Security Introduction

(FSISP) Framework Science information security policy (ISP) is a set of rules, policies, and procedures designed to ensure all users and networks within our organization meet minimum IT security and data protection security requirements.

Purpose

- An **organizational model** for information security
- **Detect and preempt** information security breaches caused by third-party vendors, misuse of networks, data, applications, computer systems, and mobile devices.
- **Protect** Framework Science organization's **reputation**
- **Uphold** ethical, legal, and **regulatory requirements** both in Mexico and the U.S.
- **Protect our client's data** and respond to inquiries and complaints about non-compliance of security requirements and data protection

Responsibilities and duties of FS employees

Operational Governance

- Security programs
- Acceptable use policies
- Network security
- Physical security
- Business continuity
- Access management
- Security awareness
- Risk assessments
- Incident response
- Data security
- Disaster recovery
- Incident management

FRAMEWORK
< SCIENCE / >

FSISP **Cyber Policy Introduction**

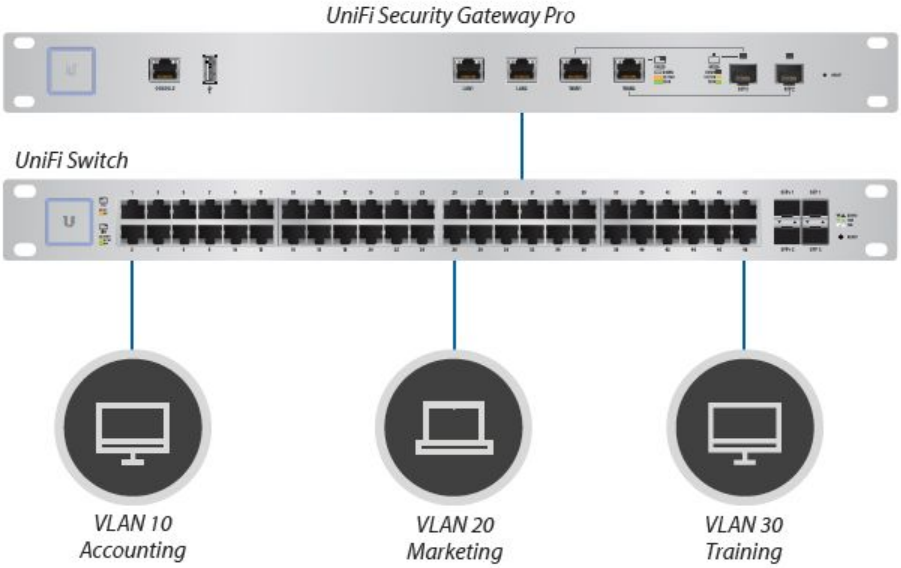
To mitigate risks apart from the Framework Science Security Policy and reinforce partners Security Policy.

We have all Software Engineering staff work on Framework Science assigned computers so we can guarantee certainty that all work is being done with the security standards to protect our client's intellectual property.

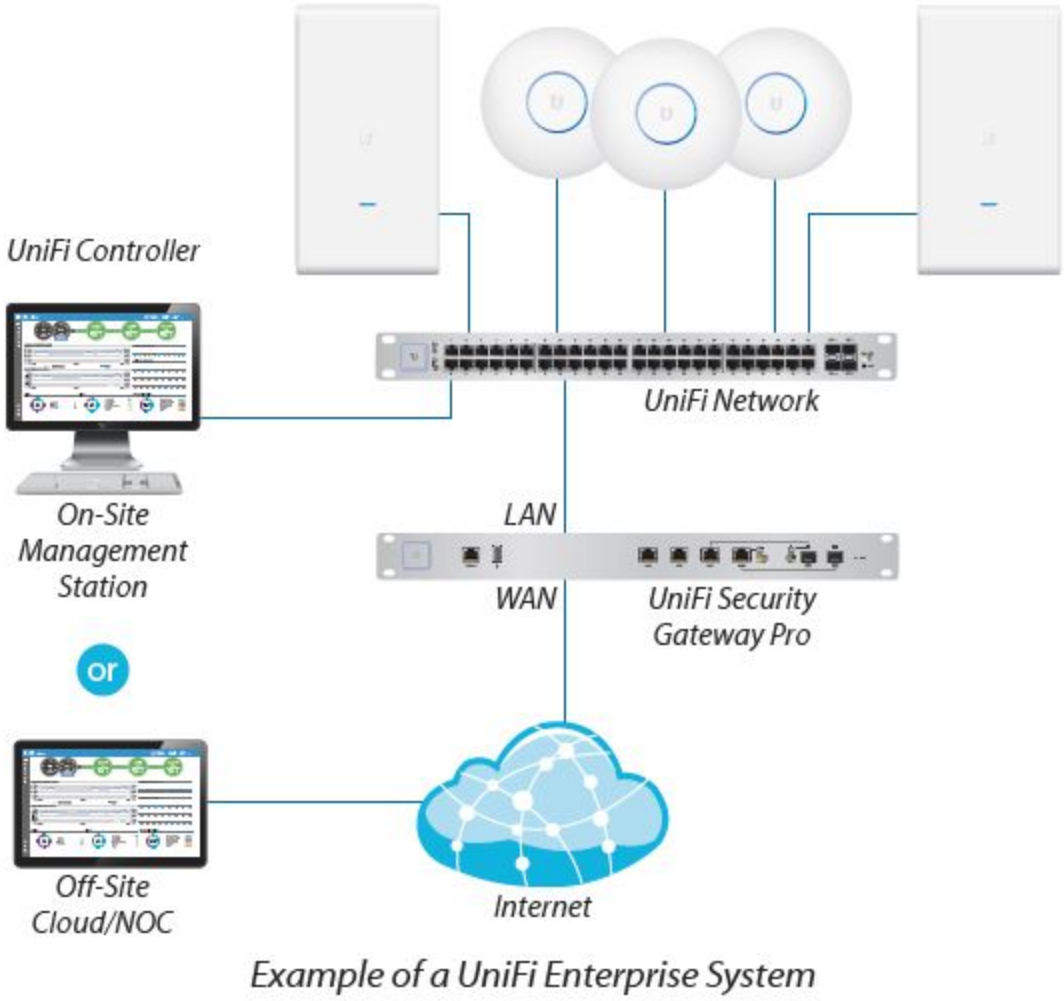
Framework Science Security Components

- The **Security Gateway** combines reliable security features with high-performance routing technology in a cost-effective unit.
- **Powerful Firewall** Performance: The Security Gateway offers advanced firewall policies to protect your network and its data.
- Convenient **VLAN Support**: The Security Gateway can create virtual network segments for security and network traffic management.
- VPN Server for Secure Communications: A **site-to-site VPN** secures and encrypts private data communications traveling over the Internet.
- **QoS for Enterprise VoIP and Video**: Top QoS priority is assigned to voice and video traffic for clear calls and lag-free, video streaming. The Security Gateway is deployed in the same manner as Access Points for wireless networking. Use the intuitive Controller to conduct device detection, provisioning, and management.
- **Detailed Analytics**: Use configurable reporting and analytics to monitor large user groups and expedite troubleshooting. Advanced search and sorting capabilities make network management more efficient.
- **Multi-Site Management**: A single Controller running in the cloud can manage multiple sites: multiple, distributed deployments, and multi-tenancy for managed service providers. Each site is logically separated and has its own configuration, maps, statistics, guest portal, and administrator read/write and read-only accounts.
- **LAN/WLAN Groups**: The Controller can manage flexible configurations of large deployments. Create multiple LAN and WLAN groups and assign them to the respective devices.

FRAMEWORK
< SCIENCE / >



Network Segmentation with VLAN



Example of a UniFi Enterprise System

Each Framework office will be required to have the same configuration and each office will be connected to an MLPS to facilitate a secure connection between branches.