Information Security Policy Extract

Public
Extract Version 1.0 (EV1.0)

Revision History

Version	Date	Author	Changes

1. Overview & Purpose

1. Introduction

Seaborn and its subsidiaries maintain a comprehensive Information Security Program designed to safeguard our data and technology assets across back-office and operational environments ("**DIT Assets**"). Built on a "security by design" approach, the program is based on Seaborn's Information Security Policy ("**ISP**") and related documents.

The ISP applies to all employees and independent consultants and aligns with recognized frameworks (e.g., NIST CSF and ISO/IEC 27001) while addressing applicable data protection and telecommunications regulations in the United States and Brazil, including the Brazil LGPD and relevant FCC and ANATEL rules.

This Information Security Policy Extract ("**Extract**") provides key information on Seaborn's information security and cybersecurity practices in order to foster trust between Seaborn and its clients.

Seaborn may update the ISP and this Extract to reflect changes in practices and legal requirements.

2. Objective

The objective of the Information Security Policy is to define the principles and controls that govern information security and cybersecurity across Seaborn's operations. It establishes measures to safeguard our DIT Assets by preserving the confidentiality, integrity and availability of information, embeds a security-by-design approach with continual improvement, and sets processes and responsibilities to identify, assess and respond to information security incidents and risks. The Policy supports compliance with applicable data protection laws—including Brazil's LGPD—and relevant telecommunications obligations, including FCC and ANATEL regulations.

3. Applicability

The ISP applies to all Seaborn employees (including Seaborn's Affiliates) and to all contracted independent consultants, who are expected to read, understand and comply with the ISP and to report actual or suspected violations through Seaborn's established channels. The Policy also applies to all Seaborn DIT Assets across operational and corporate environments.

4. References

- NIST Cybersecurity Framework 2.0 (NIST CSF).
- ABNT NBR ISO/IEC 27001:2022 — Information Security Management Systems (ISMS).
- Brazil's General Data Protection Law (LGPD).
- ANATEL Resolution No. 740/2020, as amended by Resolution No. 767/2024.
- U.S. Federal Communications Commission rules relating to the Cable Landing License Act.
- NIST Special Publication 800-88 Revision 1 — Guidelines for Media Sanitization.

The ISP may be updated to reflect changes in these sources and in applicable legal or regulatory requirements.

5. Responsibilities

Seaborn's Enterprise Risk Management Committee ("**ERMC**") oversees the Information Security Program, setting and maintaining policies, coordinating risk identification and assessment, ensuring appropriate controls and audits, and governing vendor and supply-chain security.

The Information Security Incident Response Team ("**ISIR**") coordinates the preparation for and handling of incidents, including assessment, remediation and stakeholder communications in line with legal and regulatory duties.

Employees must know and follow the ISP, protect Seaborn DIT Assets, keep credentials secure, use only authorized tools, and promptly report suspected or actual incidents and weaknesses; Independent Consultants have parallel obligations when engaged by Seaborn. All employees are legally bound to abide by the ISP.

Data Protection Officers ("**DPOs**") act as the communication channel with data subjects and authorities and guide compliance with applicable data protection laws.

Global/USA DPO: Lin Gentemann

DPO Brazil: Maria Beatriz M. de Miranda Tello.

6. Contact

For urgent matters relating to regulatory compliance, please contact: ISP@seabornnetworks.com.

Suspected information security incidents must be reported to: incident@seabornnetworks.com.

7. Training and Awareness

Seaborn conducts mandatory information security and data protection training for all employees and independent consultants, with additional modules for roles that require deeper technical or legal knowledge. Training may be delivered in person or online and addresses the importance of security, applicable privacy and telecom requirements, common threats (including phishing and social engineering), the responsibilities of each individual, among others. Training is held on a recurring basis and completion records may be provided to authorities when required.

8. Security Incident Notification

Seaborn's ISIR coordinates notifications to internal and external stakeholders when an Incident is identified, in accordance with applicable data protection and telecommunications laws. The ISIR Team works with the ERMC, Legal and the Brazil Privacy Team to ensure timely reporting to authorities and other parties as required by data protection and telecommunications laws, and maintains an incident log. Employees and independent consultants must promptly report suspected incidents through the established channels and must not disclose incident information to third parties unless authorized.

9. Key Information on Security Processes

Seaborn's ISP provides for information security processes and procedures for ensuring DIT Assets are duly protected. They include, without limitation:

- **Employee & Independent Consultant Compliance.** Lifecycle procedures for personnel onboarding, role changes and terminations, including screening as applicable. Ensures access is aligned to role changes and removed at exit.

- **Acceptable Use of DIT Assets.** Acceptable-use requirements for company IT assets, including compliance with law and licensing and prohibitions on misuse. Establishes norms for responsible use of email and other electronic communications.
- **Asset Classification and Organization.** Procedures on how information and technology assets are identified, classified and organized across the company. Supports consistent protection throughout the data/asset lifecycle.
- **Data Types & Confidentiality Levels.** Classification of data categories such as Confidential Data, Personal Data and Public Data, with handling expectations at a high level.
- **Roles & Responsibilities for IT Asset and Data Ownership.** Definitions on Data Owners and Data Groups to clarify ownership responsibilities (classification, retention/availability expectations, and related governance).
- **Record of Processing Activities (ROPA).** Requires maintaining a Brazil LGPD-compliant ROPA and maintaining current data-flow and network diagrams.
- **Information Access Controls.** Implements least-privilege/role-based access, documented approvals for access to sensitive data, periodic access reviews, and auditability of changes.
- **Data Collection, Handling and Transmission.** Requires data minimization, collection from reliable sources, careful handling and limited transmission of confidential/personal data, with encryption when transmitted electronically. Encourages secure channels and secure voice practices when needed.
- **Data Loss Prevention**. Establishes technical and procedural controls to prevent and detect data exfiltration (e.g., device/media protections and monitoring).
- **E-mail Policy.** Defines email-sender authenticity and internal email-use rules to reduce spoofing and misuse.
- **Web Filtering.** Defines web-filtering controls to restrict access to unsafe or inappropriate sites and reduce malware risk.
- **Passwords.** Establishes password/passphrase construction and protection practices and discourages reuse or sharing. Emphasizes that systems should be locked when unattended.
- **Configuration Management.** Establishes change-management and interconnection procedures so that changes are authorized, tested and auditable.
- **Network Security**. Requires perimeter protection, segregation of guest wireless, and strong authentication for any internal wireless access.
- **Asset Management.** Requires identification, classification and inventory of DIT assets, including those hosted by third parties.
- **Logging and Monitoring.** Requires maintaining and reviewing audit logs of user activities, exceptions and security events.
- **Unauthorized Hardware/Software (Shadow IT)**. Prohibits installing or using unapproved software or hardware and requires centralized approval for software requests and license acceptance.
- **Alert Response.** Defines the process to triage and respond to security alerts and escalate to incident handling where appropriate.

- **Security Audit and Network Testing.** Provides for periodic security audits, vulnerability scanning and penetration testing; also for monitoring to detect malicious activity and for remediation follow-up.
- **Brazil Data Subject Personal Data Risk Management & Privacy by Design.** Establishes risk assessment for processing Brazil personal data and articulates privacy-by-design expectations in projects and operations.
- **Hosted/Cloud IT Assets.** Sets baseline controls for cloud-hosted services (e.g., logging/monitoring, least privilege, multi-factor authentication, data protection, hardening, patching, vulnerability assessment).
- **Mobile Device and Laptop Protection.** Requires device inventory, mobile-device management enrollment, full-disk encryption, inactivity locks and related endpoint safeguards.
- **Workstation Protections.** Requires endpoint protections on corporate workstations, prohibits use of personal devices for company work, and mandates patching and malware defenses.
- **Patching.** Defines the process to apply security and stability patches to systems and applications in a timely, controlled manner.
- **Physical Security.** Establishes requirements for physical access control to facilities and points-of-presence, including visitor procedures and restricted areas.
- **Travel Security.** Establishes travel-security expectations and references the travel-notice procedure for international trips.
- **Data Subject Requests.** Requires any received Data Subject request to be immediately forwarded to the DPO; employees must not respond directly.
- **Acceptable Use of Generative AI Tools**. Prohibits using company data with public GenAI tools without prior written approval and sets do's/don'ts for safe use; reinforces that GenAI outputs must be verified and not treated as private.

10. Control and Monitoring

- **Governance & internal controls.** The ERMC establishes, oversees, and continually improves security controls, coordinating testing, audits, remediation, and compliance monitoring across risk and technology functions. It also organizes supporting teams and provides updates and recommendations to senior leadership.
- **Logging & monitoring.** The ERMC maintains audit logs of user activities, exceptions, and security events across DIT Assets, capturing items such as authentication activity, timestamps, source/location, asset/data access, use of elevated privileges, and relevant network parameters. Logs and reports for perimeter-facing assets are reviewed periodically to detect suspicious activity (e.g., unusual access, dormant accounts, unauthorized login attempts).
- **Access reviews & change traceability**. Access to confidential/personal data follows least-privilege with documented approvals; privileged access requires heightened authorization. Periodic access reviews are performed, and access changes must be auditable and reported through the change-management process.
- **Alert triage & escalation**. Security alerts from protective controls are triaged and, when warranted, escalated to incident handling. The process considers potential intrusions and impacts on IT assets, data, personnel, customers, and vendors.

Security audits, risk assessment & network testing. The ERMC conducts security risk assessments and audits of DIT assets using defined criteria to evaluate threats, vulnerabilities, and the sufficiency of controls, applying risk treatment (reduce, retain, avoid, transfer, monitor) and driving improvements to the IS Program. The ERMC also performs network testing (including internal/external scans), verifies remediation of past breaches, and uses results for process enhancement.

11. Key definitions

Capitalized terms used in this IS Policy have the meaning set forth below unless otherwise defined under applicable data protection law.

Term	Definition
DIT Assets	All data, systems, networks, applications, equipment, infrastructure, and technological resources used by Seaborn in its corporate and operational environments.
Information Security Policy (ISP)	Seaborn's comprehensive policy that defines the principles, controls, and procedures governing information and cybersecurity management to preserve the confidentiality, integrity, and availability of DIT Assets.
Enterprise Risk Management Committee (ERMC)	The governing body responsible for overseeing Seaborn's Information Security Program, including policy definition, risk identification and mitigation, auditing, and supply-chain security.
Information Security Incident Response Team (ISIR)	The team in charge of preparing for and responding to information security incidents, including incident assessment, remediation, communication, and regulatory notifications.
Data Protection Officer (DPO)	The designated individual responsible for ensuring compliance with applicable data-protection laws, serving as the point of contact with data subjects and supervisory authorities, and guiding privacy-related practices.
Confidential Data / Personal Data / Public Data	Information-classification categories that define handling, storage, and transmission requirements according to confidentiality and sensitivity levels.
Record of Processing Activities (ROPA)	A register required under Brazil's LGPD that documents the processing of personal data, including purposes, legal bases, data categories, sharing, and applied security measures.
Incident	Any event that compromises, or has the potential to compromise, the confidentiality, integrity, or availability of

Term	Definition
	Seaborn's information or DIT Assets, including unauthorized access, data leakage, malware infection, or operational failure.