Information Security Policy Statement

CODIX recognizes that the disciplines of Confidentiality, Integrity and Availability in Information Security Management are integral parts of its management function. The management of CODIX views these as primary responsibilities and fundamental to the best business practice of adopting appropriate Information Security Controls, along the lines laid down in the ISO 27001 standard.

CODIX Information Security Policy statement seeks to operate to the highest standards continuously and to implement and operate fully 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.
- In the event of an incident, ensuring that business continuity is maintained and impact minimized.

CODIX Security board Management commits to:

- Comply wit all applicable laws and regulations and contractual obligations,
- Implement continual improvement initiatives, including risk assessment and risk treatment strategies, while making best use of its management resources to better meet Information Security requirements,
- Communicate its Information Security Objectives, and its performance in achieving these objectives, throughout the organization and to interested parties,
- Take action to ensure that CODIX resources are not used against interested parties,
- Adopt an Information Security Management System comprising a security manual and procedures which provide direction and guidance on information security matters relating to employees, customers, suppliers and interested parties who come into contact with its work,
- Work closely with its Customers, Business Partners and Suppliers in seeking 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, its customer's, staff expectations.

In order to assess periodically the **effectiveness** of the undertaken security activities, we implement **key performance indicators**, which we revise during the management reviews.

CODIX recognizes that its staff have a major role to play in achieving its security objectives and therefore provides them with the resources and support that they require.

In return All ***CODIX*** employees get involved in the Information Security Management System and are obliged to follow the ISMS 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 a Top Management Representative in order to oversee the ISMS, report the status of the ISMS and support the maintenance of the ISMS.

Ilia Kirilov
CODIX Group CEO

V1.0.2_03/05/2024