# Information Security Policy

Updated: May 2026

This document was approved by Hudson Shipping Lines' Board of Directors and is publicly available on our website. All employees are informed about the contents of this document.

# Information Security Policy

## 1. Purpose and Commitment

This Information Security Policy (the "Policy") establishes the minimum governance, administrative, technical and physical safeguards required to protect information and information systems used by Hudson Shipping Lines Incorporated, its branches and its wholly owned subsidiaries (collectively, the "Company" or "Hudson").

Hudson depends on accurate, available and confidential information to conduct shipping, logistics, procurement, finance, legal, commercial and administrative activities. The Company is committed to protecting Company Data, customer and supplier information, employee information, trade secrets, business records, systems and networks from unauthorized access, loss, misuse, alteration, disclosure or disruption.

This Policy is intended to be practical and risk based. It provides a common standard for Users, management and service providers, while permitting more detailed procedures, technical standards and site specific controls to be adopted as needed.

## 2. Scope

This Policy applies to all full time, part-time and temporary employees, officers and directors of the Company, and to agents, representatives, consultants, advisors, contractors, temporary workers, outsourced service providers and other third parties who access, process, transmit, store or support Company Data or Company systems (collectively, "Users").

This Policy applies to all Company Data and Information Assets, regardless of format, location or owner of the device or system on which the information resides. This includes paper records, email, messaging systems, laptops, mobile devices, servers, cloud applications, collaboration platforms, removable media, backups, network equipment, operational technology and any system used to conduct Company business.

This Policy should be read together with the Company's Code of Conduct and Ethics, privacy notices, records retention requirements and any other Company policies, procedures or contractual commitments applicable to information security or data protection.

## 3. Definitions

**Company Data:** all information created, received, transmitted, stored, maintained or processed by or for the Company, whether in electronic, paper, verbal or other form.

**Confidential Information:** Company Data that is not public and that could harm the Company, its employees, customers, suppliers or business partners if disclosed or used without authorization.

**Information Assets:** Company systems, networks, applications, devices, databases, records, data repositories, cloud services, accounts, credentials, encryption keys and other assets used to process, store or transmit Company Data.

**Personal Information:** information relating to an identified or identifiable individual, including employee, customer, vendor, contact, visitor or other personal data protected by applicable law.

**Security Incident:** any actual or suspected event that compromises, or may compromise, the confidentiality, integrity or availability of Company Data or Information Assets.

**Privileged Access:** administrator, root, service account or other elevated access that permits a User to configure systems, bypass controls, access sensitive data or grant access to others.

**Operational Technology or OT:** hardware or software that monitors or controls physical equipment, vessel systems, terminal interfaces, logistics equipment, communications, navigation, cargo handling, sensors or other operational processes.

## 4. Governance and Responsibilities

Information security is a shared responsibility. The Company will assign reasonable governance, oversight and operational responsibilities based on the Company's size, systems, risk profile and available resources.

### 4.1 Board of Directors

The Board of Directors provides oversight of material information security and cyber risk matters, approves this Policy, receives periodic updates concerning material security risks and incidents, and supports allocation of reasonable resources for the Company's information security program.

### 4.2 Executive Management

Executive management is responsible for implementing this Policy, promoting a culture of security, assigning responsible personnel, supporting remediation of material risks and ensuring that business decisions appropriately consider information security, operational continuity and legal compliance.

### 4.3 Information Security Lead

The Chief Information Security Officer, if appointed, or the senior IT leader or other person designated by executive management (the "Information Security Lead") is responsible for coordinating the Company's information security program. The Information Security Lead will work with management, Legal, Human Resources, Finance, Operations and external providers as appropriate.

### 4.4 Legal Department

The Legal Department supports the Company's response to legal, regulatory, contractual and notification issues arising from information security matters, including incident response, preservation of privilege, third-party contract requirements, privacy obligations and regulatory communications.

### 4.5 Users

All Users must comply with this Policy, protect Company Data and Information Assets, complete required training, use good judgment, report suspected Security Incidents promptly and cooperate with investigations, audits and remediation activities.

### 4.6 Third Parties

Third parties that access Company Data or Information Assets must comply with applicable Company security requirements, contractual obligations and laws. Third parties may be required to complete security due diligence, enter into confidentiality and data protection commitments, maintain appropriate controls and promptly report suspected Security Incidents involving Company Data or systems.

## 5. Security Standards and Reference Frameworks

This Policy is designed to support a reasonable, risk based information security program and to align, where appropriate, with recognized security frameworks and guidance, including the NIST Cybersecurity Framework 2.0, ISO/IEC 27001 and ISO/IEC 27002, CISA Cross-Sector Cybersecurity Performance Goals and, where applicable to vessel or maritime operations, IMO guidance on maritime cyber risk management. These references do not create a certification obligation unless expressly approved by the Company.

The Company will consider applicable law, contractual commitments, customer expectations, operational risk, business criticality, cost, technical feasibility and threat environment when determining appropriate safeguards.

## 6. Information Classification and Handling

Company Data must be protected according to its sensitivity, business value, legal requirements and risk of harm from unauthorized disclosure, alteration or loss. Users must only access, use, share, copy, download, print or retain Company Data for legitimate business purposes.

- Public: information approved for public release, such as published website content or marketing materials. Public information may be shared externally after appropriate approval;
- Internal: business information intended for use within the Company or by approved service providers. Internal information should not be posted publicly or shared outside the Company without a business need;

- Confidential: non-public business, financial, legal, commercial, customer, supplier, personnel, technical, vessel, operational or strategic information. Confidential information must be shared only with authorized persons who have a business need to know;
- Restricted: highly sensitive information such as credentials, encryption keys, sensitive Personal Information, privileged legal materials, incident response materials, bank instructions, payment controls, trade secrets, acquisition materials or security architecture. Restricted information requires heightened controls and limited access.

Users must label or otherwise identify Confidential or Restricted information when doing so is practical and beneficial. Lack of a label does not mean information is public or may be shared without authorization.

Confidential and Restricted information must be transmitted using Company approved channels. Users may not forward Company Data to personal email accounts, personal cloud storage, personal messaging applications or unapproved file sharing services, except as specifically approved by the Information Security Lead or Legal Department.

## 7. Acceptable Use of Systems and Devices

Company systems, networks, devices, accounts and communication tools are provided for authorized business purposes. Limited personal use may be permitted if it is reasonable, lawful, does not interfere with work, does not create security risk and does not violate Company policies.

Users must not:

- use Company systems for unlawful, fraudulent, harassing, discriminatory, offensive or unauthorized activities;
- install unauthorized software, browser extensions, remote access tools or applications on Company systems;
- disable, bypass or interfere with security controls, logging, encryption, endpoint protection, access controls or monitoring tools;
- connect unauthorized equipment to Company networks or systems;
- use unauthorized peer-to-peer file sharing, cryptocurrency mining, offensive security tools or anonymizing services;
- copy, download or retain Company Data after their business need or relationship with the Company ends;
- attempt to access information or systems for which they have not been authorized.

The Company may restrict, suspend or revoke access to systems or data when required to protect the Company, comply with law, investigate misconduct, preserve evidence or maintain operations.

## 8. Identity, Access Control and Authentication

Access to Company Data and Information Assets must be based on least privilege, business need and appropriate approval. Access rights must be granted, changed and removed in a timely manner based on job responsibilities, contract status and risk.

The Company will maintain processes for onboarding, transfers, terminations and periodic access reviews for material systems. Access to sensitive systems, financial systems, cloud administration, email administration, security tools and Restricted information must receive heightened review.

Users must protect passwords, passphrases, tokens, authentication devices and recovery codes. Passwords must not be shared, reused across personal and Company accounts, stored in unapproved locations or transmitted in plain text. Multi-factor authentication must be used for remote access, email, cloud services, financial systems, privileged accounts and other high risk systems where available and practical.

Privileged Access must be limited to authorized personnel, used only when required, monitored where practical and removed promptly when no longer needed. Shared administrator accounts should be avoided unless technically necessary and approved with compensating controls.

## 9. Endpoint, Mobile Device and Remote Work Security

Company laptops, desktops, mobile devices and other endpoints must be configured and maintained with reasonable security controls, including approved operating systems, endpoint protection, screen locks, patching, encryption where appropriate and remote wipe or disablement capabilities where supported.

Users must take reasonable steps to physically protect devices and prevent unauthorized viewing or use. Devices must not be left unattended in public places or vehicles unless reasonably secured. Loss, theft or suspected compromise of any device containing or accessing Company Data must be reported immediately.

Remote work must be conducted using Company approved systems and secure connections. Public Wi-Fi should be avoided when practical and must not be used for sensitive work unless protected through Company approved safeguards. Company Data should not be printed, stored or discussed in locations where it may be observed or overheard by unauthorized persons.

Personal devices may access Company Data only if authorized and configured with required security controls. The Company may condition access on device management, screen lock, encryption, endpoint protection, separation of Company Data and the ability to remove Company Data from the device.

## 10. Network, Email, Cloud and Communications Security

Company networks and communications systems must be designed and operated to reduce unauthorized access, prevent avoidable exposure, support business continuity and protect Company Data. The Company will use reasonable controls for firewalls, secure configurations, network segmentation, wireless security, email filtering, domain protection, malware protection and secure remote access based on risk.

Email, messaging and collaboration tools are common sources of phishing, fraud, credential theft and payment redirection schemes. Users must exercise caution before opening attachments, clicking links, approving sign-in prompts, changing payment instructions, wiring funds, sharing credentials or responding to unusual requests.

Cloud services used to store, process or transmit Company Data must be approved by the Company. Users may not create or use unapproved cloud services for Company business. The Company will maintain reasonable administrative controls over approved cloud services, including access management, logging, data retention and vendor oversight where practical.

## 11. Data Retention, Backup and Secure Disposal

Company Data must be retained, archived and disposed of in accordance with applicable legal, regulatory, contractual and business requirements and the Company's records retention practices. Users must not delete, alter or destroy information that is subject to a litigation hold, investigation hold, audit request, regulatory request or instruction from the Legal Department.

Critical Company systems and data repositories should be backed up on a schedule appropriate to their business importance. Backups should be protected from unauthorized access, tested periodically where practical and maintained in a manner designed to support recovery from ransomware, accidental deletion, system failure or other disruption.

Devices, storage media, paper records and other materials containing Confidential or Restricted information must be securely erased, destroyed or disposed of using Company approved methods when no longer needed.

## 12. Secure Configuration, Patch and Vulnerability Management

The Company will maintain reasonable processes to identify and remediate vulnerabilities in Company systems based on severity, exploitability, business criticality and operational constraints. Security updates and patches should be applied in a timely manner, with emergency remediation for actively exploited or critical vulnerabilities when appropriate.

Material changes to systems, applications, networks, security settings, access controls or third-party integrations should be reviewed, approved, tested and documented commensurate with risk. Default passwords must be changed,

unnecessary services should be disabled and systems should be configured using secure baseline settings where practical.

Security testing, penetration testing, vulnerability scanning or similar activity may be performed only by authorized personnel or approved third parties and must be coordinated to avoid unnecessary disruption to Company operations.

## 13. Physical and Environmental Security

Company offices, file areas, network closets, server rooms and other locations containing Company Data or Information Assets must be protected by reasonable physical safeguards. Access to areas containing sensitive records or systems should be limited to authorized personnel.

Visitors should be managed in accordance with local site procedures. Users must not permit unauthorized persons to access Company offices, equipment, records or systems. Sensitive documents should be secured when unattended and disposed of using secure shredding or other approved methods.

Where applicable, environmental controls, power protection, fire protection and other safeguards should be maintained for critical systems and equipment.

## 14. Third-Party and Supplier Security

Third-party relationships can create information security, privacy, operational and reputational risk. Before granting a third party access to Company Data, Company systems or material business processes, the responsible business owner should consider the type of access, sensitivity of information, business criticality, location of processing, subcontractors, prior performance and security controls.

Contracts with material third parties that access Confidential or Restricted information or support critical systems should include appropriate confidentiality, data protection, security, access control, incident reporting, audit or assessment, subcontractor, return or destruction and termination provisions, as applicable.

Third-party access must be limited to the business purpose for which it was granted and removed promptly when no longer required. The Company may require third parties to provide security questionnaires, certifications, audit reports, evidence of insurance, incident notices or remediation plans where appropriate.

## 15. Maritime, Vessel and Operational Technology Security

Where the Company owns, operates, manages, supports or has direct access to vessel, terminal, logistics, communications or other Operational Technology systems, cyber risk management must be integrated with safety, security and operational risk management. The Company will consider applicable maritime cyber risk guidance and contractual or flag state requirements where relevant.

OT systems should be protected from unnecessary exposure to the internet and corporate networks. Remote access to OT systems should be approved, authenticated, limited, logged where practical and disabled when no longer needed. Changes to OT systems should be coordinated with operational personnel to avoid safety, navigation, cargo handling or business continuity impacts.

Users must promptly report suspicious activity affecting vessel, port, cargo, logistics or communications systems, including suspected GPS spoofing, navigation anomalies, unauthorized remote access, ransomware, malware, unexplained system changes or vendor compromise.

## 16. Privacy, Confidentiality and Legal Compliance

The Company will handle Personal Information and Confidential Information in accordance with applicable law, contractual commitments and Company policies. Users may collect, use, disclose and retain Personal Information only for authorized business purposes and only to the extent reasonably necessary for those purposes.

Users must notify the Legal Department before responding to regulatory inquiries, law enforcement requests, subpoenas, data subject requests, customer security questionnaires that request legal commitments, requests for incident details or requests to disclose sensitive Company information.

Nothing in this Policy is intended to prevent a User from reporting possible violations of law to a governmental authority or participating in proceedings protected by law. Users should not disclose privileged Company communications or trade secrets except as permitted by law or authorized by the Legal Department.

## 17. Security Awareness and Training

The Company will provide information security awareness and training appropriate to Users' roles and access. Training may include phishing, password security, multi-factor authentication, fraud prevention, payment instruction verification, data handling, remote work, incident reporting, privacy and role specific security obligations.

Users with privileged access, financial authority, legal duties, human resources responsibilities, IT responsibilities or access to Restricted information may be required to complete additional training or acknowledgments.

## 18. Security Incident Reporting and Response

Users must immediately report any actual or suspected Security Incident to the Information Security Lead, IT, Legal Department or their supervisor. Reports may be submitted by email to InfoSecurity@hudsonshipping.com or through any other reporting channel designated by the Company.

Security Incidents may include, without limitation:

- lost or stolen devices, files, documents or credentials;
- suspected phishing, business email compromise, ransomware, malware or unauthorized access;
- misdirected emails or unauthorized disclosure of Company Data;
- unusual payment instruction requests or suspected fraud;
- system outages, data corruption, unauthorized changes or suspected data exfiltration;
- security incidents involving vendors, cloud providers or other third parties;
- events affecting vessel, cargo, logistics, port, communication or operational systems.

Users must not investigate suspected Security Incidents beyond basic preservation and reporting unless authorized. Users must not delete evidence, wipe devices, communicate with threat actors, pay ransom, contact regulators, notify customers, communicate with media or make external statements about a Security Incident without approval from the Legal Department and executive management, except as required to protect life, safety or property in an emergency.

The Company will maintain an incident response process designed to identify, contain, investigate, remediate and recover from Security Incidents and to determine whether legal, contractual, insurance, customer or regulatory notifications are required.

## 19. Monitoring, Audit and Compliance

To the extent permitted by applicable law, the Company may monitor, access, review, preserve and disclose activity, communications, data, files, logs, devices and accounts on or connected to Company systems for legitimate business purposes, including security, operations, compliance, investigations, legal obligations, audit, preservation of evidence and protection of Company interests.

Users should have no expectation of privacy when using Company systems or Company accounts, except as required by applicable law. Monitoring will be conducted in a manner intended to be lawful, proportionate and consistent with legitimate business purposes.

The Company may conduct internal or third-party assessments, audits, access reviews, tabletop exercises, vulnerability reviews, compliance testing and other activities to evaluate and improve information security controls.

## 20. Exceptions

Exceptions to this Policy must be approved in writing by the Information Security Lead or executive management, and by the Legal Department when the exception may create legal, privacy, contractual, regulatory or material business risk. Exceptions should be documented, time limited where appropriate and supported by compensating controls when feasible.

## 21. Violations and Discipline

Violations of this Policy may result in disciplinary action, up to and including termination of employment or engagement, termination of system access, termination of contracts, civil action, referral to law enforcement or other remedial measures. The appropriate response will depend on the facts and circumstances, applicable law, contractual rights and Company policy.

The Company prohibits retaliation against any person who, in good faith, reports a suspected Security Incident or violation of this Policy or cooperates in an investigation.

## 22. Policy Review

This Policy shall be reviewed by Hudson's Board of Directors and Corporate Social Responsibility team in full on an annual basis. More frequent reviews will take place in response to organizational, operational, technological, legal or regulatory changes, material Security Incidents or changes in the Company's risk profile. Management will communicate approved material changes as appropriate after implementation.

Next scheduled review: May 2027

## 23. Acknowledgements

Read and approved by:

Board of Directors

Hudson Shipping Lines Incorporated

May 2026

_____

[Date: ]

Read and Approved

Employee [Name: ]

This Policy may be amended from time to time with or without notice by the Company.