Minimum Information Security Requirements for Third Parties

Version: 1.0
2025

Purpose

This document defines the minimum information security requirements that all third-party entities (including vendors, contractors, consultants, and service providers) must comply with when engaged with Sohar Industrial Port Group ("SIP Group"). These requirements apply only to the areas relevant to the scope of services provided by the third party, especially where access to SIP Group's information systems, networks, or data is involved.

1. Governance and Accountability

- Third parties shall implement an information security program aligned with industry standards, applicable regulations, and SIP Group's Information Security Policy.
- A designated person within the third-party organization must be accountable for ensuring compliance with SIP Group's security requirements.
- Where required, security obligations shall be documented in contractual agreements.

2. Data Protection and Privacy

- Third parties must protect SIP Group data against unauthorized access, modification, disclosure, or destruction.
- Personally Identifiable Information (PII) must be handled in accordance with Omani data protection laws and SIP Group privacy practices.
- Data shall be collected, processed, and retained only as necessary for the agreed purpose and securely destroyed after the retention period or contract termination.

3. Access Control

- Access to SIP Group systems and data must follow the principle of least privilege and be based on business need.
- All users must have unique credentials; password standards and multi-factor authentication must be enforced.
- Terminated or transferred personnel must have their access revoked promptly.

4. Network and System Security

- Third parties must maintain secure configurations of systems and protect networks through firewalls, antivirus, and intrusion detection systems.
- Remote access to SIP Group systems must be via approved secure channels with appropriate re-authentication and session timeout controls.
- Any device connecting to SIP Group's infrastructure must meet its endpoint protection standards.

5. Security Monitoring and Incident Response

- Third parties must monitor their environment for security threats and respond to incidents in a timely manner.
- Any actual or suspected security incidents involving SIP Group data or systems must be reported immediately to SIP Group IT.
- An incident response procedure should be documented and tested regularly.

6. Business Continuity and Disaster Recovery

- Appropriate business continuity and disaster recovery plans must be established and maintained by the third party.
- These plans should be tested periodically and support recovery of systems and data involved in delivering services to SIP Group.

7. Physical and Environmental Security

- Physical access to information processing facilities must be restricted to authorized personnel.
- Facilities, servers, and devices used in handling SIP Group data must be protected from environmental hazards and unauthorized access.

8. Use of Mobile and Personal Devices

- Use of personal or unmanaged devices to access SIP Group resources is prohibited unless explicitly authorized.
- Mobile devices must be encrypted, password-protected, and kept up to date with the latest patches and antivirus software.

9. Change and Configuration Management

- All system changes must follow a structured and documented change management process.
- Configuration changes affecting SIP Group’s services or infrastructure must be reviewed for impact and authorized.

10. Training and Awareness

- Third-party personnel must be trained on information security responsibilities and data protection awareness relevant to their role.
- Use of personal email accounts or communication tools for SIP Group business is strictly prohibited.

11. Use of Artificial Intelligence (If Applicable)

- AI systems must not be used to process SIP Group data without prior written approval.
- Where approved, AI systems must apply anonymization, access control, and data segregation practices in accordance with SIP Group's policies.

12. Compliance and Audit Rights

- SIP Group reserves the right to request evidence of compliance with these requirements or conduct audits, either directly or via a designated representative.
- Non-compliance may lead to suspension of services, contract termination, and legal action.
- Transmission of SIP Group confidential information outside the organization must be authorized in writing by SIP Group.
- All SIP Group-owned or issued IT assets must be returned promptly upon contract termination or as requested.
- Third parties must ensure that email and internet usage complies with professional and security standards, and exercise caution when handling attachments from unknown sources.
- Third parties must refrain from engaging in any spoofing, offensive, discriminatory, or illegal communication activities using SIP Group systems.
- If any subcontractors are engaged in delivering part of the services to SIP Group, their involvement must be governed through a formal and approved subcontracting process. All information security requirements outlined in this document shall apply equally to such subcontractors.
- All third-party personnel involved in providing services to SIP Group must undergo appropriate background verification in accordance with applicable laws and good industry practices.
- Controls must be implemented to ensure data and records are retained and disposed of in line with SIP Group policy and applicable regulatory requirements. SIP Group may request data export or deletion certification upon contract termination.
- All data storage media must be handled and disposed of securely through documented processes to prevent unauthorized access or data leakage.
- Third parties must implement robust anti-malware defenses and ensure regular updates and scans to detect and eliminate harmful code across systems.
- Security controls must be embedded in systems acquisition, development, and maintenance processes, including secure coding, access controls, and timely patch management.