# Information Security Management Policy

## 1. Purpose

The purpose of Information Security Management System (ISMS) in ***Cubic Information Systems*** is to ensure the continuity and protection of the business processes and information assets which are considered within the ISMS scope.

**"Protect Information belonging to, or under the custody of Azure Cubic Systems ACS Solutions and Services"**

The information security needs and objectives are stated in this document to minimize the impact of security incidents on the operations of ***Cubic Information Systems***.

## 2. Scope

This policy applies to all Managers and staff of ***Cubic Information Systems***, contractors, and third party employees under contract, who have any access to, or involvement with, the business processes, information assets, and supporting Information assets and processes covered under the scope of ISMS.

## 3. Definition

- Availability – Property of being accessible and usable upon demand by an authorized entity.
- Asset – Anything that has value to the organization.
- Confidentiality – Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- Integrity – Property of accuracy and completeness.
- ISMS – Information Security Management System is the part of overall management system and required to establish, implement, maintain and continually improve information security of the organization.

## 4. Corporate ISMS Policy

The Information Security Management System of ***Cubic Information Systems*** intends to ensure:

- Confidentiality of all information assets (information is not disclosed to unauthorized persons through deliberate or careless action). Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. The unauthorized disclosure of information could have limited adverse effects on organizational operations, organizational assets, or individuals.

- Integrity of all business processes, information assets, and supporting IT assets and processes, through protection from unauthorized modification, guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The unauthorized modification or destruction of information could have severe or catastrophic adverse effects on organizational operations, organizational assets, or individuals.
- Availability of all business processes, information assets, and supporting Information assets and processes to authorized users when needed, ensuring timely and reliable access to and use of information. The disruption of access to, or use of, information or an information system could have serious adverse effects on organizational operations, organizational assets, or individuals.
- All processes and stakeholders shall follow the rules and regulations, or circulars published in the organization.
- ***Cubic Information Systems*** complies with the laws, regulations and contractual obligations which are applicable to the organization in general and to its ISMS.
- ***Cubic Information Systems*** has established and implemented an Incident management process to ensure that all breaches of information security, actual or suspected are reported and investigated.
- All applicable information security requirements are satisfied.

## 5. Responsibility

***Cubic Information Systems*** shall ensure that all activities required to implement, maintain, and review this policy are performed. All personnel, regarded as included in the ISMS scope, must comply with this policy statement and its related security responsibilities defined in the information security policies and procedures that support the corporate information security policy. All personnel, even if not included in the ISMS scope, have a responsibility for reporting security incidents and identified weaknesses, and to contribute to the protection of business processes, information assets, and resources of ***Cubic Information Systems***.

## 6. Enforcement

***Cubic Information Systems*** holds the right to monitor the compliance of its personnel with this policy. Manager and staff of ***Cubic Information Systems***, contractors, and third-party employees, who fail to comply with this policy, may be subjected to appropriate disciplinary actions.

## 7. Ownership and Revision

CEO is responsible for communicating the ISMS Policy to all persons working for or on behalf of the organization and making it available to the public.

**CEO** **Date: 01-02-2024**