Driving the world

SEW EURODRIVE

Öffentliche Erklärung zur Anwendbarkeit der ISO 27001

Version: v3.0 | 09.04.2025

5 Organisatorische Maßnahmen

ISO/IEC 27002:2022	Maßnahmenname ISO/IEC 27002:2022	Maßnahmenbeschreibung	Unser Statement
5.1	Informationssicherheits-richtlinien	Informationssicherheitspolitik und themenspezifische Richtlinien sollten definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.	Innerhalb von SEW-EURODRIVE sind zahlreiche sicherheitsrelevante Themen, Vereinbarungen und Regelungen klar definiert. Ziel dieser Maßnahmen ist es, den Geschäftsbetrieb dauerhaft zu sichern und aufrechtzuerhalten. Die SEW-EURODRIVE Security Policy bildet dabei den zentralen Rahmen: Sie definiert die wesentlichen Sicherheitsaspekte und fördert ein unternehmensweites Bewusstsein für Informationssicherheit bei allen Mitarbeitenden.
5.2	Informationssicherheits-rollen und -verantwortlichkeiten	Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit sollten entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.	Der Bereich Cyber Security innerhalb der Abteilung Corporate Digital Technology verantwortet alle zentralen Themen der Informationssicherheit bei SEW-EURODRIVE. Sicherheit ist jedoch ein unternehmensweites Anliegen, das in allen Bereichen verankert ist. Einzelne Themen – beispielsweise die Klassifizierung von Informationen – erfordern eine fachbereichsspezifische Bewertung. Durch die konsequente Umsetzung der festgelegten Kontrollen werden Zuständigkeiten und Verantwortlichkeiten klar definiert und voneinander abgegrenzt.
5.3	Aufgabentrennung	Sich widersprechende Aufgaben und Verantwortungsbereiche sollten voneinander getrennt werden.	Eine klare Trennung von Aufgabenbereichen ist bei SEW-EURODRIVE Voraussetzung für effiziente Geschäftsprozesse. Aufgrund der Unternehmensgröße und -komplexität ist diese Trennung unerlässlich – sie bildet zugleich das Fundament für eine wirksame Informationssicherheit.
5.4	Verantwortlichkeiten der Leitung	Die Leitung sollte von dem gesamten Personal verlangen, dass es die Informationssicherheit im Einklang mit der eingeführten Informationssicherheitspolitik und den themenspezifischen Richtlinien und Verfahren der Organisation umsetzt.	SEW-EURODRIVE legt großen Wert auf ein ausgeprägtes Sicherheitsbewusstsein. Die Geschäftsführung verpflichtet alle Mitarbeitenden, die Informationssicherheit gemäß der geltenden Informationssicherheitspolitik sowie den zugehörigen Richtlinien und Verfahren umzusetzen. Diese Verpflichtung ist in der von der Geschäftsführung verabschiedeten Security Policy verankert, die einleitend zu sicherheitsbewusstem Handeln aufruft. So wird ein gemeinsames Verständnis geschaffen und die konsequente Anwendung der Sicherheitsstandards im gesamten Unternehmen gefördert.
5.5	Kontakt mit Behörden	Die Organisation sollte mit den zuständigen Behörden Kontakt aufnehmen und halten.	SEW-EURODRIVE hat Maßnahmen umgesetzt, welche einen angemessenen Informationsfluss zur Informationssicherheit mit Justiz-, Regulierungs- und Aufsichtsbehörden sicherstellen. Die bestehenden Kontakte werden genutzt, um die Erwartungen der Behörden hinsichtlich Informationssicherheitsvorschriften zu verstehen und die Einhaltung der Vorgaben zu fördern.
5.6	Kontakt mit speziellen Interessensgruppen	Die Organisation sollte Kontakte mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden herstellen und pflegen.	Die Pflege von Kontakten zu Interessenvertretungen hilft SEW-EURODRIVE dabei, wichtige Entwicklungen im Bereich der Informationssicherheit frühzeitig zu erkennen und den fachlichen Austausch zu stärken. Dadurch kann das Informationssicherheitsmanagementsystem (ISMS) kontinuierlich verbessert und effizient weiterentwickelt werden. Aus diesem Grund ist es für SEW-EURODRIVE wichtig, diese Kontakte aktiv zu pflegen.
5.7	Bedrohungsintelligenz	Informationen über Bedrohungen der Informationssicherheit sollten erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.	Zur Überwachung der Bedrohungslage setzt das Unternehmen Analysen von Sicherheitsvorfällen, Threat Intelligence sowie externe Penetrationstests ein. Zusätzlich werden Mitarbeitende regelmäßig geschult und sensibilisiert. Durch den Austausch mit externen Informationsquellen wird sichergestellt, dass die Informationssicherheit wirksam geschützt bleibt.
5.8	Informationssicherheit im Projektmanagement	Die Informationssicherheit sollte in das Projektmanagement integriert werden.	Innerhalb der Abteilung Corporate Digital Technology (CDT) werden jährlich zahlreiche Projekte durchgeführt. Da wesentliche Aspekte der Informationssicherheit bei CDT verankert sind, ist es erforderlich, diese in den Projekten zu berücksichtigen, um die definierten Sicherheitsziele zu erreichen. Hierbei kommen unter anderem spezifische Härtungs- und Entwicklungsrichtlinien für Informationssysteme zur Anwendung. Die Einführung neuer Systeme oder Änderungen werden durch Risikoanalysen begleitet. Im operativen Umfeld werden kontinuierlich Schwachstellen identifiziert und von den zuständigen Bereichen behoben. Darüber hinaus finden regelmäßige Sicherheitsüberprüfungen verschiedener Systeme statt.
5.9	Inventar der Informationen und anderen damit verbundenen Werten	Ein Inventar der Informationen und anderen damit verbundenen Werten, einschließlich der Eigentümer, sollte erstellt und gepflegt werden.	Assets werden im IT-Service-Management-Tool (ITSM) inventarisiert. Die organisatorischen und technischen Zuständigkeiten sind auf Asset-Ebene geregelt.
5.10	Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten	Regeln für den zulässigen Gebrauch und Verfahren für den Umgang mit Informationen und anderen zugehörigen Vermögenswerten sollten aufgestellt, dokumentiert und angewendet werden.	Die Inventarisierung aller IT-Assets erfolgt über das eingesetzte IT-Service-Management-Tool. Die zulässige Nutzung einzelner Assets ist in der Security Policy festgelegt. Die bereitgestellten Dienste dienen ausschließlich der Erfüllung geschäftlicher Aufgaben. Der Umgang mit Unternehmenseigentum verpflichtet alle Mitarbeitenden zur Wahrung der Vertraulichkeit gegenüber externen Personen.

ISO/IEC 27002:2022	Maßnahmenname ISO/IEC 27002:2022	Maßnahmenbeschreibung	Unser Statement
5.11	Rückgabe von Werten	Das Personal und gegebenenfalls andere interessierte Parteien sollten alle Werte der Organisation, die sich in ihrem Besitz befinden, bei Änderung oder Beendigung ihres Beschäftigungsverhältnisses, Vertrags oder ihrer Vereinbarung zurückgeben.	Die Rückgabe einzelner Assets bei Beendigung des Beschäftigungsverhältnisses wird mithilfe von Checklisten aus dem Personalbereich und unter Mitwirkungspflicht der Führungskraft sichergestellt. Über die Verpflichtungserklärung im Arbeitsvertrag wird die Mitwirkungspflicht der Mitarbeitenden von SEW-EURODRIVE zur Rückführung geregelt. Bei Bedarf können Mitarbeitende den Besitzwechsel ihrer Assets mitteilen. Bei Verlust eines Assets ist unverzüglich eine Verlustmeldung zu erstellen. Die Rückgabe in Zusammenarbeit mit externen Parteien wird durch Geheimhaltungsvereinbarungen abgesichert.
5.12	Klassifizierung von Information	Informationen sollten entsprechend den Informationssicherheitsanforderungen der Organisation auf der Grundlage von Vertraulichkeit, Integrität, Verfügbarkeit und relevanten Anforderungen der interessierten Parteien klassifiziert werden.	Verfahren und Verantwortlichkeiten zur Klassifizierung und Kennzeichnung von Informationen sind in der Security Policy von SEW-EURODRIVE beschrieben und werden organisationsweit angewendet. Die üblicherweise verwendete Klassifizierungsebene ist „Geschäftlich“; eine gesonderte Kennzeichnung erfolgt nach Bedarf gemäß den internen Vorgaben.
5.13	Kennzeichnung von Information	Ein angemessener Satz von Verfahren zur Kennzeichnung von Informationen sollte entsprechend dem von der Organisation eingesetzten Informationsklassifizierungsschema entwickelt und umgesetzt werden.	Verfahren und Verantwortlichkeiten zur Klassifizierung und Kennzeichnung von Informationen sind in der Security Policy von SEW-EURODRIVE beschrieben und werden organisationsweit angewendet. Die üblicherweise verwendete Klassifizierungsebene ist „Geschäftlich“; eine gesonderte Kennzeichnung erfolgt nach Bedarf gemäß den internen Vorgaben.
5.14	Informationsübertragung	Für alle Arten von Übertragungseinrichtungen innerhalb der Organisation und zwischen der Organisation und anderen Parteien sollten Regeln, Verfahren oder Vereinbarungen zur Informationsübermittlung vorhanden sein.	Technische und organisatorische Maßnahmen zur sicheren Kommunikation sind definiert und kommuniziert.
5.15	Zugangssteuerung	Regeln zur Kontrolle des physischen und logischen Zugriffs auf Informationen und andere zugehörige Werte sollten auf der Grundlage von Geschäfts- und Informationssicherheitsanforderungen aufgestellt und umgesetzt werden.	Bei SEW-EURODRIVE werden Sicherheitsmechanismen wie Authentifizierung, Autorisierung, Verschlüsselung und kontinuierliches Monitoring eingesetzt, um den Zugriff auf Informationen gezielt zu steuern und den Schutz der Unternehmenswerte sicherzustellen.
5.16	Identitätsmanagement	Der gesamte Lebenszyklus von Identitäten sollte verwaltet werden.	Der gesamte Lebenszyklus von Identitäten wird durch ein Antragswesen inkl. Genehmigungsstrukturen verwaltet und dokumentiert.
5.17	Informationen zur Authentifizierung	Die Zuweisung und Verwaltung von Authentifizierungsinformationen sollte durch einen Managementprozess gesteuert werden, der auch die Beratung des Personals über den angemessenen Umgang mit Authentifizierungsinformationen umfasst.	Das zentrale Element zur Authentifizierung bei SEW-EURODRIVE ist ein Zwei-Faktor-Verfahren mit virtuellen und physischen Smartcards. In vielen Applikationen wird nach der Anmeldung am Rechner Single Sign-On (SSO) genutzt. Für Benutzerkonten gilt eine technische AD-Passwortrichtlinie. Zusätzlich kommen Password-Safe-Lösungen zum Einsatz.

ISO/IEC 27002:2022	Maßnahmenname ISO/IEC 27002:2022	Maßnahmenbeschreibung	Unser Statement
5.18	Zugangsrechte	Zugangsrechte zu Informationen und anderen zugehörigen Werten sollten in Übereinstimmung mit den themenspezifischen Richtlinien und Regeln der Organisation für die Zugangssteuerung bereitgestellt, überprüft, geändert und entfernt werden.	Neue oder geänderte Berechtigungen werden bei SEW-EURODRIVE ausschließlich über einen definierten Genehmigungsprozess vergeben. Die bestehenden Berechtigungen unterliegen einer regelmäßigen Überprüfung und werden bei fehlender Notwendigkeit sofort angepasst oder entzogen.
5.19	Informationssicherheit in Lieferantenbeziehungen	Es sollten Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der Nutzung der Produkte oder Dienstleistungen des Lieferanten verbundenen Informationssicherheitsrisiken zu beherrschen.	Geheimhaltungsvereinbarungen und Informationssicherheitsrisiken werden über einen Kriterienkatalog dokumentiert und sind Bestandteil des Auswahlverfahrens. Im Auswahlverfahren sind die strategischen Dienstleister definiert.
5.20	Behandlung von Informationssicherheit in Lieferantenvereinbarungen	Je nach Art der Lieferantenbeziehung sollten die entsprechenden Anforderungen an die Informationssicherheit festgelegt und mit jedem Lieferanten vereinbart werden.	Anforderungen an die Informationssicherheit werden über einen Kriterienkatalog dokumentiert und sind Bestandteil des Auswahlverfahrens.
5.21	Umgang mit der Informationssicherheit in der IKT-Lieferkette	Es sollten Prozesse und Verfahren festgelegt und umgesetzt werden, um die mit der IKT-Produkt- und Dienstleistungslieferkette verbundenen Informationssicherheitsrisiken zu beherrschen.	SEW-EURODRIVE hat umfassende Prozesse und Verfahren implementiert, um die Informationssicherheitsrisiken, die aus der IKT-Produkt- und Dienstleistungslieferkette entstehen, wirksam zu steuern und zu minimieren. Der Kriterienkatalog dient als Grundlage für die Identifizierung relevanter Risiken.
5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen	Die Organisation sollte regelmäßig die Informationssicherheitspraktiken der Lieferanten und die Erbringung von Dienstleistungen überwachen, überprüfen, bewerten und Änderungen steuern.	Die jährliche Bewertung der strategischen Lieferanten bei SEW-EURODRIVE beinhaltet die Überprüfung der Informationssicherheit.
5.23	Informationssicherheit für die Nutzung von Cloud-Diensten	Die Verfahren für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten sollten in Übereinstimmung mit den Informationssicherheitsanforderungen der Organisation festgelegt werden.	Die Nutzung von Cloud-Diensten erfordert die Initiierung und formelle Genehmigung eines „Cloud Enablements“. Dieser Abnahmeprozess stellt die organisatorische Eingliederung jedes Cloud Use Cases sicher und bindet verschiedene Schlüssel-Stakeholder, einschließlich der Cybersecurity-Abteilung, ein.
5.24	Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen	Die Organisation sollte die Handhabung von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für die Handhabung von Informationssicherheitsvorfällen definiert, einführt und kommuniziert.	Das Unternehmen nutzt Playbooks, Checklisten und Formulare zur Bearbeitung und Dokumentation von Sicherheitsvorfällen. Ergänzend kommen der ISMS-Rollen- und Verbesserungsplan sowie der Notfallplan zum Einsatz. Diese schaffen klare Verantwortlichkeiten und unterstützen die kontinuierliche Weiterentwicklung.
5.25	Beurteilung und Entscheidung über Informationssicherheitsereignisse	Die Organisation sollte Ereignisse im Bereich der Informationssicherheit beurteilen und entscheiden, ob sie als Vorfälle im Bereich der Informationssicherheit eingestuft werden sollen.	SEW-EURODRIVE nutzt Playbooks um Ereignisse im Bereich der Informationssicherheit systematisch zu beurteilen und zu entscheiden, ob sie als Sicherheitsvorfälle eingestuft werden. So stellen wir sicher, dass alle relevanten Ereignisse schnell erkannt und korrekt eingeordnet werden.

ISO/IEC 27002:2022	Maßnahmenname ISO/IEC 27002:2022	Maßnahmenbeschreibung	Unser Statement
5.26	Reaktion auf Informationssicherheitsvorfälle	Auf Informationssicherheitsvorfälle sollte entsprechend den dokumentierten Verfahren reagiert werden.	SEW-EURODRIVE setzt zur Reaktion auf Sicherheitsvorfälle entsprechend der Situation Incident-Response Playbooks ein, die eine strukturierte und effiziente Reaktion ermöglichen.
5.27	Erkenntnisse aus Informationssicherheitsvorfällen	Aus Informationssicherheitsvorfällen gewonnene Erkenntnisse sollten zur Verstärkung und Verbesserung der Informationssicherheitsmaßnahmen genutzt werden.	Die Incident-Response Playbooks definieren, dass Dokumente basierend auf gewonnen Erkentnissen aus Sicherheitsvorfällen adaptiert werden.
5.28	Sammeln von Beweismaterial	Die Organisation sollte Verfahren für die Identifizierung, Sammlung, Beschaffung und Aufbewahrung von Beweismitteln im Zusammenhang mit Informationssicherheitsvorfällen einführen und umsetzen.	Das Unternehmen setzt Verfahren zur Identifizierung, Sammlung, Beschaffung und sicheren Aufbewahrung von Beweismitteln bei Informationssicherheitsvorfällen konsequent um. So stellt SEW-EURODRIVE sicher, dass alle relevanten Beweise nachvollziehbar, vollständig und korrekt dokumentiert werden.
5.29	Informationssicherheit bei Störungen	Die Organisation sollte planen, wie die Informationssicherheit während der Störung auf einem angemessenen Niveau gehalten werden kann.	SEW-EURODRIVE stellt die Geschäftskontinuität durch einen übergeordneten Notfallplan sicher, der Maßnahmen, Verantwortlichkeiten und Regelungen festlegt. Für IT-Systeme existieren spezifische Business-Continuity-Pläne, welche die Aufrechterhaltung und Wiederherstellung der Informationssicherheit stets berücksichtigen und regelmäßig getestet werden.
5.30	IKT-Bereitschaft für Business Continuity	Die IKT-Bereitschaft sollte auf der Grundlage von Business-Continuity-Zielen und IKT-Kontinuitätsanforderungen geplant, umgesetzt, aufrechterhalten und geprüft werden.	Das Unternehmen verfolgt eine Aufbaustrategie zur kontrollierten Wiederherstellung der Infrastruktur auch in schwerwiegenden Szenarien. Kontinuitätspläne werden regelmäßig aktualisiert und geprüft.
5.31	Rechtliche, gesetzliche, regulatorische und vertragliche Anforderungen	Rechtliche, gesetzliche, behördliche und vertragliche Anforderungen, die für die Informationssicherheit relevant sind, und die Vorgehensweise der Organisation zur Erfüllung dieser Anforderungenn sollen ermittelt dokumentiert und auf dem neuesten Stand gehalten werden.	Die Anforderungen werden in einem Rechtskataster dokumentiert, aktuell gehalten und entsprechende Maßnahmen abgeleitet. Die Verankerung in bestehenden Prozessen erfolgt mit Compliance, Legal und Qualitätssicherung.
5.32	Geistige Eigentumsrechte	Die Organisation sollte geeignete Verfahren zum Schutz der Rechte an geistigem Eigentum einführen.	Das geistige Eigentum von SEW-EURODRIVE und Dritten ist strategisch geregelt und wird operativ sichergestellt. Über die Richtlinie „IP-Strategie“ werden gewerbliche Schutzrechte zentral durch eine zuständige Abteilung gesichert, verwaltet und durchgesetzt. Zusätzlich sind in der Verpflichtungserklärung zum Arbeitsvertrag, in Prozessbeschreibungen (z. B. „IT-Lizenzmanagement“) sowie in der Security Policy die Aufgaben der Lizenzverantwortlichen definiert. Dazu gehören insbesondere die Pflichten zur Software-Compliance über den gesamten Lebenszyklus. Verfahren zur Kontrolle möglicher Lizenzverletzungen sind etabliert.
5.33	Schutz von Aufzeichnungen	Aufzeichnungen sollten vor Verlust, Zerstörung, Fälschung, unbefugtem Zugriff und unbefugter Veröffentlichung geschützt sein.	Bei SEW-EURODRIVE werden Aufzeichnungen und Kundendaten unter Einhaltung der jeweils geltenden nationalen Rechtsvorschriften gespeichert. Durch die Verpflichtungserklärung sind Aufzeichnungen gegenüber betriebsfremden Personen geschützt. Für Backups sowie die Speicherung und Übertragung von Informationen bestehen technische Maßnahmen.
5.34	Datenschutz und Schutz personenbezogener Daten (pbD)	Die Organisation sollte die Anforderungen an die Wahrung der Privatsphäre und den Schutz personenbezogener Daten nach den geltenden Gesetzen und Vorschriften sowie den vertraglichen Anforderungen ermitteln und erfüllen.	SEW-EURODRIVE hat zur Wahrung der Privatsphäre und zum Schutz personenbezogener Daten einen internen Datenschutzbeauftragten benannt. Diese Person erstellt die erforderlichen Prozesse und überwacht deren Einhaltung.
5.35	Unabhängige Überprüfung der Informationssicherheit	Die Vorgehensweise der Organisation für die Handhabung der Informationssicherheit und deren Umsetzung einschließlich der Mitarbeiter, Prozesse und Technologien, sollten auf unabhängige Weise in planmäßigen Abständen oder jeweils bei erheblichen Änderungen überprüft werden.	SEW-EURODRIVE verpflichtet sich, die Vorgehensweise zur Handhabung der Informationssicherheit – einschließlich Mitarbeitenden, Prozessen und Technologien – regelmäßig und unabhängig zu überprüfen, insbesondere bei wesentlichen Änderungen. Die internen Audits erfolgen in Zusammenarbeit mit externen Fachleuten und sind im Auditplan des ISMS-Verbesserungsplans verankert.
5.36	Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit	Die Einhaltung der Informationssicherheitspolitik der Organisation, der themenspezifischen Richtlinien, Regeln und Normen sollte regelmäßig überprüft werden.	Alle relevanten Dokumente, Vorgaben und Normen im Rahmen des ISMS werden regelmäßig überprüft.
5.37	Dokumentierte Betriebsabläufe	Die Betriebsverfahren für Informationsverarbeitungsanlagen sollten dokumentiert und dem Personal, das sie benötigt, zur Verfügung gestellt werden.	Die Services, die von Mitarbeitenden in großem Umfang genutzt werden und zahlreiche Konfigurationseinstellungen bieten, werden in Zusammenarbeit mit der Cyber-Security-Abteilung bewertet und freigegeben. Für jeden Service, der externen Personen zugänglich gemacht wird, werden „Terms of Use“ definiert.

6 Personenbezogene Maßnahmen

ISO/IEC 27002:2022	Maßnahmenname ISO/IEC 27002:2022	Maßnahmenbeschreibung	Unser Statement
6.1	Sicherheitsüberprüfung	Alle Personen, die in die Belegschaft aufgenommen werden, sollten vor dem Eintritt in die Organisation und fortlaufend unter Berücksichtigung geltender Gesetze, Vorschriften und ethischer Grundsätze einer Sicherheitsüberprüfung unterzogen werden und in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Information und den wahrgenommenen Risiken stehen.	Die Überprüfung von Bewerber:innen stellt sicher, dass Arbeitsplätze passend besetzt und Unternehmenswerte geschützt werden. Die Innovationskraft von SEW-EURODRIVE ist eine wesentliche Grundlage für den wirtschaftlichen Erfolg und kann nur durch die Auswahl geeigneter Mitarbeitenden gewährleistet werden. In besonders sensiblen Aufgabenbereichen erfolgt eine vertiefte Prüfung durch die HR-Administration. Die gleichen Verfahren gelten auch für Vertragspartner:innen, wie beispielsweise Leasing-Mitarbeitende.
6.2	Beschäftigungs- und Vertragsbedingungen	In den arbeitsvertraglichen Vereinbarungen sollten die Verantwortlichkeiten des Personals und der Organisation für die Informationssicherheit festgelegt werden.	Die Mitarbeitenden von SEW-EURODRIVE erhalten eine umfassende Ausstattung an Arbeitsmitteln, die ihnen den Zugriff auf Daten und Dienste ermöglicht. In vielen Bereichen wird mit hochsensiblen Daten und Informationen gearbeitet, welche für den wirtschaftlichen Erfolg des Unternehmens von entscheidender Bedeutung sind, wie beispielsweise Patenten. Um sowohl die rechtlichen Rahmenbedingungen für SEW-EURODRIVE als auch für die Mitarbeitenden zu gewährleisten, sind entsprechende Vertragsklauseln implementiert.
6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung	Das Personal der Organisation und relevante interessierte Parteien sollten ein angemessenes Bewusstsein für die Informationssicherheit, eine entsprechende Ausbildung und Schulung sowie regelmäßige Aktualisierungen der Informationssicherheitspolitik der Organisation, themenspezifischer Richtlinien und Verfahren erhalten, die für ihr berufliches Arbeitsgebiet relevant sind.	Ein jährlich verpflichtendes Security Policy E-Learning ist für alle Mitarbeitenden vorgeschrieben und muss absolviert werden. Zusätzlich wird ein Cybersecurity-Newsletter genutzt, der proaktiv über aktuelle sowie allgemeine Bedrohungen informiert.
6.4	Maßregelungsprozess	Ein Maßregelungsprozess sollte formalisiert und kommuniziert werden, um Maßnahmen gegen Mitarbeiter und andere interessierte Parteien zu ergreifen, die einen Verstoß gegen die Informationssicherheitspolitik begangen haben.	Verstöße durch Mitarbeitende gegen arbeitsvertragliche Pflichten oder sonstige Nebenpflichten des Arbeitsvertrags werden nach Bewertung des Sachverhalts durch adqäquate, disziplinarische Maßnahmen geahndet. Verstöße gegen Gesetze, Verträge und interne Regelungen werden in der Security Policy behandelt.
6.5	Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung	Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit, die auch nach Beendigung oder Änderung der Beschäftigung bestehen bleiben, sollten festgelegt, durchgesetzt und den betreffenden Mitarbeitern und anderen interessierten Parteien mitgeteilt werden.	Verantwortlichkeiten und Pflichten im Bereich der Informationssicherheit sind im Arbeitsvertrag definiert und gelten auch über das Ende oder die Änderung der Beschäftigung hinaus.
6.6	Vertraulichkeits- oder Geheimhaltungsvereinbarungen	Vertraulichkeits- oder Geheimhaltungsvereinbarungen, welche die Erfordernisse der Organisation an den Schutz von Information widerspiegeln, sollten identifiziert, dokumentiert, regelmäßig überprüft und von den Mitarbeitern und anderen interessierten Parteien unterzeichnet werden.	Vertraulichkeits- und Geheimhaltungsvereinbarungen, die den Informationsschutzanforderungen der SEW-EURODRIVE entsprechen, sind identifiziert, dokumentiert und werden regelmäßig überprüft. Diese Vereinbarungen müssen von Mitarbeitenden sowie anderen relevanten Parteien unterzeichnet werden. Dies gilt insbesondere für die Beziehungen von SEW-EURODRIVE zu externen Dienstleister:innen, Lieferant:innen und Kund:innen sowie für die Beschäftigung externer Mitarbeitenden.
6.7	Telearbeit	Es sollten Sicherheitsmaßnahmen ergriffen werden, wenn Mitarbeiter extern arbeiten, um Informationen zu schützen, die außerhalb der Räumlichkeiten des Unternehmens abgerufen, verarbeitet oder gespeichert werden.	Mitarbeitende greifen von unterwegs ausschließlich über eine gesicherte VPN-Verbindung auf Unternehmensressourcen zu. Für mobile Endgeräte wie Smartphones und Tablets ist der Zugriff ausschließlich per VPN oder über die implementierte MDM-Lösung möglich. Die Geräte sind mit relevanten Sicherheitsmechanismen gesichert.
6.8	Meldung von Informationssicherheitsereignissen	Die Organisation sollte einen Mechanismus bereitstellen, der es den Mitarbeitern ermöglicht, beobachtete oder vermutete Vorfälle im Bereich der Informationssicherheit über geeignete Kanäle rechtzeitig zu melden.	Mitarbeitende sind über die Security Policy angewiesen, beobachtete oder vermutete Vorfälle im Bereich der Informationssicherheit umgehend und rechtzeitig zu melden.

7 Physische Maßnahmen

ISO/IEC 27002:2022	Maßnahmenname ISO/IEC 27002:2022	Maßnahmenbeschreibung	Unser Statement
7.1	Physische Sicherheitsperimeter	Zum Schutz von Bereichen, in denen sich andere zugehörige Werte befinden, sollten Sicherheitsperimeter festgelegt und verwendet werden.	In der Security Policy erfolgt eine Einteilung der Gebäude in verschiedene Schutzklassen, beispielweise öffentlich oder geheim. Entsprechende Verhaltensregeln werden hier ebenfalls beschrieben. Zum Schutz gegen unbefugte Zutritte gibt es verschiedene technische Einrichtungen, darunter Zäune, Zutrittskontrollsysteme, Alarmanlagen, Schließsysteme und Kameras.
7.2	Physischer Zutritt	Sicherheitsbereiche sollten durch eine angemessene Zutrittssteuerung und Zutrittsstellen geschützt werden.	SEW-EURODRIVE nutzt ein mehrstufiges Zutrittskontrollsystem, welches nur berechtigten Mitarbeitenden Zutritt gewährt. Die Kontrolle erfolgt mittels SEW-EURODRIVE-Smartcard. Besonders schützenswerte Bereiche sind zusätzlich durch weitere Sicherheitseinrichtungen wie beispielsweise Alarmanlagen oder biometrische Zutrittskontrollen gesichert. Gäste erhalten einen Gastausweis und sind zu begleiten. Regeln hierzu sind in der Security Policy verankert. Verschiedene Ausweistypen lassen erkennen, ob es sich um interne oder externe Mitarbeitende handelt.
7.3	Sichern von Büros, Räumen und Einrichtungen	Die physische Sicherheit für Büros, Räume und Einrichtungen sollte konzipiert und umgesetzt werden.	Büros und Räumlichkeiten sind zugänglich, sobald der Zutritt über das Zutrittskontrollsystem gewährt wurde. Geschützte Bereiche werden durch zusätzliche Sicherheitseinrichtungen abgesichert. Büros und Besprechungsräume können verschlossen werden. Telefonverzeichnisse und Lagepläne sind ausschließlich intern abrufbar.
7.4	Physische Sicherheitsüberwachung	Die Räumlichkeiten sollten ständig auf unbefugten physischen Zugang überwacht werden.	Die Gebäude von SEW-EURODRIVE werden durch Kamerasysteme und Einbruchmeldeanlagen überwacht. Die Pforten sind rund um die Uhr besetzt. Es kommen verschiedene Alarmanlagensysteme zum Einsatz, die regelmäßig geprüft und gewartet werden. Alle technischen Einrichtungen sind manipulationssicher implementiert.
7.5	Schutz vor physischen und umweltbedingten Bedrohungen	Der Schutz vor physischen und umweltbedingten Bedrohungen wie Naturkatastrophen und anderen absichtlichen oder unabsichtlichen physischen Bedrohungen der Infrastruktur sollte geplant und umgesetzt werden.	Bei der Planung und dem Bau der Rechenzentren von SEW-EURODRIVE wurden physische und umgebungsbezogene Gefährdungen von Beginn an berücksichtigt. USVs und Dieselgeneratoren stellen den Betrieb auch bei einem Stromausfall sicher.
7.6	Arbeiten in Sicherheitsbereichen	Es sollten Sicherheitsmaßnahmen für die Arbeit in Sicherheitsbereichen konzipiert und umgesetzt werden.	Bei SEW-EURODRIVE ist in der Sicherheitsrichtlinie ein generelles Fotografierverbot festgelegt. Kritische Sicherheitsbereiche werden durch physische Schutzvorrichtungen gesichert.
7.7	Aufgeräumte Arbeitsumgebung und Bildschirmsperren	Es sollten klare Regeln für eine aufgeräumte Arbeitsumgebung hinsichtlich Unterlagen und Wechseldatenträgern und klare Regeln für Bildschirmsperren für informationsverarbeitende Einrichtungen festgelegt und angemessen durchgesetzt werden.	Regeln zum Umgang mit Informationen sind i n der Security Policy festgelegt. Diese enthält Vorgaben zur sicheren Verwahrung sowie zur Löschung von Informationen. Zudem ist geregelt, dass Räumlichkeiten verschlossen werden müssen. Bildschirme werden bei SEW-EURODRIVE durch eine technische Policy automatisch gesperrt. Darüber hinaus gelten Clean-Desk-Vorgaben. Ergänzende Regelungen finden sich in einer Richtlinie für die Arbeitsumgebung, die Aspekte wie Arbeitssicherheit, Ordnung und Sauberkeit sowie Informationssicherheit umfasst.
7.8	Platzierung und Schutz von Geräten und Betriebsmitteln	Die Geräte und Betriebsmittel sollten sicher und geschützt aufgestellt werden.	Die Server werden ausschließlich in geschützten Rechenzentren von SEW-EURODRIVE betrieben. Für die Netzwerktechnik gibt es dezentrale Verteilerräume, zu denen nur autorisierte Administrator:innen Zugang haben. Alle Geräte werden regelmäßig elektrostatisch geprüft. Die Raumtemperatur und Luftfeuchtigkeit werden zentral überwacht und gesteuert. Zusätzlich kommt spezielle Hardware zum Einsatz, die an die jeweiligen Umgebungsbedingungen, wie beispielsweise erhöhte Temperaturen, angepasst ist.
7.9	Sicherheit von Werten außerhalb der Räumlichkeiten	Werte außerhalb des Standorts sollten geschützt werden.	Auf mobilen Geräten sind Sicherheitsmechanismen aktiviert. Als USB-Speichermedien sind ausschließlich verschlüsselte USB-Sticks und Festplatten zugelassen. Die Bildschirmsperre sowie weitere Maßnahmen zur Härtung der Clients greifen auch außerhalb des Unternehmens. Smartphones werden zentral verwaltet und gehärtet. Darüber hinaus existieren dokumentierte Sicherheitsvorgaben für Geschäftsreisen.

ISO/IEC 27002:2022	Maßnahmenname ISO/IEC 27002:2022	Maßnahmenbeschreibung	Unser Statement
7.10	Speichermedien	Speichermedien sollten während ihres gesamten Lebenszyklus – Erwerb, Verwendung, Transport und Entsorgung – in Übereinstimmung mit dem Klassifizierungsschema und den Handhabungsanforderungen der Organisation verwaltet werden.	Geräte und Betriebsmittel werden am Ende ihres Lebenszyklus entweder sicher gelöscht oder physisch vernichtet. Die Nutzung von Wechseldatenträgern ist ausschließlich in verschlüsselter Form zulässig.
7.11	Versorgungseinrichtungen	Informationsverarbeitungseinrichtungen sollten vor Stromausfällen und anderen Störungen, die durch Ausfälle von Versorgungseinrichtungen verursacht werden, geschützt werden.	In den Rechenzentren von SEW-EURODRIVE kommen verschiedene Systeme zum Einsatz, um die Stromversorgung und Internetanbindung sicherzustellen. Die Rechenzentren sind miteinander verbunden und auf Redundanz ausgelegt. Die Server nutzen in der Regel mehrere Stromquellen. Auch die Netzwerkinfrastruktur und die Klimatechnik verfügen über Maßnahmen zur Ausfallsicherheit.
7.12	Sicherheit der Verkabelung	Kabel, die Strom, Daten oder unterstützende Informationsdienste transportieren, sollten vor Unterbrechung, Störung oder Beschädigung geschützt werden.	Die Verkabelung bei SEW-EURODRIVE erfolgt gemäß aktuellen Richtlinien. Die Kabel werden in Kabelkanälen verlegt und es sind redundante Verbindungen vorgesehen, um eine zuverlässige Funktion sicherzustellen.
7.13	Instandhaltung von Geräten und Betriebsmitteln	Geräte und Betriebsmittel sollten ordnungsgemäß gewartet werden, um die Verfügbarkeit, Integrität und Vertraulichkeit der Informationen sicherzustellen.	Für alle relevanten Systeme bestehen Wartungsverträge, die zentral hinterlegt sind. Wartungen werden in regelmäßigen Intervallen durchgeführt.
7.14	Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln	Arten von Geräten und Betriebsmitteln, die Speichermedien enthalten, sollten überprüft werden, um sicherzustellen, dass jegliche sensiblen Daten und lizenzierte Software vor ihrer Entsorgung oder Wiederverwendung entfernt oder sicher überschrieben worden sind.	Geräte und Betriebsmittel werden am Ende ihres Lebenszyklus entweder sicher gelöscht oder physisch zerstört, um den Schutz sensibler Daten zu gewährleisten.

8 Technologische Maßnahmen

ISO/IEC 27002:2022	Maßnahmenname ISO/IEC 27002:2022	Maßnahmenbeschreibung	Unser Statement
8.1	Endpunktgeräte des Benutzers	Informationen, die auf Endpunktgeräten der Benutzer gespeichert sind, von ihnen verarbeitet werden oder über sie zugänglich sind, sollten geschützt werden.	Bei SEW-EURODRIVE kommen ausschließlich firmeneigene, zentral verwaltete Endgeräte zum Einsatz. Diese unterliegen einem umfassenden Sicherheitskonzept mit verschiedenen Schutzmaßnahmen, darunter aktuelle Authentifizierungsmethoden, moderne Verschlüsselungstechnologien sowie regelmäßige Software- und Sicherheitsupdates. Ziel dieser Maßnahmen ist es, unberechtigten Zugriff auf sensible Unternehmensdaten zu verhindern und die Integrität der IT-Infrastruktur zu gewährleisten.
8.2	Privilegierte Zugangsrechte	Zuteilung und Gebrauch von privilegierten Zugangsrechten sollte eingeschränkt und verwaltet werden.	Privilegierte Zugriffsrechte werden bei SEW-EURODRIVE ausschließlich bei tatsächlichem Bedarf vergeben. Standardmäßig verfügt niemand über diese Rechte. Nach einer festgelegten Frist laufen die Zugriffsrechte automatisch ab und müssen bei Bedarf erneut beantragt werden.
8.3	Informationszugangsbeschränkung	Der Zugang zu Informationen und anderen zugehörigen Werten sollte in Übereinstimmung mit der festgelegten themenspezifischen Richtlinie zur Zugangssteuerung eingeschränkt werden.	Bei SEW-EURODRIVE ist eine Informationszugangsrichtlinie etabliert, die alle Aspekte der Benutzer:innen- und Berechtigungsverwaltung regelt. Sie stellt sicher, dass Zugriffe auf Systeme und Informationen klar definiert, kontrolliert und nachvollziehbar gesteuert werden.
8.4	Zugriff auf den Quellcode	Der Lese- und Schreibzugriff auf den Quellcode, die Entwicklungswerkzeuge und die Softwarebibliotheken sollte angemessen verwaltet werden.	Der Quellcode von SEW-EURODRIVE ist im zentralen SEW-EURODRIVE-Repository zu hinterlegen und der Lese- und Schreibzugriff ist klar geregelt.

ISO/IEC 27002:2022	Maßnahmenname ISO/IEC 27002:2022	Maßnahmenbeschreibung	Unser Statement
8.5	Sichere Authentifizierung	Sichere Authentifizierungstechnologien und -verfahren sollten auf der Grundlage von Informationszugangsbeschränkungen und der themenspezifischen Richtlinie zur Zugangssteuerung implementiert werden.	Bei SEW-EURODRIVE werden Smartcards für eine sichere Authentifizierung eingesetzt. Das Verfahren funktioniert passwortlos und nutzt ein Logon-Zertifikat. Am Anmeldebildschirm wird das Passwort bei Eingabefehlern nicht angezeigt. Die Datenübertragungen sind verschlüsselt. Fehlgeschlagene Anmeldeversuche können nachvollzogen werden, und Protokolle werden sowohl lokal als auch im Backend geführt.
8.6	Kapazitätssteuerung	Die Nutzung von Ressourcen sollte überwacht und entsprechend den aktuellen und erwarteten Kapazitätsanforderungen angepasst werden.	Die IT-Systeme, Infrastrukturkomponenten, Speichermedien und Netzverbindungen bei SEW-EURODRIVE sind sowohl technisch als auch personell mit ausreichenden Ressourcen ausgestattet. Dadurch ist eine sichere und vollständige Überwachung durch das Operating-Team gewährleistet.
8.7	Schutz gegen Schadsoftware	Schutz gegen Schadsoftware sollte umgesetzt und durch angemessene Sensibilisierung der Benutzer unterstützt werden.	SEW-EURODRIVE setzt verschiedene Sicherheitsmaßnahmen ein, um sich vor Schadsoftware zu schützen. Dazu gehören präventive Ansätze wie die Absicherung der Systeme und Schulungen für Nutzer:innen sowie reaktive Maßnahmen, beispielsweise der Einsatz von Schutzlösungen für Endgeräte und Netzwerke, um Bedrohungen frühzeitig zu erkennen und abzuwehren.
8.8	Handhabung von technischen Schwachstellen	Es sollten Informationen über technische Schwachstellen verwendeter Informationssysteme eingeholt, die Gefährdung der Organisation durch derartige Schwachstellen bewertet und angemessene Maßnahmen ergriffen werden.	Bei SEW-EURODRIVE werden Schwachstellenscans kontinuierlich durchgeführt, und die Ergebnisse nachverfolgt. Zusätzlich finden strukturierte Sicherheitsüberprüfungen statt, ergänzt durch feste Termine zur Bewertung von Schwachstellen auf unterschiedlichen Gerätetypen. Für die Systeme gibt es regelmäßige Patchdays. Der Informationsfluss von Hersteller:innen und Anbieter:innen wird über verschiedene Kanäle sichergestellt und in die internen Prozesse integriert.
8.9	Konfigurationsmanagement	Konfigurationen, einschließlich Sicherheitskonfigurationen, von Hardware, Software, Diensten und Netzwerken sollten festgelegt, dokumentiert, umgesetzt, überwacht und überprüft werden.	SEW-EURODRIVE nutzt Härtungsrichtlinien zur Konfiguration von IT-Systemen und führt regelmäßig Anpassungen durch. Sicherheitsüberprüfungen unterstützen dabei, Schwachstellen zu identifizieren und zu beheben.

ISO/IEC 27002:2022	Maßnahmenname ISO/IEC 27002:2022	Maßnahmenbeschreibung	Unser Statement
8.10	Löschung von Informationen	Informationen, die in Informationssystemen, Geräten oder auf anderen Speichermedien gespeichert sind, sollten gelöscht werden, wenn sie nicht mehr benötigt werden.	Vorgaben und Prozesse stellen sicher, dass Daten auf Geräten und Speichermedien zuverlässig gelöscht werden.
8.11	Datenmaskierung	Die Datenmaskierung sollte in Übereinstimmung mit den themenspezifischen Richtlinien der Organisation zur Zugangssteuerung und anderen damit zusammenhängenden themenspezifischen Richtlinien sowie den geschäftlichen Anforderungen und unter Berücksichtigung der geltenden Rechtsvorschriften eingesetzt werden.	SEW-EURODRIVE setzt technische und kryptografische Maßnahmen ein, die sich am Stand der Technik orientieren, um sensible Daten, einschließlich der Daten unserer Kund:innen, zuverlässig zu schützen.
8.12	Verhinderung von Datenlecks	Maßnahmen zur Verhinderung von Datenlecks sollten auf Systeme, Netzwerke und alle anderen Geräte angewendet werden, die sensible Informationen verarbeiten, speichern oder übertragen.	SEW-EURODRIVE ergreift verschiedene Maßnahmen, um Datenlecks zu verhindern und sensible Informationen zu schützen. Dabei kommen Technologien und Konzepte zum Einsatz, die helfen, potenzielle Risiken frühzeitig zu erkennen.
8.13	Sicherung von Information	Sicherungskopien von Informationen, Software und Systemen sollten in Übereinstimmung mit den vereinbarten themenspezifischen Richtlinien für Datensicherungen aufbewahrt und regelmäßig geprüft werden.	Sicherungskopien von Informationen, Software und Systemen werden bei SEW-EURODRIVE gemäß den festgelegten Richtlinien für Datensicherung aufbewahrt und regelmäßig überprüft.
8.14	Redundanz von informationsverarbeitenden Einrichtungen	Informationsverarbeitende Einrichtungen sollten mit ausreichender Redundanz für die Einhaltung der Verfügbarkeitsanforderungen realisiert werden.	Für geschäftskritische Systeme setzt SEW-EURODRIVE auf redundante Auslegungen. Dazu gehören doppelte Strom- und Internetanbindungen sowie räumlich getrennte Rechenzentren, in denen die Systeme ebenfalls redundant betrieben werden.
8.15	Protokollierung	Protokolle, die Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse aufzeichnen, sollten erstellt, gespeichert, geschützt und analysiert werden.	SEW-EURODRIVE nutzt technische Lösungen, um Protokolle zu erstellen, zu speichern, zu schützen und zu analysieren. Diese Protokolle erfassen Aktivitäten, Ausnahmen, Fehler und andere relevante Ereignisse. So wird sichergestellt, dass alle notwendigen Informationen für die Überwachung der Informationssicherheit verfügbar sind.

ISO/IEC 27002:2022	Maßnahmenname ISO/IEC 27002:2022	Maßnahmenbeschreibung	Unser Statement
8.16	Überwachungstätigkeiten	Netzwerke, Systeme und Anwendungen sollten auf anormales Verhalten überwacht und geeignete Maßnahmen ergriffen werden, um potentielle Informationssicherheitsvorfälle zu bewerten.	SEW-EURODRIVE überwacht kontinuierlich Netzwerke, Systeme und Anwendungen auf anomales Verhalten und analysiert Auffälligkeiten, um potenzielle Informationssicherheitsvorfälle gezielt zu erkennen und zu bewerten. Die Sicherheitsüberwachung und Incident-Bewertung wird dabei unter anderem durch externe Dienstleister unterstützt.
8.17	Uhrensynchronisation	Die Uhren der von der Organisation verwendeten Informationsverarbeitungssysteme sollten mit zugelassenen Zeitquellen synchronisiert werden.	Als externe Zeitquelle nutzt SEW-EURODRIVE öffentlich verfügbare Zeitserver. Intern steht ein NTP-Dienst über einen speziellen Server bereit, von dem sich Geräte synchronisieren.
8.18	Gebrauch von Hilfsprogrammen mit privilegierten Rechten	Der Gebrauch von Hilfsprogrammen, die fähig sein können, System- und Anwendungsschutzmaßnahmen zu umgehen, sollte eingeschränkt und streng überwacht werden.	SEW-EURODRIVE hat auf den Clients ein Least-Privilege-Konzept umgesetzt. Nutzer:innen verfügen standardmäßig nicht über Administratorrechte, können diese jedoch bei Bedarf anfordern. Alle Zugriffe werden serverseitig protokolliert. Im industriellen Umfeld wird überwiegend mit Servicekonten gearbeitet, die ohne Adminrechte auskommen.
8.19	Installation von Software auf Systemen im Betrieb	Es sollten Verfahren und Maßnahmen umgesetzt werden, um die Installation von Software auf Betriebssystemen sicher zu verwalten.	Bestimmte Software ist fester Bestandteil des Firmenauftritts von SEW-EURODRIVE. Zusätzliche Anwendungen werden zentral verteilt. Darüber hinaus wurden technische Maßnahmen implementiert, um die Installation potenziell schädlicher Software zu verhindern.
8.20	Netzwerksicherheit	Netzwerke und Netzwerkgeräte sollten gesichert, verwaltet und kontrolliert werden, um Informationen in Systemen und Anwendungen zu schützen.	Der Zugriff auf Netzwerkkomponenten ist ausschließlich geschulten internen Mitarbeitenden mit administrativen Berechtigungen vorbehalten. Diese Personen sind speziell autorisiert und verfügen über die erforderliche Fachkompetenz, um sicherheitsrelevante Aufgaben verantwortungsvoll auszuführen. Alle Netzwerkgeräte und -systeme werden gesichert und kontinuierlich hinsichtlich Verfügbarkeit, Telemetrie und Compliance überwacht. So wird die Integrität und Sicherheit der Informationen in den Systemen und Anwendungen von SEW-EURODRIVE jederzeit gewährleistet.
8.21	Sicherheit von Netzwerkdiensten	Sicherheitsmechanismen, Dienstgüte und Dienstanforderungen für Netzwerkdienste sollten ermittelt, umgesetzt und überwacht werden.	Die Sicherheitsmechanismen für Netzwerkdienste von SEW-EURODRIVE werden regelmäßig getestet, um ihre Wirksamkeit und Zuverlässigkeit sicherzustellen. Die Ergebnisse dieser Tests werden systematisch dokumentiert und bilden die Grundlage für kontinuierliche Verbesserungen. Die Dienstgüte sowie die spezifischen Anforderungen werden von den zuständigen Fachbereichen definiert und in enger Abstimmung mit der IT-Abteilung technisch umgesetzt. Zur Einhaltung und Überwachung dieser Vorgaben erfolgt eine fortlaufende Kontrolle durch mehrere Monitoring-Systeme, die sowohl technische Parameter als auch Compliance-Aspekte erfassen und auswerten.
8.22	Trennung von Netzwerken	Informationsdienste, Benutzer und Informationssysteme sollten in Netzwerken der Organisation gruppenweise voneinander getrennt gehalten werden.	SEW-EURODRIVE führt eine umfassende Risikobewertung einzelner IT-Assets durch und ermöglicht deren dediziertes Hosting in zugewiesenen Netzwerksegmenten. Es erfolgt eine klare Trennung zwischen internen und externen Netzwerken sowie zwischen zentral verwalteten und dezentral verwalteten Geräten auf globaler Ebene. Zum Einsatz kommen Technologien wie Firewalls und Routing über Gateways. Operativ werden die Zuordnung von Usern zu IP-Adressen sowie die gezielte Bewertung aller Verbindungen umgesetzt.
8.23	Webfilterung	Der Zugang zu externen Websites sollte verwaltet werden, um die Gefährdung durch bösartige Inhalte zu verringern.	Zur Absicherung des Internetzugangs setzt SEW-EURODRIVE verschiedene Sicherheitsmechanismen ein, darunter Firewalls, DNS-Security und erweiterte Antivirus-Funktionen. Zusätzlich wird für aus E-Mails geöffnete URLs ein Browser-Sandboxing verwendet.
8.24	Verwendung von Kryptographie	Es sollten Regeln für den wirksamen Einsatz von Kryptographie, einschließlich der Verwaltung kryptographischer Schlüssel, festgelegt und umgesetzt werden.	Die Regeln zum Umgang mit Kryptografie sind Bestandteil der Kryptografie-Richtlinie von SEW-EURODRIVE. Ein zentrales Element für die technische Umsetzung kryptografischer Verfahren bilden mehrere interne Zertifikatsinfrastrukturen.

ISO/IEC 27002:2022	Maßnahmenname ISO/IEC 27002:2022	Maßnahmenbeschreibung	Unser Statement
8.25	Lebenszyklus einer sicheren Entwicklung	Regeln für die sichere Entwicklung von Software und Systemen sollten festgelegt und angewendet werden.	Die technischen und organisatorischen Vorgaben sind unter anderem in der Arbeitsanweisung zu DevSec bei SEW-EURODRIVE definiert und werden eingehalten.
8.26	Anforderungen an die Anwendungssicherheit	Die Anforderungen an die Informationssicherheit sollten bei der Entwicklung oder Beschaffung von Anwendungen ermittelt, spezifiziert und genehmigt werden.	Die technischen und organisatorischen Vorgaben sind unter anderem in der Arbeitsanweisung zu DevSec sowie im Cloud-Enablement-Prozess von SEW-EURODRIVE definiert und werden eingehalten.
8.27	Sichere Systemarchitektur und technische Grundsätze	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme sollten festgelegt, dokumentiert, aktuell gehalten und bei allen Entwicklungsaktivitäten eines Informationssystems angewendet werden.	SEW-EURODRIVE hat Sicherheitsgrundsätze für das konzeptionelle Lösungsdesign definiert und verfolgt eine produktorientierte Defense-in-Depth-Strategie. Die Zugriffe und die Konfiguration aller Systeme richten sich nach den Prinzipien „Need-to-Know“ und „Least Privilege“.
8.28	Sicheres Coding	Bei der Softwareentwicklung sollten die Grundsätze der sicheren Kodierung angewandt werden.	Die technischen und organisatorischen Vorgaben sind unter anderem in der Arbeitsanweisung zu DevSec sowie in den Secure-Coding-Empfehlungen von SEW-EURODRIVE definiert und werden eingehalten.
8.29	Sicherheitsprüfung bei Entwicklung und Abnahme	Sicherheitsprüfverfahren sollten definiert und in den Entwicklungslebenszyklus integriert werden.	Die technischen und organisatorischen Vorgaben sind unter anderem in der Arbeitsanweisung zu DevSec bei SEW-EURODRIVE definiert und werden eingehalten. Zusätzlich wird der Code technisch auf Schwachstellen geprüft.
8.30	Ausgegliederte Entwicklung	Die Organisation sollte die Aktivitäten im Zusammenhang mit der ausgelagerten Systementwicklung leiten, überwachen und überprüfen.	Ausgegliederte Entwicklungen werden unter organisatorischen Vorgaben der SEW-EURODRIVE durchgeführt und beim Einspielen in Systeme von SEW-EURODRIVE überpüft.
8.31	Trennung von Entwicklungs-, Prüf- und Produktionsumgebungen	Entwicklungs-, Prüf- und Produktionsumgebungen sollten getrennt und gesichert werden.	Die Umgebungen für Entwicklung (D-Systeme), Qualitätssicherung (Q-Systeme) und Produktion (P-Systeme) sind so voneinander getrennt, dass nicht autorisierte Änderungen und Zugriffe auf die Produktivumgebung verhindert werden. Dafür gelten bei SEW-EURODRIVE die Entwicklungsrichtlinien sowie Richtlinien zum Transportwesen und zum Change-Management.
8.32	Änderungssteuerung	Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen sollten Gegenstand von Änderungsmanagementverfahren sein.	Änderungen an Informationsverarbeitungseinrichtungen und Informationssystemen bei SEW-EURODRIVE werden nach den Verfahren des Änderungsmanagements gemäß ITIL (Information Technology Infrastructure Library) und ISO 20000 umgesetzt.
8.33	Prüfinformationen	Die Prüfinformationen sollten in geeigneter Weise ausgewählt, geschützt und verwaltet werden.	Die organisatorischen Vorgaben sind in internen Arbeitsanweisungen zu DevSec-Testdaten bei SEW-EURODRIVE definiert und werden eingehalten.
8.34	Schutz der Informationssysteme während der Überwachungsprüfung	Auditprüfungen und andere Sicherheitstätigkeiten, die eine Beurteilung der betrieblichen Systeme beinhalten, sollten zwischen dem Prüfer und dem zuständigen Management geplant und vereinbart werden.	Mehrmals jährlich lässt das Unternehmen abgestimmte Systeme bei SEW-EURODRIVE von externen Expert:innen auf Schwachstellen prüfen. Die Ergebnisse werden mit Handlungsempfehlungen dokumentiert, bearbeitet und bei Bedarf durch Wiederholungstests zur Überprüfung der Maßnahmen kontrolliert.

2270 7247 / 0326

Weitere Informationen unter
www.sew-eurodrive.de/cybersecurity

SEW-EURODRIVE GmbH & Co KG
Ernst-Blickle-Str. 42
76646 Bruchsal
T 07251 75-0
F 07251 75-1970
sew@sew-eurodrive.de
www.sew-eurodrive.de