing appropriate Information Security Controls, in line with the ISO 27001 standard.

The CODIX Information Security Policy statement aims to operate at the highest standards at all times and to fully implement and maintain the ISO 27001 standard, including continual improvement, through registration and annual review.

The security objectives of our ISMS are to:

- Protect all CODIX's information assets against loss of confidentiality, integrity or availability.
- Protect all Cloud's information assets, managed by Codix in the scope of the SaaS offer, against loss of confidentiality, integrity or availability.
- Mitigate the risks associated with the theft, loss, misuse, damage or abuse of these assets.
- Ensure that information users are aware of and comply with all current and relevant information security regulations and legislation.
- Provide a safe and secure information system working environment for employees and any other authorized users.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the information they handle.
- Maintain business continuity and minimize impact in the event of an incident.

The CODIX Security board Management is committed to:

- Comply with all applicable laws and regulations and contractual obligations,
- Implemente continual improvement initiatives, including risk assessment and risk treatment strategies, while optimizing management resources to meet information security requirements,
- Communicate its Information Security Objectives and performance in achieving them across the organization and to interested parties,
- Ensure that CODIX resources are not used in ways that compromise the interests of stakeholders.
- Maintain an Information Security Management System (ISMS), including a security manual and procedures, to provide guidance on information security matters for employees, customers, suppliers, and other stakeholders,
- Collaborate closely with customers, business partners, and suppliers to establish appropriate Information Security Standards,
- Adopt a forward-looking view on future business decisions, including the continual review of risk evaluation criteria, which may have an impact on Information Security,
- Train all members of staff in the needs and responsibilities of Information Security Management,
- Constantly strive to meet, and where possible exceed, the expectations of customers and staff.

To periodically assess the effectiveness of security activities, CODIX implements key performance indicators, which are reviewed during management reviews.

CODIX recognizes that its staff play a vital role in achieving its security objectives and provides them with the necessary resources and support. In return, all CODIX employees are actively involved in the ISMS and are required to comply with its rules.

*This policy statement applies to all employees, contractors, and third-party users who have access to the organization's information assets, including information systems, networks, data, and physical facilities.*

The ISO Group Manager is appointed as the Top Management Representative to oversee the ISMS, report on its status, and support its maintenance.

Ilia Kirilov  
CODIX Group CEO