switch
software solutions

SWITCH-POL-SG-25- Information security policy

Version 1.0

Classification: **public**

Table of contents

Revisions

Date (DD/MM/YYYY)	Version	Authors	Description
10/03/2025	1.0	Joaquín Pérez	Initial version

Policy

Purpose

Switch's Board of Directors recognizes the importance of identifying and protecting information security assets belonging to Switch and their customers. Measures will be taken to protect this information against destruction, unauthorized access, disclosure, modification, or usage, regardless of its media format.

Additionally, the Board of Directors commits to implementing, developing and maintaining an information security management system, which will in turn help preserve these basic principles:

a. Confidentiality: ensure only explicitly authorized parties can access an information asset
b. Integrity: ensure information and its processing methods are exact and complete.
c. Availability: ensure authorized parties can access information assets when required.

Responsibilities

Switch's Board of Directors is responsible for providing all necessary means to communicate this information security policy, at the CISO's request, and provide the required resources to implement all required controls.

All line managers and middle managers (leadership) are responsible for implementing this Information Security Policy on areas under their watch, as well as providing the means for their personnel to apply what is stated in this Policy.

All Switch personnel, regardless of their contract, are responsible for complying with what is stated in this Policy.

Description

Switch's Board of Directors declares that Switch is in compliance with all local laws and requirements regarding information security.

To effectively manage information security, the Board of Directors will establish an Information Security Committee. This committee will be responsible for promoting, communicating and supporting information security development efforts, integrating into the organization's planning processes. It will also define strategies to protect information assets, approve plans, policies and any additional element that can support asset protection. Additionally, a Chief Information Security Officer (CISO) will be appointed, who will guide on the implementation of controls, as well as develop, maintain and revise an Information Security Management System (ISMS).

Switch's policy entails:

a. Establishing annual objectives related to Information Security, as well as developing an action plan to achieve them.
b. Developing an information security risk assessment and treatment process, and implementing any necessary corrective and preventive actions.

c. Classifying and protecting information in compliance with local laws, regulations, and its sensitivity.
d. Complying with information security requirements from contracts, laws or regulations.
e. Providing information security awareness training to all staff.
f. Developing an Information Security Incident Management Policy.
g. Requiring all personnel to report suspected or confirmed information security violations according to established procedures.
h. Providing all necessary resources to ensure business continuity.

This Information Security Policy will be part of all the documents that are part of Switch's ISMS.

Compliance

Non-compliance with this Policy increases risk exposure and the likelihood of information security incidents. Upon verification of non-compliance, the Board of Directors may take any measures deemed adequate to ensure proper compliance with the provisions of this policy.