SUMITOMO ELECTRIC BORDNETZE

Information Security Policy for Suppliers

Document Data			
Classification:	**PUBLIC**	Status:	APPROVED
SESAM doc N°:	D1564158	Doc. Owner:	CIT Governance & Security Office
Issue No:	1v0	Issue date:	20-10-2026
Applicable to: All suppliers/third parties processing SEBN information			

Contents

1 Purpose and definitions 3
1.1 Definitions 3
1.2 Document structure and target group 3
2 General requirement for all suppliers 4
2.1 Information classification 4
2.2 Information Handling 4
3 Information Security Requirements 5
3.1 Access Control 5
3.2 Protection of SEBN information 6
3.3 Logging, Monitoring, and Audit Trails 6
3.4 Physical Security 6
3.5 Business Continuity and Disaster Recovery 6
3.6 Subcontractor Management 6
4 Incident Management, Notification and Response 7
5 Compliance Monitoring and Audit 7
6 Compliance with Laws and Standards 7
7 Information Transfer and Confidentiality 7
8 Termination and Offboarding Procedures 8
9 Exceptions and Risk Acceptance 8
10 Change and Review History Record 8

1 Purpose and definitions

This Information Security Policy for Suppliers ("Policy") defines the organizational requirements and rules for information security that must be followed by suppliers/third parties when handling SEBN information and/or when accessing SEBN systems, networks, or facilities. The objective is to protect the confidentiality, integrity, availability, and traceability of SEBN information throughout the supplier lifecycle (due diligence, contracting, onboarding, operations, change, incident handling, audit, and offboarding) and to support compliance with applicable laws, regulations, and standards, including ISO/IEC 27001:2022 (Annex A Control 5.19) and ISO/IEC 27036.

Where local regulations, contractual provisions, or specific frameworks impose stricter requirements, the stricter requirement shall prevail.

1.1 Definitions

- Supplier / Third Party: Any external entity providing goods, services, or resources to SEBN. Subcontractors engaged by a supplier are included.
- Information assets: Data, systems, devices, applications, services, and infrastructure managed by or relied upon by SEBN.
- Security incident: Any event that compromises or threatens the confidentiality, integrity, availability, or traceability of SEBN information assets or services.
- Subcontractor / Sub-processor: Any entity engaged by the supplier to deliver part or all the contracted services and/or that may access SEBN information or systems.
- High/Critical supplier (risk-based): A supplier whose compromise, failure, or service disruption may materially impact SEBN operations, security, safety, or compliance.

1.2 Document structure and target group

This Policy is aimed at supplier management and supplier security leadership. Supplier management must ensure that their employees, temporary staff, and subcontractors are bound to and comply with this Policy.

This document covers the following target groups:

- Suppliers working in SEBN infrastructure
- Suppliers who have access to SEBN information outside SEBN infrastructure
- Suppliers who provide/operate SEBN information outside SEBN infrastructure

Depending on the cooperation model, a supplier can belong to several target groups at the same time.

2 General requirement for all suppliers

2.1 Information classification

All SEBN information is classified according to the following confidentiality Level:

Classification	Definition
Public	Information that is available to the public and intended for distribution outside SEBN. This information may be freely disseminated without potential harm.
Internal	Information that is only intended for internal distribution among SEBN employees and authorized third parties
Company-Confidential	Information whose knowledge or disclosure to unauthorized persons could impede the achieving of product and project objectives and must therefore only be accessible to a limited group of authorized persons.
Customer-Confidential	Information that belongs to customer and needed for business operation and SEBN is obligated to protect by contractual requirements.
Secret	Information whose knowledge or disclosure to unauthorized people could seriously impede the achieving of company objectives and must therefore be subject to a highly restrictive distribution list and strict controls.

2.2 Information Handling

Suppliers who handle SEBN information are responsible for ensuring that information is classified and protected appropriately. The following table defines for each classification categories the associated handling requirements for marking, storage, transmission, sharing, use, and disposal to ensure an adequate level of protection throughout the information lifecycle.

Classification	Requirements
Public	• **Marking:** No marking required • **Reproduction & distribution:** No restrictions; available to general public • **Storage:** No special precautions required • **Transmission:** No special handling required • **Disposal:** Dispose according to environmental regulations or general waste
Internal	• **Marking:** First page marked "Internal / Internal use only"; all pages marked accordingly • **Reproduction & distribution:** Only to employees, contractors, and authorized third parties on a **need-to-know basis** • **Storage:** Protection required (e.g., access control; encryption for devices) • **Transmission:** No special handling internally, but external/public sharing prohibited • **Use in tools:** Restricted in AI/translation tools unless approved • **Disposal:** Must be securely destroyed (e.g., shredding, data overwrite)
Company-Confidential	• **Marking:** Clearly marked "Company-Confidential" on each page • **Reproduction & distribution:** Strictly limited to authorized SEBN staff and contracted third parties with NDA, on **need-to-know basis** • **Storage:** Stored on secure SEBN servers with restricted access; encryption required • **Transmission:** Only via **secure channels** (VPN, TLS, FTP) with authorization • **Restrictions:** Must NOT be shared via public platforms, instant messaging,

	AI tools, or translation services • **Handling:** Printing minimized and supervised; no use in public places or unsecured environments • **Disposal:** Secure destruction required (overwriting, shredding, NDA for third parties, certificate of destruction)
Customer-Confidential	• **Marking:** Clearly marked "Customer-Confidential" on each page • **Reproduction & distribution:** Limited to authorized staff and approved third parties under NDA, **need-to-know basis** • **Access control:** Requires **two-factor authentication** • **Storage:** Secure servers only; restricted access folders; encryption required • **Transmission:** Only authorized and via secure channels • **Restrictions:** Strictly prohibited from AI tools, public internet, instant messaging, or translation services • **Handling:** Cannot be printed outside company; must not be used in public places • **Disposal:** High-security disposal (P4 Shredder or higher according to DIN 66399 shredding, NDA vendors, certificates)
Secret	• **Marking:** Clearly marked "Secret" on each page • **Reproduction & distribution:** Strictly limited; only authorized staff with explicit approval, **need-to-know basis** • **Access control:** Mandatory **two-factor authentication** • **Storage:** Highly restricted, encrypted, secure server storage; no local storage unless strictly controlled • **Transmission:** Only secure channels and owner authorization • **Restrictions:** No use in AI tools, internet, messaging apps, or external services • **Handling:** Cannot leave premises; printing highly restricted; controlled environments only • **Disposal**: High-security disposal (P4 Shredder or higher according to DIN 66399 shredding, NDA vendors, certificates)

3 Information Security Requirements

3.1 Access Control

- **Least privilege** and **need-to-know principles** are mandatory.
- **Strong authentication** must be enforced; **MFA** is required for remote access, administrative accounts, and access to sensitive data or systems.
- **Privileged Access Management** (PAM) controls must be implemented for administrative roles, including session logging and approved workflows.
- Joiner-Mover-Leaver processes shall ensure **timely provisioning/de-provisioning** and **periodic access recertification** (minimum quarterly for High/Critical).
- Supplier accounts must be **unique**, **traceable** to individuals, and **segregated** from personal accounts.

3.2 Protection of SEBN information

- **Information classification and handling** procedures must be enforced commensurate with sensitivity in accordance with the guidelines stipulated in section 2.2.
- **Encryption in transit and at rest** is mandatory for non-public and personal data, using industry-standard algorithms and key management practices.
- **Key management** must ensure segregation of duties, secure storage, rotation, and revocation controls.
- **Data minimization**, **purpose limitation**, and **retention controls** must be documented; retention aligned with contractual and legal requirements.
- **Secure transfer** protocols (e.g., TLS, SFTP) must be used; ad-hoc transfers require approval and logging.
- **Cross-border data transfers** must comply with applicable laws and contractual mechanisms (e.g., SCCs).
- **Backups** must be protected, tested regularly, and stored with appropriate physical and logical controls.

3.3 Logging, Monitoring, and Audit Trails

- Suppliers must maintain tamper-evident logs for authentication events, administrative actions, data access, and security-relevant activities.
- Logs must be time-synchronized, protected, retained per contractual requirements, and made available to SEBN upon request where legally permissible and duly authorized.
- High/Critical suppliers shall support security logging integration (e.g., SIEM, API-based feeds) where feasible.

3.4 Physical Security

- Facilities housing relevant systems or data must implement access controls (badging, visitor logs), surveillance, and environmental protections.
- Media handling and disposal must follow secure sanitization standards.

3.5 Business Continuity and Disaster Recovery

- Suppliers shall maintain documented BCP/DR plans, including RTO/RPO objectives aligned to contractual obligations.
- Plans must be tested at least annually; test results and remediation plans shall be provided upon request for High/Critical suppliers.

3.6 Subcontractor Management

- Suppliers must obtain prior written approval before engaging subcontractors that may access SEBN's information or systems.
- Subcontractors must be bound to equivalent security obligations; suppliers remain fully responsible for subcontractor compliance.

4 Incident Management, Notification and Response

- Suppliers must maintain an incident response plan and designate a security point of contact.
- Notification Timelines:
  - Immediate (within 24 hours): Suspected or confirmed compromise affecting SEBN's data, credentials, systems, or service continuity.
  - Within 72 hours: Any security incident with potential regulatory impact (e.g., personal data breach) or material risk to SEBN.
- Notifications must include incident description, scope, data impacted, root cause (if known), containment actions, mitigation steps, and provisional timeline.
- Suppliers must cooperate with investigations, preserve evidence, provide access to relevant logs and forensic data, and participate in joint response activities.
- Post-incident, suppliers must deliver a Root Cause Analysis (RCA) and Corrective Action Plan within an agreed time frame.

5 Compliance Monitoring and Audit

- SEBN reserves the right to audit supplier security controls, processes, and facilities (onsite or remote) with reasonable notice.
- Suppliers shall provide evidence of compliance, including policy documents, control attestations, penetration test summaries, vulnerability scan results, TISAX/ISO certifications, and remediation plans, where necessary and applicable.
- Non-compliance requires documented corrective actions with agreed timelines; persistent non-compliance may trigger escalation, contractual remedies, or termination.

6 Compliance with Laws and Standards

Suppliers must comply with:

- All applicable laws and regulations in the relevant country (including data protection, cybersecurity, export controls, intellectual property).
- Relevant industry standards and frameworks; where certifications (e.g., ISO/IEC 27001, TISAX) are claimed, suppliers must provide current certificates and scope statements.
- Contractual obligations regarding confidentiality, privacy, IP rights, and acceptable use.

7 Information Transfer and Confidentiality

- All information exchanges must adhere to documented procedures with confidentiality agreements (NDAs) in place.
- All information exchange between SEBN and suppliers shall follow defined and secure processes (e.g., EDI, reporting systems, and approved communication channels) and comply with applicable contractual obligations.

- All commercial and technical information related to SEBN, including but not limited to drawings, specifications, development data, pricing, and customer information, shall be treated as strictly confidential and protected against unauthorized access, disclosure, or misuse.
- Suppliers shall implement appropriate technical and organizational measures to ensure the confidentiality, integrity, and security of SEBN data throughout its lifecycle.
- Any public disclosure or reference to SEBN (e.g., in marketing materials, case studies, or references) requires prior written approval.
- Confidentiality obligations shall remain in effect for the duration of the business relationship and continue thereafter in accordance with applicable contractual agreements.

8 Termination and Offboarding Procedures

Upon termination or expiration of services (or upon request):

- All logical and physical access rights to SEBN systems, facilities, and data (including user accounts, credentials, tokens, and encryption keys) shall be revoked without undue delay after termination. Completion must be formally confirmed in writing.
- All SEBN data shall be returned in agreed formats. Any remaining data, including backups and residual copies, must be securely deleted using recognized industry-standard sanitization methods. The supplier shall provide written proof of destruction upon completion.
- All SEBN-owned assets, including hardware, documents, storage media, and prototypes, shall be returned or securely destroyed in accordance with SEBN instructions.

9 Exceptions and Risk Acceptance

- Exceptions to this Policy must be documented, justified by business need, and approved.
- Risk acceptance decisions must include compensating controls, defined review dates, and owner accountability.

10 Change and Review History Record

Issue	Issue Date	Description of Change
1v0	20.10.2026	Initial issue