Information Security Policy

Introduction

Information security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of our organisation. The goal of the Sempre Information Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within the organisation while providing value to the way we conduct business. Protection of the Confidentiality, Integrity, and Availability are basic principles of information security, and can be defined as:

- Confidentiality – Ensuring that information is accessible only to those entities that are authorised to have access, many times enforced by the classic "need-to-know" principle.
- Integrity – Protecting the accuracy and completeness of information and the methods that are used to process and manage it.
- Availability – Ensuring that information assets (information, systems, facilities, networks, and computers) are accessible and usable when needed by an authorised entity.

Sempre has recognised that our business information is a critical asset and as such our ability to manage, control, and protect this asset will have a direct and significant impact on our future success.

This document establishes the framework from which other information security policies may be developed to ensure that our company can efficiently and effectively manage, control and protect business information assets and those information assets entrusted to Sempre by its stakeholders, partners, customers and other third-parties.

The Sempre Information Security Program is built around the information contained within this policy and its supporting policies.

Purpose

The purpose of the Sempre Information Security Policy is to describe the actions and behaviors required to ensure that due care is taken to avoid inappropriate risks to Sempre, customers, business partners, and its stakeholders.

Audience

The Sempre Information Security Policy applies equally to any individual, entity, or process that interacts with any Sempre Information Resource.

Responsibilities

Executive Management

- Ensure that an appropriate risk-based Information Security Program is implemented to protect the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of Sempre.
- Ensure that information security processes are integrated with strategic and operational planning processes to secure Sempre's mission.

- Ensure adequate information security financial and personnel resources are included in the budgeting and/or financial planning process.
- Ensure that the Security Team is given the necessary authority to secure the Information Resources under their control within the scope of the Sempre Information Security Program.
- Designate an Information Security Officer and delegate authority to that individual to ensure compliance with applicable information security requirements.
- Ensure that the Information Security Officer, in coordination with the Security Team, reports annually to Executive Management on the effectiveness of the Sempre Information Security Program.

Information Security Officer

- Chair the Security Team and provide updates on the status of the Information Security Program to Executive Management.
- Manage compliance with all relevant statutory, regulatory, and contractual requirements.
- Participate in security related forums, associations and special interest groups.
- Assess risks to the confidentiality, integrity, and availability of all Information Resources collected or maintained by or on behalf of Sempre.
- Facilitate development and adoption of supporting policies, procedures, standards, and guidelines for providing adequate information security and continuity of operations.
- Ensure that Sempre has trained all personnel to support compliance with information security policies, processes, standards, and guidelines. Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities.
- Ensure that appropriate information security awareness training is provided to Sempre personnel, including contractors.
- Implement and maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of Sempre.
- Develop and implement procedures for testing and evaluating the effectiveness of the Sempre Information Security Program in accordance with stated objectives.
- Develop and implement a process for evaluating risks related to vendors and managing vendor relationships.
- Report annually, in coordination with the Security Team, to Executive Management on the effectiveness of the Sempre Information Security Program, including progress of remedial actions.

Information Security Team

- Ensure compliance with applicable information security requirements.
- Formulate, review and recommend information security policies.
- Approve supporting procedures, standards, and guidelines related to information security.

- Provide clear direction and visible management support for information security initiatives.
- Assess the adequacy and effectiveness of the information security policies and coordinate the implementation of information security controls.
- Ensure that ongoing security activities are executed in compliance with policy.
- Review and manage the information security policy waiver request process.
- Review information security incident information and recommend follow-up actions.
- Promote information security education, training, and awareness throughout Sempre, and initiate plans and programs to maintain information security awareness.
- Report annually, in coordination with the Security Officer, to Executive Management on the effectiveness of the Sempre Information Security Program, including progress of remedial actions.

All Employees, Contractors, and Other Third-Party Personnel

- Understand their responsibilities for complying with the Sempre Information Security Program.
- Use Sempre Information Resources in compliance with all Sempre Information Security Policies.
- Seek guidance from the Information Security Team for questions or issues related to information security.

Policy

- Sempre maintains and communicates an Information Security Program consisting of topic-specific policies, standards, procedures and guidelines that:
    - Serve to protect the Confidentiality, Integrity, and Availability of the Information Resources maintained within the organisation using administrative, physical and technical controls.
    - Provide value to the way we conduct business and support institutional objectives.
    - Comply with all regulatory and legal requirements, including: (adjust as appropriate)
        - HIPAA Security Rule,
        - PCI Data Security Standard,
        - Information Security best practices, including ISO 27002 and NIST CSF,
        - Contractual agreements,
- The information security program is reviewed no less than annually or upon significant changes to the information security environment.

References

- ISO 27002: 5, 6, 7, 18
- NIST CSF: ID.AM, ID.BE, ID.GV, PR.AT, PR.IP

Waivers

Waivers from certain policy provisions may be sought following the Sempre Waiver Process.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	September 2021	September 2021	Richard Hoare	Document Origination
1.0.1	September 2022	September 2022	Richard Hoare	Document reviewed
1.0.2	October 2023	October 2023	Richard Hoare	Document reviewed and amended
1.0.3	September 2024	September 2024	Richard Hoare	Document reviewed and amended

Ownership

The Sempre information security manager keeps this document updated on behalf of the Executive leadership team. Should you have any questions with this document, please contact us via our email support@sempre.co.nz