भारत सरकार/ GOVERNMENT OF INDIA
पत्तन,पोत परिवहन और जलमार्ग मंत्रालय /
MINISTRY OF PORTS, SHIPPING AND WATERWAYS
नौवहन महानिदेशालय, मुंबई
DIRECTORATE GENERAL OF SHIPPING, MUMBAI

File no. 11-33/12/20245-COMP-DGS **Dated: 05.05.2025**

OFFICE MEMORANDUM

Cybersecurity and data protection have become integral for any organization's operations in the ever-evolving cybersecurity threat landscape. This memorandum formally establishes the scope of authority, functional responsibilities of the Chief Information Security Officer (CISO), including the mandatory compliance procedures and Standard Operating Procedures (SOPs) that all departments must implement to maintain alignment with organizational requirements.

1. Role and Responsibilities of the CISO

- The CISO organization will establish a DGS cybersecurity strategy and governance framework.
- Report cybersecurity posture, incidents, and risk exposures to executive leadership and the board.
- Developing and maintaining policies, procedures, SOP's for information security and data protection in line with standards, framework and regulatory guidelines.
- Perform regular risk assessments, define risk mitigation strategies, and conduct periodic audits to identify vulnerabilities and recommend mitigations.
- Responsible for overseeing the implementation and maintenance of security tools, infrastructure, and controls to protect data and systems.
- Design and periodically update the incident response and recovery plan (IRP). Coordinate IRP in the event of cybersecurity breaches. Ensure timely and effective recovery and root-cause analysis to prevent recurrence.
- Ensure compliance with applicable legal, regulatory, and contractual cybersecurity requirements.

- Define, assess, implement and monitor the cybersecurity posture of vendors and partners.
- Promote a cyber-safe environment through training and awareness programs for all staff, fostering a security-conscious culture.
- Liaison with external cybersecurity agencies, auditors, and stakeholders as needed.
- Work with stakeholders to design and implement a whistleblower policy for the Information Security program.

2. Compliance with Cybersecurity and Data Standards

All departments and field establishments are required to adhere to the following:

a. Security Policy Adherence

- Review and comply with the organization's Information Security Policy as published on CERT-IN
- It is expected that employees are aware of and understand their responsibilities to cybersecurity.
- Train staff, encrypt transmissions, implement audit logs.

b. Data Ownership, Handling, and Classification

- Each department is accountable for the ownership, integrity, and protection of the data it generates, accesses, or manages, and that should be under defined policies
- Each department and individual is expected to handle sensitive, confidential, and personal data under classification guidelines.
- Avoid unauthorized storage, sharing, or transmission of protected data. Any transmission of data outside of DGS network should be in line with business alignment and requirements.

c. User Access Management

- Access to each resource should be based on the principle of least privilege.
- Ensure timely provisioning and de-provisioning of user access to files, folders, applications, networks, and systems.
- The organization must ensure that default login credentials of devices such as routers, firewall, storage equipment etc., are changed prior to the deployment of such devices in the operational environment

- Implement Geo-fencing for restricting remote access from unauthorized geolocations.
- Temporary and third-party access must be time-bound and monitored.

d. Endpoint and Network Security

- Ensure antivirus, anti-malware, and endpoint protection systems are updated and functional.
- Connect only authorized devices to the organizational network.
- Network administration team of the organization shall periodically review network configuration at least every 6 months or as and when new access controls are introduced in the network.
- IDS/IPS systems must be deployed to detect and respond to threats in real time.

e. Incident Reporting and Response

- Report any cybersecurity incidents, suspicious activity, or data breaches immediately to the Information Security Team.
- Cooperate with the investigation and remediation efforts.

f. Data Backup

- Each department is responsible for ensuring that critical data is regularly backed up per data retention and recovery policies.
- Backups must be securely stored and periodically tested to ensure data integrity and availability during incidents.
- Conduct periodic reviews and performance assessments of both Data Centre (DC) and Disaster Recovery (DR) infrastructure to ensure alignment with operational requirements, compliance mandates, and business continuity objectives.

g. SOPs for Compliance

- All concerned must refer to the guidelines as shared by CISO organization, which outline:
    - Daily, weekly, and monthly compliance checks.
    - Procedures for patch management and vulnerability remediation.
    - Guidelines for safe internet and email usage.
    - Templates for incident reporting and log maintenance.

h. Security Standardization and Certification

- The organization adheres to recognized cybersecurity standards and maintains appropriate certifications as part of its commitment to information security, compliance, and continual improvement.
- Internal audits shall be conducted at regular intervals (minimum annually) to ensure compliance with adopted standards and prepare for external certification audits.
- The organization shall ensure third-party service providers conform to equivalent security standards and require them to demonstrate such compliance upon request.
- All critical systems must undergo annual security audits by CERT-In empanelled agencies. The department shall pursue formal ISO 27001 certification for its core IT infrastructure, including applications handling seafarer data, ship registration, and licensing portals.

3. Training and Awareness

Mandatory cybersecurity training sessions will be scheduled periodically. Attendance and completion of assessments will be tracked.

Cybersecurity training must be conducted every 6 months, and completion must be recorded in annual performance reports.

Action Required:

1. Disseminate this memorandum to all staff.
2. Ensure strict compliance with outlined SOPs and standards.
3. Designate a point-of-contact for coordination with the CISO's office.

All aforementioned aspects shall be ensured by the CISO who by definition shall be the DDG IT & e-Governance.

The DDG IT & e-Governance shall be assisted by the following officials:

1. Asst DG IT & e-Governance
2. Tier 1 IT & e-Governance for consultancy services
3. Asst/UDC handling the said matter
4. Technical resources (M/S A3S Tech & Co) for technical support for the CISO functioning

All officials shall be subject to the Superintendence and specific Technical Compliance instructions of the CISO to ensure compliance with the aforementioned cybersecurity and data security norms/standards.

This issues with the approval of the Director General of Shipping, Mumbai

5/May/25

(Deependra Singh Bisen)
Dy. Director General of Shipping,
Directorate General of Shipping, Mumbai