

Group | Information Security Policy

1. Introduction

Information security safeguards the Berndorf Group's strategic and operational business processes, which depend substantially on information, communication and operational technologies (IT/OT). This policy aims to ensure an appropriate and effective level of security for the availability, integrity and confidentiality of information and IT/OT systems, preventing business interruption, data loss, financial damage and loss of reputation or trust.

It establishes a uniform, binding minimum standard for all Group companies. It is based on Directive (EU) 2022/2555 (NIS-2) and the applicable national implementing legislation in Austria and Germany. Companies within the statutory scope must meet all applicable legal and regulatory requirements fully and on time. The minimum requirements in this policy apply to every Group company, regardless of statutory applicability.

2. Scope

All Berndorf Group companies must implement these minimum requirements. They may adopt supplementary or stricter policies and work instructions. This policy covers:

- all information-processing systems, networks, applications and data;
- all IT and OT systems, particularly production, control and automation systems;
- all employees and external service providers, suppliers, contractors and other third parties with access to company systems or data.

Companies must ensure compliance by their employees. For external partners, the security requirements relevant to the service, access and associated risk must be secured through appropriate contractual and organisational measures.

The initial assessment and classification under national NIS-2 implementing legislation was conducted at Group level. Changes to business activities, company size, Group structure or technical or operational organisation that may affect the classification must be reported immediately to the responsible function at Berndorf AG.

The classification must be reviewed at least annually and whenever significant changes occur, in coordination with the responsible function at Berndorf AG, and documented in a traceable manner.

3. Information security objectives

3.1. Security awareness

Technical and organisational measures are sufficiently effective only if all employees understand potential threats and act responsibly within their duties. Risk management under section 5.1 and regular training for employees and management under section 5.3 are therefore essential.

3.2. Legal and contractual obligations

The measures support compliance with all relevant legal, regulatory and contractual requirements, particularly NIS-2 requirements.

3.3. Prevention of material damage

Financial losses arising from data loss, manipulation and system failures are to be prevented.

Group | Information Security Policy

3.4. Personality rights and business secrets

The confidentiality and integrity of personal data, business secrets and all other important company information must be protected, regardless of its form. Clear confidentiality instructions must be established and observed for electronic documents and information.

3.5. Protection of reputation

The policy provides a basis for preventing security incidents and the associated loss of reputation and trust.

3.6. Continual improvement

Berndorf AG seeks continual improvement of information security processes and measures in cooperation with the Group companies.

4. Responsibilities and governance

The decentralised organisation requires clear responsibilities at Group and company level.

4.1. Group / Berndorf AG

- Executive Board: holds non-delegable overall responsibility, approves the policy, receives regular reports on risks, incidents and measures, and attends information security training.
- Bee Security GmbH / Group Information Security Officer: leads and coordinates Group-wide activities, provides methods and templates, conducts risk analyses and annual Group-wide security audits, and reports on them.
- IT department: implements technical security measures and ensures system availability. Employees comply with security policies and report incidents.

4.2. Subgroup / subsidiary

- Management: is responsible for implementing this policy and applicable laws, providing resources and resolving deviations within appropriate timeframes. It receives regular risk information, attends training and reports classification-related changes under section 2.
- Information Security Officer: leads and coordinates local activities, coordinates and documents risk analyses, supports audits and tracks the resulting measures.
- IT department: implements technical security measures and ensures system availability. Employees comply with security policies and report incidents.

5. Mandatory minimum requirements

5.1. IT risk management

A documented IT risk management process is mandatory. Analysis of business processes and risks must inform controls and measures to prevent damage or minimise its impact. Berndorf AG templates may be used to establish or review the process.

The process must include, at a minimum: a Business Impact Analysis (BIA) identifying business processes and their criticality; structural analysis; protection needs analysis; risk assessment; risk treatment; and regular review and updating at least annually or as circumstances require. Results must be documented.

Group | Information Security Policy

Documentation must include at least the affected business processes and IT/OT systems, their criticality, responsible persons, identified risks, existing and planned measures, action owners, implementation deadlines and residual risks. Significant residual risks must be submitted to management for a decision and documented risk acceptance. The process is reviewed during security audits.

Management must ensure that the human, financial and technical resources required for information security are available in the short, medium and long term.

5.2. Access control and access rights

Access rights must follow least privilege and be limited to what each role requires. Granting or materially changing administrative or other privileged rights requires documented approval by the responsible system, process or data owner. Rights must be adjusted or withdrawn immediately when employees or external service providers join, change duties or roles, or leave.

Appropriate authentication is mandatory. Multi-factor authentication (MFA) is required in particular for:

- administrative and other privileged access;
- remote access from outside the company network;
- administrative, privileged or maintenance access by external service providers;
- access to cloud-based administration interfaces.

If MFA is technically impossible, particularly on older OT systems, this must be documented and compensated for through appropriate measures such as network segmentation, secured jump servers, time-limited access enablement or enhanced logging.

Privileged rights and external administrative, privileged or maintenance access must be reviewed at least annually and as circumstances require. Reviews must verify continued need, unambiguous identification of the person or provider, necessity and appropriateness of the rights, and implementation of required safeguards, particularly MFA.

The annual review forms part of the Group-wide IT security audits. Companies must provide the required information and resolve deviations within the specified deadlines. A separate annual review of all ordinary user, file, folder, drive or SharePoint permissions is not required.

An up-to-date register of privileged persons and accounts and relevant external providers must be maintained. It must include at least the account holder or provider, system, type and scope of rights, and responsible internal function.

Administrative rights must not be shared. Each authorised person must use a personalised administration account, separate from ordinary user accounts, exclusively for administrative work and with additional protection. Shared technical accounts are permitted only where personalised accounts are technically impossible or inappropriate for substantiated operational reasons. They must be documented, specially protected and their use logged traceably as far as technically possible.

5.3. Information security awareness and training

Regular security training is mandatory. Each company determines participants and scope, taking working conditions and risk exposure into account. Minimum intervals are:

Group | Information Security Policy

- employees: annually and during onboarding;
- management: annually and as circumstances require.

Training may be delivered by Group Legal, Bee Security GmbH or other suitably qualified internal or external providers. Group Legal and Bee Security GmbH may provide materials, organisational support and personnel to deliver it.

Suitable external training is permitted. Companies need not develop their own materials or deliver training internally if the relevant topics are adequately covered. Each company remains responsible for timely completion. Content, delivery and attendance must be documented traceably; suitable attendance or training evidence must be retained for external courses.

5.4. Physical and environmental security

Outside persons must not enter company premises unsupervised. Access controls and organisational measures must prevent unauthorised entry to security-critical areas, particularly server rooms, network distribution points, control rooms and rooms containing critical IT/OT components.

Critical IT/OT systems must be protected against fire, water, power failures, overheating and other relevant environmental hazards according to risk. Measures must be reviewed regularly and documented.

5.5. Supply chain security

A documented, risk-based process to identify, assess and treat supply chain cyber risks must be established and maintained.

Identifying relevant suppliers

Direct suppliers, service providers and other contractual partners must first be assessed to determine whether their products, services, access rights, digital interfaces or other involvement can materially affect the security or availability of the company's network and information systems.

Similar suppliers or supplier groups may be assessed together initially. An individual in-depth cyber risk assessment of every supplier is not required. Suppliers meeting all of the following conditions may, in particular, be excluded from further assessment:

- they provide no ICT products, services or processes;
- they have no access to systems, networks or information requiring protection;
- they have no digital interface or other technical connection;
- their failure or impairment cannot materially affect the security or availability of network and information systems or essential business processes.

The initial assessment and any resulting exclusions must be documented traceably.

5.5. Supply chain security (continued)

Supplier register

An up-to-date register of cyber-relevant direct suppliers, service providers and contractual partners must contain at least:

- name and products, services or processes procured;

Group | Information Security Policy

- responsible internal function or department;
- affected business processes and IT/OT systems;
- type and scope of system, data, remote or administrative access;
- risk classification, date and outcome of the latest assessment;
- outstanding actions and next review date.

Risk classification

Cyber-relevant suppliers must be classified as critical, high or normal before engagement and subsequently on a risk basis. Existing suppliers must be classified according to their risk relevance. The department responsible for procurement or use performs and documents the classification in coordination with IT or the Information Security Officer.

The following criteria must be considered in particular:

- access level: type and scope of access to systems, networks, OT systems, data and information;
- dependency: importance to essential business processes and IT/OT systems, and replaceability;
- maturity: quality and effectiveness of security measures;
- trust: reliability, currency and evidential value of information and supporting evidence;
- potential impact of failures or incidents, and the nature and protection needs of processed information;
- administrative, privileged, maintenance and other remote access;
- security-relevant subcontractors and security of development, maintenance and update processes.

Suppliers must be classified as critical in particular if they operate or substantially support critical IT/OT systems, hold administrative or privileged rights, or their failure or impairment could cause significant operational disruption.

Assessing cyber resilience

The type and depth of assessment depend on risk classification. Overall product and service quality and cyber resilience may be assessed using, in particular:

- documented internal risk assessments and supplier self-assessments;
- assessments under the current Cyber Risk Rating scheme of Kompetenzzentrum Sicheres Österreich and KSV1870;
- valid Cyber Risk Ratings, Cyber Trust Labels and relevant certifications;
- audit, examination and inspection reports, supplier audits conducted internally or by qualified third parties, and equivalent evidence.

A formal rating or specific certification is not mandatory for every supplier if other suitable, traceably documented measures allow adequate assessment. Certificates, ratings and audit reports must cover the actual products and services procured and be current and sufficiently informative.

Group | Information Security Policy

5.5. Supply chain security (continued)

Supplier security requirements

For critical suppliers, the following enhanced requirements must be defined in particular, where relevant to the service:

- evidence of an appropriate information security level;
- contractual incident notification duties that enable timely fulfilment of the company's own statutory reporting duties;
- assistance in investigating, containing and resolving incidents;
- rules governing subcontractors and the flow-down of applicable security requirements;
- audit, control, information and inspection rights, or equivalent evidence;
- defined response, emergency, recovery and business continuity processes;
- appropriate availability, recovery and service-level requirements;
- appropriate liability provisions for security incidents and contractual breaches.

For high-risk suppliers, requirements from this catalogue must be applied according to the service and risk. General security and confidentiality requirements may suffice for normal-risk suppliers.

Contractual safeguards

The requirements must be secured contractually. Depending on the nature and risk of the service, particular consideration must be given to:

- data processing agreements where applicable, confidentiality agreements and service level agreements;
- secure remote access, particularly MFA, logging and assignment of rights;
- incident notification and assistance duties;
- subcontractors and further subcontracting;
- provision and updating of security evidence;
- data location and processing in accordance with applicable law;
- secure development, maintenance and update processes;
- appropriate transparency concerning third-party and open-source components in security-relevant software;
- service termination, particularly data return or deletion and withdrawal of access rights.

Security requirements apply equally to systems and services operated internally and by external providers.

5.5. Supply chain security (continued)

Review and monitoring

The supplier register and risk classification must be reviewed and documented at least annually and whenever material changes occur in services, access rights, subcontractors or the risk situation.

Group | Information Security Policy

Critical suppliers' cyber resilience must be reviewed at least annually. For other cyber-relevant suppliers, risk classification determines the extent and frequency of reassessment. If there have been no material changes, confirming existing information and checking relevant changes may suffice.

Reassessment is required particularly after significant security incidents, material service changes, new administrative or remote access, expiry or withdrawal of security evidence, or substantiated doubts about earlier assessments.

Risks and deviations must be treated with appropriate measures whose implementation is monitored. Significant residual risks must be submitted to management for a documented decision.

The process, particularly initial assessment, classification, evaluation and evidence, may follow the current Cyber Risk Rating scheme of Kompetenzzentrum Sicheres Österreich and KSV1870 (Annex 1). Alternative processes are permitted.

5.6. Operational security and technical system operation

Suitable technical and organisational measures must ensure secure IT/OT operation, particularly patch and vulnerability management, secure configurations, state-of-the-art cryptography, secured remote access and regular maintenance of security-critical components.

Specific measures must be defined in technical policies and operating documentation. They must be guided by relevant technical controls in recognised information security standards and the state of the art; certification to a particular standard is not required.

5.7. Emergency preparedness and recovery

This section governs strategic emergency, recovery and crisis management for business continuity. Section 6 governs operational incident handling. Companies must implement:

- Emergency and recovery planning: plans for critical IT/OT systems, regular backups, and regular review and validation of recovery processes. Recoverability must be verified at least annually through a documented recovery test or equivalent technical validation.
- Business continuity: define recovery objectives, such as RTO, RPO or equivalent parameters, and validate them regularly through tests and reviews.
- Emergency manual and exercises: maintain a manual, conduct regular strategic emergency and crisis exercises, document results and derive improvements.
- Crisis management: define organisation, roles, responsibilities, alerting and communication plans; coordinate as necessary with relevant internal and external bodies, such as CERT, authorities, providers and system integrators.

5.8. Personnel security

Suitable processes and policies must ensure personnel integrity and security. Required measures are:

- checking new employees' qualifications and trustworthiness, for example through a criminal record extract;
- defined onboarding, change and offboarding processes;
- immediate adjustment of system and physical access rights when duties or roles change;

Group | Information Security Policy

- withdrawal of these rights no later than the effective departure date;
- binding security and IT policies, including sanctions for violations.

5.9. Security architecture

Secure configuration and hardening: systems and applications must be secured according to documented hardening and configuration standards. Configuration records must remain current; unnecessary services and components must be disabled or removed.

Asset and ownership model: an up-to-date inventory of IT/OT systems, components, software platforms and applications must include criticality classifications and designated owners.

Network segmentation and interfaces: networks must be segmented physically or logically according to protection needs. Connections between segments must be limited to the necessary minimum. Interfaces with suppliers or customers, such as remote access, monitoring and data exchange, must be secured and documented.

Network security: inbound, outbound and internal traffic must be filtered and limited to what is necessary. Filtering rules must be reviewed and adjusted regularly.

5.10. Use of artificial intelligence (AI)

AI systems must be used in accordance with the Group AI Policy. Companies must establish supplementary internal rules where AI systems may have security-critical, data-protection-critical or business-critical effects. These must address in particular:

- protection of confidential company information;
- transfer of data to external systems;
- transparency of use;
- risk assessment before production use.

6. Information security incidents

Each company must establish a documented process to detect, report, assess and handle security incidents. It must cover, in particular, detection of security-relevant events, impact assessment, operational containment and recovery, and internal and external reporting duties.

Employees and external persons must immediately report actual or suspected incidents through the designated internal channel to the Information Security Officer or internal reporting function. The reporting person does not need to make a final assessment.

a. Reporting duties

The designated responsible function determines whether statutory external reporting is required, in coordination with management and the responsible information security functions. Companies subject to national NIS-2 implementing legislation must observe statutory deadlines:

- early warning immediately, no later than 24 hours after becoming aware;
- detailed notification within 72 hours;
- final report after the incident has been resolved.

The competent national reporting bodies must be involved in accordance with applicable legal requirements.

Group | Information Security Policy

b. Escalation and coordination

Procedures, escalation levels and responsibilities must be aligned between incident response and emergency and crisis management, and documented as binding arrangements.

c. Tests and operational exercises

Incident response processes must be tested regularly, for example through tabletop exercises or technical tests, and updated.

d. Forensic capability

Forensic expertise and capacity must be maintained internally or made available through contractually secured providers.

e. Lessons learned

Lessons from incidents and exercises must be documented and incorporated into continual improvement.

7. Monitoring and effectiveness assessment

Companies must establish processes for ongoing monitoring and assessment of information security. Suitable metrics, maturity assessments or action reviews must be defined in the IT policy. Scope and technical design depend on system criticality, risk and technical conditions. Internal systems, central Group solutions or suitable external providers may be used.

7.1. Logging and monitoring

Logging and monitoring must cover critical IT/OT systems, security components, administrative workstations and central services. Logs must include date and time stamps from synchronised time sources, be stored centrally and retained securely for a defined period. Retention periods and responsibilities for operating, analysing and protecting logging systems must be defined and documented.

7.2. Correlation and analysis

Security events must be evaluated using suitable mechanisms, such as central correlation and analysis, to detect and assess incidents promptly. Stored log data must remain confidential.

8. Documentation and reporting

All security-relevant processes, measures and incidents must be documented traceably. Documentation must include at least:

- risk analyses and registers of critical IT/OT systems and administrative access;
- supplier classifications and training evidence;
- results of recovery and emergency tests;
- information security incidents and audit findings;
- implementation status of resulting actions.

Reports must be provided to the management of the top-level company in each subgroup at least annually and when significant risks, incidents or substantial implementation delays arise. That management reports the subgroup's current status to the Executive Board of Berndorf AG.

Group | Information Security Policy

9. Annual audits

Bee Security GmbH reviews implementation of and compliance with these minimum requirements as an additional item in the annual Group-wide security audits. A consistent audit approach applies to every subgroup.

Deviations and improvement opportunities must be recorded in the audit report. Appropriate measures, owners and deadlines must be defined for deviations, and implementation must be tracked.

Significant deviations or delays must be reported to the management of the affected company and, through Group-wide reporting, to the responsible functions at Berndorf AG.

10. Final provisions

This information security policy takes effect upon publication. It must be reviewed regularly and updated as needed to reflect current requirements and threats.

On behalf of the Management:

Josef Unterberger