IT-SEC-010 Information Security Policy

Version 1.0.0

Introduction

Information security is a holistic discipline, meaning that its application, or lack thereof, affects all facets of an organization or enterprise. The goal of the Sonesta Information Security Program is to protect the Confidentiality, Integrity, and Availability of the data employed within the organization 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 authorized 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 authorized entity.
- **Safety** – Managing risk to prevent a cybersecurity incident so it doesn't result in injuries, environmental disasters or loss of life.

Sonesta has recognized 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 the enterprise can efficiently and effectively manage, control and protect its business information assets and those information assets entrusted to Sonesta by its stakeholders, partners, customers and other third parties.

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

Purpose

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

Scope

This policy prescribes, in high-level terms, the types of technical, administrative, and physical security controls that will be implemented to protect the confidentiality, integrity, and availability of information technology resources and information assets for which the Company has ownership, management, or stewardship responsibilities. The policy also

prescribes responsibilities to ensure these controls are implemented, maintained, and monitored.

Audience

The Sonesta Information Security Policy applies equally to any individual, entity, or process that interacts with any Sonesta **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 Sonesta.
- Ensure that information security processes are integrated with strategic and operational planning processes to secure the organization'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 Sonesta 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 Information Security Committee, reports annually to Executive Management on the effectiveness of the Sonesta Information Security Program.

Information Security Officer

- Director, Office of Information Security will provide updates on the status of the Information Security Program to Executive Management.
- Own and administer the Information Security Policy that serves as the framework for identifying, implementing, and maintaining information security at the Company.
- 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 Sonesta.

- Facilitate development and adoption of supporting policies, procedures, standards, and guidelines for providing adequate information security and continuity of operations.
- Ensure that Sonesta 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 company 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 Sonesta.
- Develop and implement procedures for testing and evaluating the effectiveness of the Sonesta 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 Director, Office of Information Security to Executive Management on the effectiveness of the Sonesta Information Security Program, including progress of remedial actions.

Security, Risk and Compliance (SRC)

- Ensure compliance with applicable information security requirements.
- Formulate, implement, review and maintain appropriate enterprise information security policies and standards and if required, technology, to successfully meet the ISP objectives.
- Approve supporting procedures, standards, and guidelines related to information security.
- Assess the adequacy and effectiveness of the information security policies and coordinate the implementation of information security controls.
- Maintain Sonesta's IT Compliance obligations, including but not limited to Sarbanes-Oxley (SOX) 404 IT General and Application Controls and Payment Card Industry (PCI) Compliance. SRC tests compliance controls on a regular basis, and existing controls may be modified as part of this testing.
- Review and manage the information security policy waiver request process.
- Identify and recommend how to handle non-compliance.
- Provide clear direction and visible management support for information security initiatives.
- Promote information security education, training, and awareness throughout Sonesta, and initiate plans and programs to maintain information security awareness and risk assessments are performed and reported.

- Educate the team and staff on ongoing legal, regulatory and compliance changes as well as industry news and trends.
- Identify securable resources and help business unit management select appropriate information owners and work with information owners in business units to determine appropriate security policies for securing their resources.
- Identify significant threat changes and vulnerabilities.
- Evaluate information received from monitoring processes.
- Review information security incident information and recommend follow-up actions.
- Provide appropriate enterprise security strategic vision and determine methods of implementing and enforcing security policy.
- Assist executive management in governance, policy creation, identifying roles and responsibilities, risk assessment, education, and communication of the enterprise information security program.
- Report annually, in coordination with the Information Security Officer, to Executive Management on the effectiveness of the Sonesta Information Security Program, including progress of remedial actions.

All Employees, Contractors, and Other Third-Party Personnel

- Understand their responsibilities for complying with the Sonesta Information Security Program.
- Formally sign off and agree to abide by all applicable policies, standards, and guidelines that have been established.
- Use Sonesta **Information Resources** in compliance with all Sonesta Information Security Policies.
- Seek guidance from the Information Security Team for questions or issues related to information security.

Policy

- Sonesta maintains and communicates an Information Security Program consisting of topic-specific policies, standards, procedures and guidelines that: o Serve to protect the Confidentiality, Integrity, and Availability of the **Information Resources** maintained within the organization 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: □ _State breach notification laws,

- PCI Data Security Standard,
- Information Security best practices, including ISO 27001, 27002 and NIST CSF,
- Contractual agreements,
- All other applicable federal and state laws or regulations.

- The information security program is reviewed no less than annually or upon significant changes to the information security environment.

Governance and Program Management

Security Governance is the system by which and organization directs and controls IT security. Security Management is concerned with making decisions to mitigate risks; governance determines who is authorized to make decisions. Governance specifies the accountability framework and provides oversight to ensure that risks are adequately mitigated, while management ensures that controls are implemented to mitigate risks. Management recommends security strategies. Governance ensures that security strategies are aligned with business objectives and consistent with regulations.

Security Governance and Program Management will include key functions such as:

Program Oversight

- Manage and implement a program to ensure the Company is adequately protected against emerging risks and threats and to evaluate future emerging risks and threats.

Strategic and Annual Planning

- Provide vision and leadership of the ISP that adapts to and mitigates current and emerging information security threats, risk, and technologies that can have negative impacts on the fulfillment of corporate goals and objectives.
- Annual planning and budgets.
- Project management to deliver security program initiatives.

Regulatory Assessment and Mapping

- Establish the framework for meeting the applicable regulatory requirements regarding the security of Sonesta information assets.

Policy and Standards

- Oversight and governance of all information security policies, standards, and procedures.
- Provide clear direction towards consistent adherence to policy for information security across Sonesta.
- Provide oversight and governance to the implementation of Company information security policies and practices. The Information Security Policies, Standards, and Procedures shall be reviewed annually or based on need.

- A formal policy management process shall be developed and maintained to provide guidance on drafting, reviewing, approving, publishing, communicating, and maintaining information security policies and standards.

Risk Management and Risk Registers

- A risk management program shall be developed, implemented, and maintained to document and communicate potential risks to an acceptable level.
- Risk assessment shall be performed on a periodic basis and at least annually to identify and quantify risks.
- Risks shall be mitigated to an acceptable level.
- Manage and address changes in the risk environment.
- Report and track risks for the Company.

Compliance Management

- The Company shall be monitored for compliance with policies, standards, and procedures, contractual security obligations, and federal/state legal security requirements.
- Non-compliance shall be identified and remediated according to a process based upon Risk management.

Security Training and Awareness

- Information security training and awareness content development.

Operations

Security Operations are responsible for tactical and security administrative of the infrastructure and defining processes for implementing new policy requirements. Security Operations will include functions such as:

Security Monitoring

- Track remediation activities in accordance with information security policies.
- Develop and maintain an effective monitoring and alerting program sufficient to provide timely, structured, and managed awareness of security threats, incidents, events, and trends.

Security Event and Incident Management

- Providing investigative oversight of information security incidents.
- Security incidents and similar circumvention of security controls, from within or externally sourced, shall be reported, escalated, and remediated following a managed process.
- A Computer Incident Response Team (CIRT) shall be established to address such security incidents.

Vulnerability and Threat Management

- Manage an effective vulnerability management framework to: o Establish an appropriate frequency for detecting vulnerabilities.
    - Detect such vulnerabilities across the enterprise's public services and internal resources.
    - Attribute an appropriate severity rating to the vulnerability.
    - Link the detection capability to the enterprise change, configuration and release management processes.
    - Appropriately address the issues according to their vulnerability.
    - Confirm that remediation activities have lowered the exposure to, or removed in total, the initial vulnerability.
    - Perform ongoing vulnerability management through a continuous improvement lifecycle.
- Manage an effective threat management framework to: o Identify threats that may lead to degradation in performance, or an attack, of an enterprise resource.
    - Evaluate the risk that a threat presents and take appropriate action.
    - Direct the appropriate information about threats to the affected parties so an informed decision can be made.
    - Ultimately have the capability to focus and utilize the security resources where most are needed.

Identity and Access Management

- Authorize appropriate user access to information resources based on their job responsibilities.
- Access privileges are documented, authorized and periodically reviewed as required by policy, procedure, standard, or other regulatory entity.

Operational Security Management

- All critical patches and hot fixes provided by the vendors shall be installed and tested prior to placing the equipment in the production environment and maintained on a regular basis in a production environment.
- Operational security management activities shall be managed by their respective IT operational teams. For example:
    - File Integrity Management (FM) will be managed by Systems Operations.
    - Desktop AV, configuration, encryption server, patch management will be managed by Endpoint Operations.
    - Server AV, configuration, patch management will be managed by Systems Operations.
    - Email SPAM, AV, will be managed by Systems Operations.
    - Network devices, firewalls, and IDS/IPS will be managed by Network Operations.

Legal Hold and eDiscovery

- Lead on IT Legal Hold and eDiscovery process and ensure business requirements are being met as required.

Change Control Management

- Responsible for reviewing proposed changes to IT systems for potential risk as part of the Change Activity Board.

Compliance and Auditing

Sonesta employees may perform administrative and maintenance tasks in accordance with Sonesta's compliance obligations. This includes but is not limited to the security controls required to comply with both Sarbanes-Oxley (SOX) and Payment Card Industry (PCI) compliance.

These controls are tested regularly and may be modified as a result of the tests. Failure to follow the controls as documented, either deliberately or through failure to follow supplied procedures, is a violation of this policy.

For all Sonesta IT Audit failures, a findings letter will be written and sent to the manager of the employee responsible for the failed control. These letters require written remediation plans to address the failed control.

Continued failure to follow Sonesta's required IT General Controls may result in disciplinary action including possible employment termination.

Assessment and Monitoring

Assessment and Monitoring will include functions such as:

Security Testing Assessments

- Define testing requirements
- Manage and conduct security testing and remediation.

Third Party Vendor Assessments and Monitoring

- Controls shall be documented to implement and maintain information security and service delivery, consistent with this policy and existing Company security policy.
- These controls shall be specified in applicable Vendor outsourced service delivery agreements.
- Appropriate due diligence shall be conducted on all Vendors prior to entering into any new engagement.
- Controls shall be applied to implantation of agreements, monitoring compliance with the agreements and manage changes to ensure that the Services delivered are consistent with the relevant vendor service provider agreement, this policy, and existing Company security policy.
- All controls shall be specified in any vendor outsourced service delivery agreements.
- A formal process shall be documented for the selection, purchase, implementation, and ownership of vendor Services.

Policy Exception Tracing and Reporting

- An exception process shall be documented and managed to ensure security exceptions are identified, assessed for risk to the Company, remediated, and tracked.

Program Benchmarking

- Conduct periodic benchmarking to assess maturity level of security and compare to peers.
- Manage improvement.

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 Sonesta 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	February 12, 2021			Document Origination
1.1.0		March 29, 2022	Michael Woodson, Director Security & Privacy	Annual review; no changes
1.1.2		February 14, 2023	Carrie Reid, Manager IT Audit & Compliance	Annual review; no changes