CyberGate

DOCUMENT NAME

Information Security Policy

Document Control

Information				
Version	Document level	Reference Code	Published Date	Review Frequency
2.3	(POL) Policy	CG-POL-005	05.04.2022	Yearly

Review & Approval Record		
Prepared by	Reviewed by	Approved by
Mariam Abdelrahman Information Security Specialist	Srdjan Babic Director of Information Security Governance, Risk and Compliance	Mo Bin Bouta Al-Harsousi Managing Director
05.04.2022	05.04.2022	06.04.2022

Revision Record				
Version	Date	Page	Author	Description of change
1.0	26.01.2020	0X	CG GRC Team	Introduction of Information Security Policy
2.0	07.02.2021	0X	CG GRC Team	Revision
2.1	29.03.2021	08	CG GRC Team	Updated continual Improvement as per CG ISO 27001 Stage 1 Audit Finding + Management Review
2.2	04.04.2021	0X	CG GRC Team	Updated Classification to Public- Minor change
2.3	05.04.2022	05	CG GRC Team	Added Policy statement and Information Security Objective, non-operational function removed, Training for 3rd party revoked.

Table of Contents

DOCUMENT CONTROL 1

1. PURPOSE 3

2. SCOPE 3

3. REQUIREMENTS 3

3.1 ISO 27001:2013 3

4. POLICY STATEMENT 3

5. INFORMATION SECURITY OBJECTIVES 4

6. PRINCIPLES FOR IMPLEMENTATION 4

6.1 INFORMATION SECURITY POLICY 4

7. MANAGEMENT REVIEW 5

8. KEY PERFORMANCE INDICATOR (KPI) 5

9. REFERENCES 5

1. Purpose

The purpose of the ISMS policy is to demonstrate and express the intention and commitment of CYBERGATE to:

- Protect information assets from all threats, whether internal or external, deliberate or accidental thereby ensuring uninterrupted services to Employees, Customers and investors.
- Manage the risk to the acceptable level through design, implementation and maintenance of an effective Information Security Management system

This policy forms the basis and identifies key principles of all Information Security initiatives in CYBERGATE.

2. Scope

This document defines CYBERGATE ISMS policy and principles that need to be followed at CYBERGATE.

3. Requirements

The requirements are set and defined in Annex A of ISO 27001:2013.

3.1 ISO 27001:2013

A.5 Information security policies		
A.5.1 Management direction for information security		
Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles of which they are considered.		
A.5.1.1	Policies for information Security	**Control** A set of policies for information security shall be defined, approved by management, published, and communicated to employees and relevant external parties.
A.5.1.2	Review of the policies for information security	**Control** The policies for information security shall be reviewed at planned intervals, or if significant changes occur, to ensure their continuing suitability, adequacy, and effectiveness.

4. Policy Statement

CYBERGATE will ensure that the information security management framework and controls are aligned with its business activities. CYBERGATE shall establish information security objectives aligned to its business objectives, information security requirements and pertaining risks.

CYBERGATE shall protect the Confidentiality, Integrity and Availability of all information assets, in order to enhance the trust, reliability and confidence of all employees, investors and Managed Customers.

The CYBERGATE Information Security Risk Management Framework defines following terms as identified in the above policy statement:

Confidentiality concerns with the protection of sensitive information from unauthorized disclosure.

Integrity is related to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.

Availability relates to information being available when required by the business. It also concerns the safeguarding of necessary resources and associated capabilities.

5. Information Security Objectives

The CYBERGATE management has developed the following information security objectives:

- To meet client's requirements and satisfaction.
- Protect client data and safeguard shareholder value,
- Manage information security risks, enhance controls and gain competitive advantage,
- Validate compliance to legal and regulatory requirements,
- Ensure that contractual liabilities regarding information protection are adhered to,
- Demonstrate due diligence and inspire confidence in all stakeholders of the entity,
- Manage and reduce costs related to information security, management of IT and business processes,
- To minimize the security incidents
- Enable certification against ISO standards.

6. Principles for Implementation

6.1 Information Security Policy

CYBERGATE management acknowledges the importance of ensuring information security and is committed to supporting the information security goals and principles. CYBERGATE management has given below principles for the effective implementation of ISMS in the organization:

6.1.1 Establish the 'ISMS Governance Committee' representing the Executive Management of CYBERGATE to demonstrate CYBERGATE management commitment towards information security management.

6.1.2 Appoint an 'Information Security Manager' responsible for managing all ISMS related activities of CYBERGATE on behalf of CYBERGATE Executive Management.

6.1.3 Appoint Management Representative (MR) & Secretary for representing CYBERGATE for coordinating and managing ISMS activities as per the requirements of ISO 27001 Standards.

6.1.4 Define the roles and responsibilities of all ISMS Committee.

6.1.5 Prepare ISMS Scope, Objectives, Policies, and Guidelines to support the implementation of the ISMS Policy.

6.1.6 Develop an Information Security Risk Management framework to assess Information Security risks.

6.1.7 Develop Risk Assessment Report and Risk Treatment Plan.

6.1.8 Attain management approval for implementing controls for risk mitigation and formal acceptance of residual risk.

6.1.9 Allocate appropriate resources for the implementation, management and operation of ISMS.

6.1.10 Define and conduct training and awareness programme for all CYBERGATE Staff.

6.1.11 Establish the process in organisation for continual improvement of Information Security Management System.

7. Management review

7.1. Management shall review, communicate, and make available this document to all Cybergate ISMS Affected Parties (as defined within the ISMS ISO 27001 Scope) and other interested parties to ensure compliance of this policy.

7.2. Management shall review the management objectives and approve the ISMS at planned intervals or at least once annually.

7.3. Policies, procedures, and all documents of ISMS will be reviewed on annual basis.

7.4. Management shall determine corrective actions as an output of the management review meeting.

7.5. Internal Audit will be done at least once a year.

8. Key Performance Indicator (KPI)

- Information Security Management System (ISMS) Policy should be at least communicated once in a year to all CYBERGATE end users.

9. References

- ISO 27001:2013

CyberGate

YOUR TRUSTED DEFENDERS

TELEPHONE & FAX

+971 (0) 2 6655855
+971 (0) 2 6712 211

ADDRESS

Al Bostan Tower (Office 103)
Abu Dhabi, UAE. PO BOX 43123

WEB

www.cybergate.tech
info@cybergate.tech