

GE-19 Security Policy

Applicability: All employees of Sempra Infrastructure must comply with full policy.

Responsible Dept.: Health, Safety and Security

Contact: Carlos Barajas

CBarajas@sempraglobal.com.mx

Effective Date: 08/20/2024

Revision Date: mm/dd/yyyy

Revision: 00



Policy at a Glance



Policy Overview

This policy establishes the guidelines and responsibilities to preserve the physical safety and integrity of all Sempra Infrastructure (“SI”) employees, assets, and critical information, inside or outside SI facilities, from a security perspective.

GE-19 Security Policy

Applicability: All employees of Sempra Infrastructure must comply with full policy.

Responsible Dept.: Health, Safety and Security

Contact: Carlos Barajas

CBarajas@sempraglobal.com.mx

Effective Date: 08/20/2024

Revision Date: mm/dd/yyyy

Revision: 00



Policy

1. Applicability

- This policy applies inside SI facilities and in any location where an SI employee is conducting business on behalf of SI.

2. Scope

- This policy establishes guidelines and responsibilities that all SI employees must follow to preserve the physical safety and security of all SI employees, assets, and Non-digital critical information.

3. Security Guidelines

- All SI employees must comply with the applicable laws and regulations, SI policies and procedures and ethical standards of business and observe, promote, and respect human rights to safeguard the physical safety, security, and integrity of other employees and SI assets and critical information from any injury, damage, misuse, or loss.
- The Security department is responsible for implementing security measures and coordinating activities that detect and prevent threatening scenarios to provide peace of mind to SI employees and preserve the safety, security, integrity, reliability and reputation of SI, its employees, assets, and SI Critical Information.
- The Security department shall implement security measures based on at least the following:
 - Identification of vulnerabilities through analyses of activities, assets, and regions.
 - Communication and response to security incidents.
 - Investigation and analysis of incidents and identification of opportunities for improvement.
 - Collaboration with SI Vendors, Clients, and Guests to enhance security and assure adherence to SI policies.
 - Establishment of security expectations for SI employees, each asset, and critical information.
 - Implementation of training and auditing processes to assure compliance with security measures and procedures.
 - Management of resources for the surveillance, access control, threat deterrence, and monitoring.
 - Continuous contact with authorities and other interest groups to anticipate risks, vulnerabilities, and responses.
- Incident response will be conducted by the Security department and law enforcement, when necessary, to maximize the protection of personnel, assets, and information and minimize any losses through effective collaboration, reduced response times, and improved information sharing.
- Vendors and Guests may be subject to security measures and procedures established by the Security department. In such case, the Security department or responsible SI employee shall inform the Vendor and Guest of the applicable requirements through a safety orientation.

Any non-compliance by Vendors or Guests of SI policies, guidelines, measures, procedures, or requirements may lead to removal from SI facilities and further access restrictions. In the event of such restrictions, the SI department responsible for the Vendor or Guest must be notified and is required to proceed with the applicable measures and procedures, which may include the termination of a service and commercial agreement.

GE-19 Security Policy

Applicability: All employees of Sempra Infrastructure must comply with full policy.

Responsible Dept.: Health, Safety and Security

Contact: Carlos Barajas

CBarajas@sempraglobal.com.mx

Effective Date: 08/20/2024

Revision Date: mm/dd/yyyy

Revision: 00



4. SI Employee Responsibilities

- All SI employees must follow these guidelines when performing their work and conducting business on behalf of SI in any location:
 - Adhere to all SI security measures and procedures and be familiar with and comply with all sites, job, or task-specific security requirements that may apply based on the nature or location of their work or business.
 - Safeguard the physical integrity of other SI employees, SI sites, and equipment by adhering to the applicable security policies, procedures, and all equipment usage guidelines and management directives.
 - Safeguard SI non-digital critical information from any loss or unauthorized disclosure based on SI policies and applicable procedures.
 - Assure the good reputation of SI, its affiliates, or its personnel by preventing threatening scenarios that impact the peace of mind of SI employees and the integrity and reliability of SI, its employees, assets, and critical information.
 - Timely alert management and the Security department of any site or equipment issue that negatively impacts the security and that should be addressed by technicians or specialists.



Definitions

- *Client* – means any Person who requests or acquires one or more products or services from SI.
- *Critical Information* - Confidential business data or knowledge that is essential for the safe, efficient, and reliable development, operation, construction, and business continuity of Sempra Infrastructure, that is not publicly known and may provide a competitive advantage, as well as a safe and secure environment for our people and locations where SI is present.
- *Non-digital critical information* – *Vital data in non-digital formats, such as printed documents.*
- *Guest* – means any non-SI employee, client or Vendor.
- *Person* – means any individual, corporation, limited partnership, general partnership, limited liability partnership, limited liability company, joint stock company, joint venture, corporation, unincorporated organization, association, company, trust, group, or any governmental or political subdivision or any agency, department, or instrumentality thereof.
- *Sempra* – means the parent company of Sempra Infrastructure.
- *SI* – means Sempra Infrastructure.
- *Vendor* – means any distributor, contractor, merchant, supplier, or other seller providing goods or services to SI.



Related Documents - documents available at TheHub and SempraNet.

- Code of Business Conduct
- Sempra Human Rights Policy
- GE-20 Safety Policy
- GE-21 Health Policy
- GE-M01 Health, Safety and Security Directives
- GE-M01-I01 Instruction for SI Guests

GE-19 Security Policy

Applicability: All employees of Sempra Infrastructure must comply with full policy.

Responsible Dept.: Health, Safety and Security

Contact: Carlos Barajas

CBarajas@sempraglobal.com.mx

Effective Date: 08/20/2024

Revision Date: mm/dd/yyyy

Revision: 00



Information Retention Guidance

For guidance as to the appropriate retention period for information related to this policy, please refer to the Information Management Policy – *Corporate Policy available at SempraNet.*



Help is a Click Away

You may raise questions or concerns about compliance or ethics issues through one the anonymous [Ethics & Compliance Helpline Reporting Options](#).



Revision Dashboard

Number of revision	Date of revision (mm/dd/yyyy)	Affected Section(s)	Included changes	Authorization