# Enterprise Information Security Policy (EISP)

SECP

SECURITIES AND EXCHANGE
COMMISSION OF PAKISTAN

# Table of Contents



# Record of Amendments

This is a record of changes made to this document, based on review.

| Rev | Approval Date/ Revision Date | Document ID /Code | Description of Change | Approved By |
|---|---|---|---|---|
| 0.0 | May'2015 | P-EISP | First approval | The Commission |
| 1.0 | October'2019 | P-EISP | Revision has been made, based on M/s Deloittee ISMS Gap Analysis report. | The Commission |

# Table of Abbreviations & Definitions

| Abbreviation / Term | Full Word / Definitions |
|---|---|
| Availability | Property of being accessible and usable upon demand by an authorized entity |
| Confidentiality | Property that information is not made available or disclosed to unauthorized individuals, entities, or processes |
| EISP | SECP's Enterprise Information Security Policy |
| HoD | Head of the Department/Division |
| IA&CD | Internal Audit & Compliance Department |
| Information Asset | Piece of information or data, stored in any manner that has value to SECP |
| Information Security | Protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities |
| Information Security Management System (ISMS) | Set of policies and processes established by management to assess the security requirements, develop and implement controls, evaluate effectiveness of controls and implement improvements following a continual improvement process |
| Integrity | Property of accuracy and completeness |
| ISD | Information Security Department |

| Abbreviation / Term | Full Word / Definitions |
|---|---|
| IS-GRC | Information Security –Governance, Risk Management and Compliance |
| IS-GRCC | Information Security –Governance, Risk Management and Compliance Council |
| ISMS | Information Security Management System |
| ISMS Manual | SECP's Information Security Management System Manual |
| Policy | Intentions and direction of SECP as formally expressed by its Top Management |
| Risk | Effect of uncertainty on objectives |
| SECP | Securities & Exchange Commission of Pakistan |
| ToR | Terms of Reference |
| User | All employees of SECP, consultants, advisors, interns, vendors, contractors, suppliers, and any others using, accessing, processing, storing or communicating the SECP's information and information processing facilities. |

## 1. Purpose

The main purpose of the policy is to protect information and information assets of SECP by ensuring:

a. Confidentiality of information — SECP information assets shall only be accessible to those authorized to access such information.

b. Integrity of information — SECP information assets shall remain accurate and error free without omissions.

c. Availability of information — Authorized Users shall have access to SECP information assets when required.

## 2. Scope

The policy included in this document applies to all SECP Users [1]and it covers the high level policies required to be in place to support and ensure effectiveness of information security at all levels in SECP in accordance with business requirements and applicable Pakistan's and International laws & regulations.

## 3. Policy

a. SECP is committed to the protection of its business information and to mitigate risks associated with theft, loss, misuse, damage or abuse of information or information systems.

b. All SECP Divisions, Departments, Wings & Users are equally committed to the implementation of information security related policies and shall be responsible for protection of SECP information and comply with the ISMS Manual and related documents.

c. SECP's IS-GRC Council shall:

i. establish, operate and maintain an ISMS[2] with a defined scope and boundaries to meet the information security objectives;

ii. ensure the objectives for information security management system are designed in alignment with SECP strategic goals;

iii. shall ensure the ISMS is implemented through a set of policies, procedures and standards and are communicated to all information users; and

iv. ensure the ISMS will be reviewed regularly in light of changing business environment, corporate strategy and compliance obligations.

d. Information security violations & breaches shall be promptly reported to management and will be subject to disciplinary actions as mentioned in the Human Resources Manual under the section titled as 'Grounds for Disciplinary Action'.

[1] SECP USERS: All employees of SECP, consultants, advisors, interns, vendors, contractors, suppliers, and any others using, accessing, processing, storing or communicating the SECP's information and information processing facilities.

[2] ISMS: Information Security Management System

## 4. Roles and Responsibilities

Please refer to the Terms of Reference for Information Security –Governance, Risk Management, and Compliance Council (ToR IS-GRCC) and ISMS Roles & Responsibilities document.

## 5. Compliance & Enforcement

### 5.1 Enforcement

Respective HoDs shall be responsible for enforcing the Enterprise Information Security Policy (EISP) within their division / department.

### 5.2 Compliance Measurement

The IA&CD will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

### 5.3 Non-Compliance

Users that do not adhere to this policy may be subject to disciplinary action based on SECP's Human Resource Manual.

## 6. Exceptions

Any exception to the policy must follow the ISMS Policy Exception Handling Process.

## 7. Reference

a. ISMS Roles & Responsibilities;
b. ISMS Manual;
c. SECP's Human Resource Manual;
d. Control of Documents and Control of Records; and
e. ISMS Policy Exception Handling Process.