Information Security Policy

DCS-SICPA-000477-POL-PO-EN
Version : 2
Effective Date : 30-Apr-2025

Policy owner: Doron Tenne

SICPA

A Platform
for Sovereignty

TABLE OF CONTENTS

1 PURPOSE

Information is a valuable and key asset supporting SICPA's business, it must be protected appropriately. Information protection and security is integral to SICPA's value proposition of "Enabling Trust". Handling and protection of information is also subject to laws and regulations.

The aim of this policy is to set the foundation for information security at SICPA so as to reduce to an acceptable level SICPA's risk exposure related to information and information systems and to enable the company to achieve a higher level of maturity in this area. Company information includes information that is electronically generated, printed, filmed, typed, stored or verbally communicated.

2 POLICY

1. Information security must be seen in the context of evolving threats. The means adopted to protect information must adapt accordingly. Information security risks must therefore be assessed on a regular basis.

2. Risk is managed by implementing security measures that aim to preserve the confidentiality, integrity and availability of information resources. This is done by ensuring an appropriate level of traceability and protecting against unauthorized access, use, disclosure, disruption, modification or destruction, whether deliberate or accidental. Security measures must be adopted and implemented in a balanced manner (e.g. where costs are justified by risk mitigation benefits) and consistent with SICPA's business strategy.

3. Information and information systems must be protected, in all security respects by taking into account confidentiality, integrity and availability requirements. This includes SICPA's information and also information relating to third parties.

4. SICPA must establish a comprehensive, professional, effective, Group-wide cyber and information security program, validated by the Executive Committee and supported by the local management of SICPA entities. The aim of the program is to continuously improving the overall level of information security.

5. SICPA staff must be made aware of and responsible for information security. The education, training and awareness programs implemented to promote this must be designed and implemented world-wide and should be reviewed and updated periodically.

6. SICPA must comply with the requirements of software licenses and with other legal, regulatory and contractual obligations relating to information security, as well as to the company security standards.

7. Security incidents, breaches of the information security policy and suspected information security weaknesses must be analysed, managed and reported through the defined management process as appropriate.

8. A disaster recovery planning process (DRP) must be implemented for critical IT systems to reduce the disruption caused by any disaster or a security failure to an acceptable level. The plan will combine preventive and recovery measures and must be aligned with Company business continuity plans.

3 RESPONSIBILITY FOR ENFORCEMENT AND MONITORING

The Policy Owner is responsible for the implementation of this policy. The Policy Owner is also responsible for ensuring compliance with the policy, maintaining the related procedures (escalation, remediation, non-conformity) and documenting all remedial actions in case on non-compliance.

The Policy Owner must ensure that all SICPA employees and specifically Heads of Divisions, Corporate Functions and Entities across the Group, have read, understood and signed-off the Policy.

The Policy Owner will leverage and involve the relevant functions/departments such as Group Security and Cyber Office, Strategic Affairs, Compliance, Legal and Finance to enforce compliance across all SICPA.

4 RELATED DOCUMENTS

Item No.	ID number or Link	Title
1	DCS-SICPA-000249	Information Classification Standard
2	DCS-SICPA-000170	Acceptable Use of Information Resources Standard
3	DCS-SICPA-000215	Information Retention and Disposal Standard
4	DCS-SICPA-000214	Social Media and Social Networking Standard
5	DCS-SICPA-000208	Personal Data Confidentiality Standard
6	DCS-SICPA-000250	Disaster Recovery Planning Standard
7	DCS-SICPA-000173	Connect your Own Device Standard
8	DCS-SICPA-000207	Information Archiving Standard

SIGNING PAGE

This is a representation of an electronic record that was signed electronically in Livelink.
This page is the manifestation of the electronic signature(s) used in compliance with the organizations electronic signature policies and procedures.

UserName: Doron.Tenne@sicpa.com
Title: Mr
Date: Tuesday, 29 April 2025, 05:06 PM W. Europe Daylight Time
Meaning: Document approved and signed as Document Owner
==========

UserName: Vivian.Teixeira@sicpa.com
Title: Ms
Date: Wednesday, 30 April 2025, 10:43 AM W. Europe Daylight Time
Meaning: Document approved and signed as Releaser
==========