SEW EURODRIVE

Public declaration on the applicability of ISO 27001

Version: V3.0 | April 9, 2025

5 Organizational measures

ISO/IEC 27002:2022	Name of measure ISO/IEC 27002:2022	Description of measure	Our statement
5.1	Policies for information security	Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Numerous security-related topics, agreements, and regulations are clearly defined within SEW-EURODRIVE. The objective of these measures is to secure and maintain business operations on a permanent basis. The SEW-EURODRIVE Security Policy forms the central framework: It defines the essential security aspects and promotes a company-wide awareness of information security among all employees.
5.2	Information security roles and responsibilities	Information security roles and responsibilities should be defined and allocated according to the organization needs.	The Cybersecurity area within the Corporate Digital Technology department is responsible for all key information security issues at SEW-EURODRIVE. However, security is a company-wide concern that is anchored in all areas. Individual topics – such as the classification of information – require a department-specific evaluation. By consistently implementing the defined controls, roles and responsibilities are clearly defined and segregated from each other.
5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility should be segregated.	A clear segregation of duties is a prerequisite for efficient business processes at SEW-EURODRIVE. Due to the size and complexity of the company, this segregation is essential – at the same time, it forms the basis for effective information security.
5.4	Management responsibilities	Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.	SEW-EURODRIVE attaches great importance to a pronounced security awareness. The management commits all employees to implement information security in accordance with the applicable information security policy and the associated guidelines and procedures. This obligation is anchored in the Security Policy adopted by the management, which calls for security-conscious action from the outset. This creates a common understanding and promotes consistent application of security standards throughout the company.
5.5	Contact with authorities	The organization should establish and maintain contact with relevant authorities.	SEW-EURODRIVE has implemented measures that ensure an appropriate flow of information on information security with judicial, regulatory; and supervisory authorities. The existing contacts are used to understand the expectations of the authorities regarding information security regulations and to promote compliance with the regulations.
5.6	Contact with special interest groups	The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.	Maintaining contacts with interest groups helps SEW-EURODRIVE to identify important developments in the area of information security at an early stage and to strengthen the exchange of expertise. This makes it possible to improve the information security management system (ISMS) continuously and to enhance it efficiently. For this reason, it is important for SEW-EURODRIVE to actively maintain these contacts.
5.7	Threat intelligence	Information relating to information security threats should be collected and analyzed to produce threat intelligence.	To monitor the threat situation, the company uses analyses of security incidents, threat intelligence, and external penetration tests. In addition, employees are trained and sensitized regularly. Exchanging information with external sources ensures that information security continues to be protected effectively.
5.8	Information security in project management	Information security should be integrated into project management.	Numerous projects are carried out annually within the Corporate Digital Technology (CDT) department. Since essential aspects of information security are anchored at CDT, it is necessary to take them into account in the projects in order to achieve the defined security goals. Specific resilience and development guidelines for information systems are used, among other things. The introduction of new systems or changes is accompanied by risk analyses. In the operational environment, weaknesses are continuously identified and remedied by the responsible areas. In addition, regular security checks of various systems take place.
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, should be developed and maintained.	Assets are inventoried in the IT Service Management Tool (ITSM). The organizational and technical responsibilities are regulated at asset level.
5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets should be identified, documented, and implemented.	The IT service management tool is used to make an inventory of all IT assets. The permitted use of individual assets is defined in the Security Policy. The services provided are intended solely for the performance of business tasks. The handling of company property obligates all employees to maintain confidentiality with regard to external persons.

ISO/IEC 27002:2022	Name of measure ISO/IEC 27002:2022	Description of measure	Our statement
5.11	Return of assets	Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.	The return of individual assets at the end of the employment relationship is ensured by means of checklists from the Human Resources department and under the obligation of the manager to cooperate. The declaration of commitment in the employment contract regulates the obligation of employees of SEW-EURODRIVE to cooperate in the return of assets. If necessary, employees can notify the change of ownership of their assets. If an asset is lost, a loss report must be produced immediately. Any return in cooperation with external parties is secured by non-disclosure agreements.
5.12	Classification of information	Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability, and relevant interested party requirements.	Procedures and responsibilities for classifying and identifying information are described in the Security Policy of SEW-EURODRIVE and are applied throughout the organization. The commonly used classification level is "Business"; a separate identification is implemented according to the internal specifications as required.
5.13	Labeling of information	An appropriate set of procedures for information labeling should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Procedures and responsibilities for classifying and identifying information are described in the Security Policy of SEW-EURODRIVE and are applied throughout the organization. The commonly used classification level is "Business"; a separate identification is implemented according to the internal specifications as required.
5.14	Information transfer	Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.	Technical and organizational measures for secure communications have been defined and communicated.
5.15	Access control	Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	SEW-EURODRIVE uses security mechanisms such as authentication, authorization, data encryption, and continuous monitoring to specifically control access to information and to ensure the protection of corporate assets.
5.16	Identity management	The full life cycle of identities should be managed.	The full life cycle of identities is managed and documented by a request system, including approval structures.
5.17	Authentication information	Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	The central element for authentication at SEW-EURODRIVE is a two-factor method with virtual and physical smart cards. In many applications, single sign-on (SSO) is used after logging on to the computer. A technical AD password policy applies to user accounts. Password-safe solutions are also used.
5.18	Access rights	Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	At SEW-EURODRIVE, new or changed authorizations are assigned exclusively via a defined approval process. The existing authorizations are subject to regular review and are immediately adjusted or revoked, if necessary.
5.19	Information security in supplier relationships	Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Non-disclosure agreements and information security risks are documented via a list of criteria and are part of the selection process. The strategic service providers are defined in the selection process.
5.20	Addressing information security within supplier agreements	Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Information security requirements are documented via a criteria catalog and are part of the selection process.
5.21	Managing information security in the ICT supply chain	Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	SEW-EURODRIVE has implemented comprehensive processes and procedures to effectively manage and minimize the information security risks that arise from the ICT products and services supply chain. The criteria catalog serves as the basis for identifying relevant risks.
5.22	Monitoring, review, and change management of supplier services	The organization should regularly monitor, review, evaluate, and manage change in supplier information security practices and service delivery.	The annual evaluation of strategic suppliers at SEW-EURODRIVE includes the verification of information security.
5.23	Information security for use of cloud services	Processes for acquisition, use, management, and exit from cloud services should be established in accordance with the organization's information security requirements.	The use of cloud services requires the initiation and formal approval of a "cloud enablement". This acceptance process ensures the organizational integration of each cloud use case and integrates various key stakeholders, including the Cybersecurity department.
5.24	Information security incident management planning and preparation	The organization should plan and prepare for managing information security incidents by defining, establishing, and communicating information security incident management processes, roles, and responsibilities.	The company uses playbooks, checklists, and forms to process and document security incidents. The ISMS role and improvement plan and the emergency plan are also used. They establish clear responsibilities and support continuous development.
5.25	Assessment and decision on information security events	The organization should assess information security events and decide if they are to be categorized as information security incidents.	SEW-EURODRIVE uses playbooks to systematically assess events in the area of information security and to decide whether they are classified as security incidents. In this way, we ensure that all relevant events are detected quickly and classified correctly.

ISO/IEC 27002:2022	Name of measure ISO/IEC 27002:2022	Description of measure	Our statement
5.26	Response to information security incidents	Information security incidents should be responded to in accordance with the documented procedures.	SEW-EURODRIVE uses incident response playbooks to respond to security incidents according to the particular situation, which enable a structured and efficient response.
5.27	Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	The incident response playbooks define that documents are adapted based on the knowledge gained from security incidents.
5.28	Collection of evidence	The organization should establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.	The company consistently implements procedures for identifying, collecting, procuring, and safely storing evidence in the event of information security incidents. In this way, SEW-EURODRIVE ensures that all relevant evidence is documented comprehensibly, completely, and correctly.
5.29	Information security during disruption	The organization should plan how to maintain information security at an appropriate level during disruption.	SEW-EURODRIVE ensures business continuity through a higher-level emergency plan that defines measures, responsibilities, and regulations. Specific business continuity plans exist for the IT systems that always take into account the maintenance and restoration of information security and that are tested regularly.
5.30	ICT readiness for business continuity	ICT readiness should be planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements.	The company is pursuing a development strategy for the controlled restoration of the infrastructure, even in severe scenarios. Continuity plans are updated and reviewed regularly.
5.31	Legal, statutory, regulatory, and contractual requirements	Legal, statutory, regulatory, and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented, and kept up to date.	The requirements are documented in a legal register, kept up-to-date, and corresponding measures are derived. The Compliance, Legal, and Quality Assurance departments ensure that these aspects are anchored in existing processes.
5.32	Intellectual property rights	The organization should implement appropriate procedures to protect intellectual property rights.	The intellectual property of SEW-EURODRIVE and third parties is strategically regulated and operationally safeguarded. The "IP strategy" guideline ensures, manages, and enforces industrial property rights centrally via a responsible department. In addition, the tasks of the license managers are defined in the declaration of commitment associated with the employment contract, the process descriptions (e.g. "IT license management"), and the Security Policy. These tasks include, in particular, the obligations for software compliance throughout the entire life cycle. Procedures for monitoring possible license violations have been established.
5.33	Protection of records	Records should be protected from loss, destruction, falsification, unauthorized access, and unauthorized release.	At SEW-EURODRIVE, records and customer data are stored in compliance with the applicable national laws. The declaration of commitment protects records from persons outside the company. There are technical measures for backups and the storage and transfer of information.
5.34	Privacy and protection of PII	The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	SEW-EURODRIVE has appointed an internal data protection officer to protect privacy and personal data. This person will create the required processes and monitor their compliance.
5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes, and technologies should be reviewed independently at planned intervals, or when significant changes occur.	SEW-EURODRIVE undertakes to regularly and independently review the procedure for handling information security – including employees, processes, and technologies – especially in the event of significant changes. The internal audits are carried out in cooperation with external experts and are anchored in the audit plan of the ISMS improvement plan.
5.36	Compliance with policies, rules, and standards for information security	Compliance with the organization's information security policy, topic-specific policies, rules, and standards should be regularly reviewed.	All relevant documents, specifications, and standards within the scope of the ISMS are regularly reviewed.
5.37	Documented operating procedures	Operating procedures for information processing facilities should be documented and made available to personnel who need them.	The services that are widely used by employees and offer numerous configuration settings are evaluated and approved in collaboration with the Cybersecurity department. "Terms of Use" are defined for each service that is made available to external persons.

6 People controls

ISO/IEC 27002:2022	Name of measure ISO/IEC 27002:2022	Description of measure	Our statement
6.1	Screening	Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis, taking into consideration applicable laws, regulations, and ethics and be proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.	Screening applicants ensures that jobs are filled appropriately and corporate assets are protected. The innovative power of SEW-EURODRIVE is an essential basis for economic success and can only be ensured by selecting suitable employees. In particularly sensitive areas of responsibility, HR Administration performs an in-depth check. The same procedures also apply to contractual partners, such as leasing employees.
6.2	Terms and conditions of employment	The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.	SEW-EURODRIVE employees receive a comprehensive range of work equipment that allows them to access data and services. In many areas, highly sensitive data and information are used that are crucial for the economic success of the company, such as patents. Appropriate contractual clauses have been implemented to ensure the legal framework conditions for both SEW-EURODRIVE and its employees.
6.3	Information security awareness, education, and training	Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education, and training and regular updates of the organization's information security policy, topic-specific policies, and procedures, as relevant for their job function.	An annual mandatory Security Policy e-learning course is stipulated for all employees and must be completed. In addition, a cybersecurity newsletter is used to proactively inform about current and general threats.
6.4	Disciplinary process	A disciplinary process should be formalized and communicated to take action against personnel and other relevant interested parties who have committed an information security policy violation.	Violations by employees against employment contract obligations or other ancillary obligations of the employment contract shall be punished by adequate disciplinary measures after the facts have been assessed. Violations of laws, contracts, and internal regulations are covered in the Security Policy.
6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced, and communicated to relevant personnel and other interested parties.	Responsibilities and obligations in the area of information security are defined in the employment contract and also apply beyond the end or change of employment.
6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed, and signed by personnel and other relevant interested parties.	Confidentiality and non-disclosure agreements that meet the information protection requirements of SEW-EURODRIVE are identified, documented, and regularly reviewed. These agreements must be signed by employees and other relevant parties. This applies in particular to SEW-EURODRIVE's relationships with external service providers, suppliers, and customers, as well as to the employment of external employees.
6.7	Remote working	Security measures should be implemented when personnel are working remotely to protect information accessed, processed; or stored outside the organization's premises.	Employees only access corporate resources remotely via a secure VPN connection. Mobile end devices such as smartphones and tablets can only be accessed via VPN or via the implemented MDM solution. The devices are secured with relevant security mechanisms.
6.8	Information security event reporting	The organization should provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Employees are instructed by the Security Policy to report any observed or suspected incidents in the area of information security immediately and in good time.

7 Physical controls

ISO/IEC 27002:2022	Name of measure ISO/IEC 27002:2022	Description of measure	Our statement
7.1	Physical security perimeters	Security perimeters should be defined and used to protect areas that contain information and other associated assets.	The Security Policy classifies the buildings into various protection classes, for example public or secret. Corresponding rules of behavior are also described here. There are various technical facilities to protect against unauthorized access, including fences, access control systems, alarm systems, locking systems, and cameras.
7.2	Physical entry	Secure areas should be protected by appropriate entry controls and access points.	SEW-EURODRIVE uses a multi-stage access control system that only grants access to authorized employees. The check is carried out using an SEW-EURODRIVE smartcard. Areas that are particularly vulnerable are additionally secured with additional security devices such as alarm systems or biometric access controls. Guests receive a guest pass and must be accompanied. Rules for this are anchored in the Security Policy. Different types of identification show whether they are internal or external employees.
7.3	Securing offices, rooms, and facilities	Physical security for offices, rooms, and facilities should be designed and implemented.	Offices and premises are accessible as soon as access has been granted via the access control system. Protected areas are protected by additional security devices. Offices and meeting rooms can be locked. Telephone directories and location plans are only available internally.
7.4	Physical security monitoring	Premises should be continuously monitored for unauthorized physical access.	SEW-EURODRIVE buildings are monitored by camera systems and intrusion detection systems. The gates are staffed around the clock. Various alarm systems are used which are checked and maintained regularly. All technical equipment is tamper-proof.
7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure, should be designed and implemented.	Physical and environmental hazards were taken into account from the outset during the planning and construction of SEW-EURODRIVE's data centers. Several UPS and diesel generators ensure operation even in the event of a power failure.
7.6	Working in secure areas	Security measures for working in secure areas should be designed and implemented.	At SEW-EURODRIVE, a general photo ban is stipulated in the Security Policy. Critical secure areas are protected by physical protection devices.
7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.	Rules for dealing with information are defined in the Security Policy. It contains specifications for safe storage and the deletion of information. t is also stipulates that premises must be locked. Screens are automatically locked by a technical policy at SEW-EURODRIVE. In addition, clean desk specifications apply. Additional regulations can be found in a guideline for the working environment that covers aspects such as occupational safety, order and cleanliness, and information security.
7.8	Equipment siting and protection	Equipment should be sited securely and protected.	The servers are operated exclusively in protected SEW-EURODRIVE data centers. For network technology, there are decentralized distribution rooms to which only authorized administrators have access. All devices are regularly tested electrostatically. The room temperature and humidity are monitored and controlled centrally. In addition, special hardware is used that is adapted to the respective ambient conditions, such as increased temperatures.
7.9	Security of assets off-premises	Off-site assets should be protected.	Security mechanisms are activated on mobile devices. Only encrypted USB sticks and hard disks are permitted as USB storage media. The screen lock and other measures to make the clients more resilient also apply outside the company. Smartphones are managed and made more resilient centrally. In addition, there are documented security requirements for business trips.

ISO/IEC 27002:2022	Name of measure ISO/IEC 27002:2022	Description of measure	Our statement
7.10	Storage media	Storage media should be managed through their life cycle of acquisition, use, transportation, and disposal in accordance with the organization's classification scheme and handling requirements.	Devices and operating resources are either safely deleted or physically destroyed at the end of their life cycle. The use of removable data carriers is permitted only in encrypted form.
7.11	Supporting utilities	Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.	Various systems are used in the SEW-EURODRIVE data centers to safeguard the current supply and Internet connection. The data centers are connected to each other and designed for redundancy. The servers usually use several power sources. The network infrastructure and air-conditioning technology also have measures for fail-safety.
7.12	Cabling security	Cables carrying power, data, or supporting information services should be protected from interception, interference, or damage.	Cabling at SEW-EURODRIVE complies with current guidelines. The cables are routed in cable ducts and redundant connections are provided to ensure reliable function.
7.13	Equipment maintenance	Equipment should be maintained correctly to ensure availability, integrity, and confidentiality of information.	Maintenance contracts exist for all relevant systems, which are stored centrally. Maintenance is performed at regular intervals.
7.14	Secure disposal or reuse of equipment	Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or reuse.	Devices and equipment are either safely deleted or physically destroyed at the end of their life cycle to ensure the protection of sensitive data.

8 Technological controls

ISO/IEC 27002:2022	Name of measure ISO/IEC 27002:2022	Description of measure	Our statement
8.1	User endpoint devices	Information stored on, processed by, or accessible via user endpoint devices should be protected.	SEW-EURODRIVE only uses proprietary, centrally managed end devices. They are subject to a comprehensive security concept with various protective measures, including current authentication methods, modern encryption technologies, and regular software and security updates. The objective of these measures is to prevent unauthorized access to sensitive company data and to ensure the integrity of the IT infrastructure.
8.2	Privileged access rights	The allocation and use of privileged access rights should be restricted and managed.	Privileged access rights are only assigned at SEW-EURODRIVE if they are actually required. By default, no-one has these rights. After a specified period, the access rights expire automatically and must be requested again if necessary.
8.3	Information access restriction	Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	SEW-EURODRIVE has set up an information access policy that regulates all aspects of user and authorization management. It ensures that access to systems and information is clearly defined, controlled, and traceable.
8.4	Access to source code	Read and write access to source code, development tools, and software libraries should be appropriately managed.	The source code of SEW-EURODRIVE must be stored in the central SEW-EURODRIVE repository and read and write access is clearly regulated.

ISO/IEC 27002:2022	Name of measure ISO/IEC 27002:2022	Description of measure	Our statement
8.5	Secure authentication	Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	SEW-EURODRIVE uses smart cards for secure authentication. The procedure works without a password and uses a login certificate. The password is not displayed on the login screen in the event of input errors. The data transmissions are encrypted. Failed login attempts can be traced, and logs are kept both locally and in the back end.
8.6	Capacity management	The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	The IT systems, infrastructure components, storage media, and grid connections at SEW-EURODRIVE are equipped with sufficient resources both technically and in terms of personnel. This ensures safe and complete monitoring by the operating team.
8.7	Protection against malware	Protection against malware should be implemented and supported by appropriate user awareness.	SEW-EURODRIVE uses various security measures to protect itself from malware. This includes preventive approaches such as securing systems and training for users and reactive measures, such as the use of protection solutions for end devices and networks to detect and defend against threats at an early stage.
8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated, and appropriate measures should be taken.	At SEW-EURODRIVE, vulnerability scans are performed continuously and the results are tracked. In addition, structured security checks are carried out, supplemented by fixed deadlines for evaluating vulnerabilities on various device types. There are regular patch days for the systems. The information flow of manufacturers and suppliers is ensured via various channels and integrated into the internal processes.
8.9	Configuration management	Configurations, including security configurations, of hardware, software, services, and networks should be established, documented, implemented, monitored, and reviewed.	SEW-EURODRIVE uses resilience guidelines for configuring IT systems and makes regular adjustments. Security checks help to identify and eliminate vulnerabilities.
8.10	Information deletion	Information stored in information systems, devices, or in any other storage media should be deleted when no longer required.	Specifications and processes ensure that data on devices and storage media is reliably deleted.
8.11	Data masking	Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies and business requirements, taking applicable legislation into consideration.	SEW-EURODRIVE uses state-of-the-art technical and cryptographic measures to reliably protect sensitive data, including the data of our customers.
8.12	Data leakage prevention	Data leakage prevention measures should be applied to systems, networks, and any other devices that process, store, or transmit sensitive information.	SEW-EURODRIVE takes various measures to prevent data leaks and to protect sensitive information. Technologies and concepts are used to help identify potential risks at an early stage.
8.13	Information backup	Backup copies of information, software, and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Backup copies of information, software, and systems are kept at SEW-EURODRIVE in accordance with the defined guidelines for data backup and checked regularly.
8.14	Redundancy of information processing facilities	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.	For business-critical systems, SEW-EURODRIVE relies on redundant designs. They include duplicate power and Internet connections as well as spatially separate data centers where the systems are also operated redundantly.
8.15	Logging	Logs that record activities, exceptions, faults, and other relevant events should be produced, stored, protected, and analyzed.	SEW-EURODRIVE uses technical solutions to create, save, protect, and analyze logs. These logs record activities, exceptions, errors, and other relevant events. This ensures that all necessary information for monitoring information security is available.

ISO/IEC 27002:2022	Name of measure ISO/IEC 27002:2022	Description of measure	Our statement
8.16	Monitoring activities	Networks, systems, and applications should be monitored for anomalous behavior and appropriate actions taken to evaluate potential information security incidents.	SEW-EURODRIVE continuously monitors networks, systems, and applications for anomalous behavior and analyzes any discrepancies to specifically identify and evaluate potential information security incidents. Security monitoring and incident evaluation are supported by external service providers, among other things.
8.17	Clock synchronization	The clocks of information processing systems used by the organization should be synchronized to approved time sources.	SEW-EURODRIVE uses publicly available time servers as an external time source. An NTP service with which devices synchronize is available internally via a special server.
8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.	SEW-EURODRIVE has implemented a least-privilege concept on the clients. Users do not have administrator rights by default, but can request them if necessary. All accesses are logged by the server. In the industrial environment, service accounts that do not have admin rights are used primarily.
8.19	Installation of software on operational systems	Procedures and measures should be implemented to securely manage software installation on operational systems.	Certain software is an integral part of SEW-EURODRIVE's corporate presence. Additional applications are distributed centrally. In addition, technical measures have been implemented to prevent the installation of potentially harmful software.
8.20	Networks security	Networks and network devices should be secured, managed, and controlled to protect information in systems and applications.	Access to network components is reserved exclusively for trained internal employees with administrative authorizations. These persons are specially authorized and possess the necessary expertise to perform security-related tasks responsibly. All network devices and systems are secured and continuously monitored for availability, telemetry, and compliance. This ensures the integrity and security of the information in SEW-EURODRIVE's systems and applications at all times.
8.21	Security of network services	Security mechanisms, service levels, and service requirements of network services should be identified, implemented, and monitored.	The security mechanisms for network services from SEW-EURODRIVE are tested regularly to ensure their effectiveness and reliability. The results of these tests are systematically documented and form the basis for continuous improvements. The service quality and the specific requirements are defined by the responsible departments and technically implemented in close coordination with the IT department. In order to comply with and monitor these specifications, a continuous check is performed by several monitoring systems that record and evaluate both technical parameters and compliance aspects.
8.22	Segregation of networks	Groups of information services, users, and information systems should be segregated in the organization's networks.	SEW-EURODRIVE performs a comprehensive risk assessment of individual IT assets and enables their dedicated hosting in assigned network segments. There is a clear segregation of internal and external networks and between centrally managed and decentrally managed devices at global level. Technologies such as firewalls and routing via gateways are used. The assignment of users to IP addresses and the targeted evaluation of all connections are implemented operationally.
8.23	Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	SEW-EURODRIVE uses various security mechanisms to secure Internet access, including firewalls, DNS security, and advanced anti-virus functions. In addition, browser sandboxing is used for URLs opened from e-mails.
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, should be defined and implemented.	The rules for dealing with cryptography are part of the SEW-EURODRIVE cryptography guideline. Several internal certificate infrastructures form a central element for the technical implementation of cryptographic processes.

ISO/IEC 27002:2022	Name of measure ISO/IEC 27002:2022	Description of measure	Our statement
8.25	Secure development life cycle	Rules for the secure development of software and systems should be established and applied.	The technical and organizational specifications are defined in the work instructions for DevSec at SEW-EURODRIVE, among other things, and are complied with.
8.26	Application security requirements	Information security requirements should be identified, specified, and approved when developing or acquiring applications.	The technical and organizational specifications are defined in the work instructions for DevSec and in the cloud enablement process of SEW-EURODRIVE, among other things, and are complied with.
8.27	Secure system architecture and engineering principles	Principles for engineering secure systems should be established, documented, maintained, and applied to any information system development activities.	SEW-EURODRIVE has defined security principles for conceptual solution design and pursues a product-oriented defense-in-depth strategy. The access and configuration of all systems are based on the “Need-to-Know” and “Least-Privilege” principles.
8.28	Secure coding	Secure coding principles should be applied to software development.	The technical and organizational specifications are defined in the work instructions for DevSec and in the secure coding recommendations of SEW-EURODRIVE, among other things, and are complied with.
8.29	Security testing in development and acceptance	Security testing processes should be defined and implemented in the development life cycle.	The technical and organizational specifications are defined in the work instructions for DevSec at SEW-EURODRIVE, among other things, and are complied with. In addition, the code is technically checked for vulnerabilities.
8.30	Outsourced development	The organization should direct, monitor, and review the activities related to outsourced system development.	Outsourced developments are performed under the organizational specifications of SEW-EURODRIVE and checked when they are imported into SEW-EURODRIVE systems.
8.31	Separation of development, test, and production environments	Development, testing, and production environments should be separated and secured.	The environments for development (D systems), quality assurance (Q systems), and production (P systems) are segregated from each other in such a way that unauthorized changes and access to the production environment are prevented. For this purpose, the development guidelines as well as guidelines for transportation and change management apply at SEW-EURODRIVE.
8.32	Change management	Changes to information processing facilities and information systems should be subject to change management procedures.	Changes to information processing facilities and information systems at SEW-EURODRIVE are implemented according to the change management procedures in accordance with ITIL (Information Technology Infrastructure Library) and ISO 20000.
8.33	Test information	Test information should be appropriately selected, protected, and managed.	The organizational specifications are defined in internal work instructions for DevSec test data at SEW-EURODRIVE and are complied with.
8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.	Several times a year, the company has coordinated systems at SEW-EURODRIVE checked for vulnerabilities by external experts. The results are documented with recommendations for action, processed, and monitored with repeat tests to check the measures, if necessary.

2270 7255 / 0326

Further information is available at:
www.sew-eurodrive.de/en/cybersecurity

SEW-EURODRIVE GmbH & Co KG
Ernst-Blickle-Str. 42
76646 Bruchsal/Germany
T +49 7251 75-0
F +49 7251 75-1970
sew@sew-eurodrive.com
www.sew-eurodrive.com