Sicherheitskonzept

Stand: 30.12.2025
Version: 1.2.1

Datensicherheit

Technische und organisatorische Maßnahmen / Controls

BEX /einfach/grenzenlos

Verfasser:	Vanessa Kleiber
Verwendung:	~~Intern~~ | ~~Partner~~ | Öffentlich
Status:	~~Entwurf~~ | Final

Inhaltsverzeichnis

1 Einleitung

Dieses Dokument beschreibt die technischen und organisatorischen Sicherheitsmaßnahmen der BEX zum Schutz von Informationen und Daten. Die beschriebenen Maßnahmen orientieren sich am Stand der Technik, an den Anforderungen der ISO/IEC 27001 sowie an den gesetzlichen Vorgaben, insbesondere der DSGVO (Art. 32). Umfang und Ausgestaltung richten sich nach Schutzbedarf, Zweck der Verarbeitung und betrieblichem Kontext.

Die IT-Systeme der BEX werden beim Mutterkonzern, der AEB SE, betrieben. Die dort umgesetzten Sicherheitsmaßnahmen sind Bestandteil dieses Sicherheitskonzepts und gelten übergreifend für alle Kunden, sofern keine abweichenden Vereinbarungen bestehen.
Das Sicherheitskonzept der AEB SE ist versioniert und öffentlich im Trust Center einsehbar:
https://www.aeb.com/sicherheitskonzept-aeb.pdf

Standortspezifische Ergänzungen der BEX, insbesondere für den Standort Aalen, werden in den jeweiligen Abschnitten berücksichtigt.

2 Allgemeines

Zertifizierung

Die BEX sowie auch die AEB sind nach ISO/IEC 27001 zertifiziert.

Die Wirksamkeit des Informationssicherheitsmanagementsystems wird durch regelmäßig stattfindende Überwachungsaudits unabhängiger externer Stellen überprüft.

Zertifikat BEX, Zertifikat AEB

Qualitätssicherung

Qualitätssicherung ist fester Bestandteil der Entwicklung, des Betriebs und des Supports. Prozesse orientieren sich am PDCA-Zyklus. Neue Funktionen werden fachlich, technisch und hinsichtlich der Nutzbarkeit geprüft. Wartung und Service werden kontinuierlich auf Grundlage von Rückmeldungen und Betriebserfahrungen weiterentwickelt.

Im Bereich der Applikationen werden dabei nicht nur Funktions- sondern auch Usability-Tests durchgeführt. Jede Neuerung wird dabei mehrfach geprüft und abgenommen. Die Aktualität fachlicher Anforderungen wird ständig verfolgt und umgesetzt. Im engen Kundenkontakt wird Wartung und Service bewertet und optimiert. Die Arbeitsweise ist service- und prozessorientiert.

3 Datenschutz - Technische und organisatorische Maßnahmen (TOMs)

Der betriebliche Datenschutzbeauftragte überwacht die Einhaltung der datenschutzrechtlichen Anforderungen.
Die nachfolgende Zuordnung der TOMs erfolgt auf Grundlage der geltenden Datenschutz- und Sicherheitsanforderungen.

Die nachfolgenden Maßnahmen sind den Schutzzielen Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit zugeordnet.

Zutrittskontrolle
Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Der Zutritt zu den Geschäftsräumen der BEX ist durch ein Zutrittskontrollsystem geregelt. Zutrittsrechte werden ausschließlich autorisierten Personen erteilt. Die Ausgabe und Rücknahme von Schlüsseln oder Transpondern erfolgt nachvollziehbar.

Besucher erhalten nur in Begleitung Zugang. Alle Besucher werden in einem Besucherprotokoll dokumentiert.

Externe Personen, die über einen längeren Zeitraum in den Räumen tätig sind, unterliegen vertraglichen Regelungen zur Vertraulichkeit und zum Datenschutz.

Zugangskontrolle
Um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Automatische Sperrung der Arbeitsplatzrechner.

Die Systeme besitzen hohe Komplexitätsvoraussetzungen für Passwörter. Dafür wird kein regelmäßiger Passwortwechsel verlangt. Dabei wird systemseitig auf die Eignung (Mindestanforderung: 15 Zeichen, a-z, A-Z, 0-9, Sonderzeichen) geachtet und verhindert, dass das gleiche Passwort wiederverwendet werden kann.
Zusätzlich wird in Systemen, wo möglich, eine Zwei-Faktor-Authentifizierung eingesetzt.

Mobile Endgeräte sind verschlüsselt (mindestens XTS-AES-128).

Um die Systeme der BEX vor Viren- und Malwarebefall zu schützen, werden auf zentralen und dezentralen Systemen marktübliche Schutzprogramme eingesetzt.

Während des mobilen Arbeitens (z. B. Hotels, Veranstaltungen, Messen) ist sichergestellt, dass der Mitarbeiter nur mittels persönlicher Zugangskennung via VPN auf die Systeme zugreifen kann.

Die Einrichtung und der Entzug von Rollen und Berechtigungen erfolgen nur auf Anweisung hierzu besonders autorisierter Personen. Dies wird dokumentiert und in regelmäßigen Abständen überprüft.

Zugriffskontrolle
Um sicherzustellen, dass nur berechtigte Personen auf die Daten zugreifen und diese nicht unbefugt lesen, kopieren, verändern oder löschen können.

Das Grundprinzip der Zugriffskontrollleitlinie ist, dass der Zugang zu allen Systemen, Diensten und Informationen verboten und technisch unterbunden wird, solange er nicht einzelnen Benutzern oder Benutzergruppen ausdrücklich erlaubt wird.

Mitarbeiter werden bei Einstellung zu Vertraulichkeit verpflichtet.

Der Einsatz generischer Benutzerkonten ist auf technisch notwendige Sonderfälle beschränkt und erfolgt ohne Zugriff auf kundenbezogene Daten.

Papiergebundene sensible Informationen werden nach Sicherheitsstufe P-4 vernichtet. Datenträger werden vor Entsorgung datenschutzkonform gelöscht oder zerstört.

Trennungskontrolle
Um zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können.

Entwicklungs- und Testumgebungen sind organisatorisch und technisch von Produktivsystemen getrennt und verwenden Testdaten.

Die Trennung von Kundendaten ist softwareseitig umgesetzt. Jeder Kunde verfügt über eine eindeutige technische Kennung, über die Zugriffe und Datenzuordnung erfolgen. Ein Zugriff auf Daten anderer Kunden ist technisch ausgeschlossen.

Pseudonymisierung und Verschlüsselung
Um Sorge zu tragen, dass eine Rückbeziehbarkeit von Daten auf (natürliche) Personen zumindest eingeschränkt ist.

Privacy-by-Design- und Privacy-by-Default-Prinzipien werden bei der Entwicklung berücksichtigt. Client-Festplatten sind standardmäßig verschlüsselt. Mobile Geräte werden zentral verwaltet (MDM), inklusive der Möglichkeit zum Remote-Wipe.

Eine Pseudonymisierung personenbezogener Daten ist derzeit nicht vorgesehen. Die verarbeiteten personenbezogenen Daten sind überwiegend geschäftlicher Natur; aus Gründen der Nachvollziehbarkeit und Revisionssicherheit überwiegt das berechtigte Interesse an einer eindeutigen Zuordnung.

Weitergabekontrolle
Um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Elektronische Übertragungen personenbezogener Daten erfolgen verschlüsselt.

Bei Systemübernahmen („Transition“) werden die Datenträger verschlüsselt übergeben. Die Übermittlung von Zugangsinformationen erfolgt getrennt und abgestimmt.

Personenbezogene Daten werden nach Abschluss eines Auftrags regelmäßig gelöscht. Eine längere Speicherung erfolgt nur, wenn Aufbewahrungspflichten bestehen oder aber eine andere Rechtsgrundlage zu finden ist.

Eingabekontrolle
Um zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Eingaben, Änderungen und Löschungen werden in den Produkten der BEX protokolliert und nachvollziehbar Nutzern zugeordnet.

Interne Systeme, die personenbezogene Stammdaten verarbeiten, führen eine Aufzeichnung sämtlicher Eingaben, Änderungen und Löschungen. Dadurch lässt sich jederzeit nachvollziehen, welche Daten bearbeitet wurden und durch welchen Benutzer die Aktionen erfolgt sind.

Die Anwendungen arbeiten mit individuellen, personalisierten Benutzerkonten, um die Nachvollziehbarkeit der Zugriffe sicherzustellen.

Verfügbarkeitskontrolle
Um zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind

Personenbezogene Daten werden auf zentralen Serversystemen im Rechenzentrum der AEB SE betrieben.
Weitere Informationen zum Betrieb und zu Verfügbarkeitsmaßnahmen sind im Sicherheitskonzept der AEB SE dokumentiert: https://www.aeb.com/sicherheitskonzept

Auftragskontrolle
Um zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können.

Subunternehmer werden sorgfältig ausgewählt, vertraglich verpflichtet und regelmäßig überprüft.
Eine Übersicht der eingesetzten Subunternehmer ist öffentlich verfügbar:
https://bex.ag/static_downloads/BEX_Subunternehmer.pdf

4 Informationssicherheits-Maßnahmen ISO 27001:2024 - Annex A

A.5 Organisatorische Maßnahmen

Die Informationssicherheit ist organisatorisch verankert und wird unternehmensweit nach anerkannten Standards gesteuert. Alle organisatorischen Sicherheitsmaßnahmen gemäß ISO/IEC 27002:2024 Annex A.5 – A8 sind implementiert, dokumentiert und operativ wirksam.

Governance und Richtlinien

Die Informationssicherheitspolitik ist durch die Unternehmensleitung formell verabschiedet und bildet die Grundlage sicherheitsrelevanter Entscheidungen. Sie wird regelmäßig überprüft und an technische Entwicklungen, aktuelle Bedrohungen sowie gesetzliche und regulatorische Vorgaben angepasst. Mitarbeitende werden regelmäßig geschult und verpflichten sich zur Einhaltung der Richtlinien.

Rollen, Verantwortlichkeiten und Aufgabentrennung

Rollen, Verantwortlichkeiten und Zuständigkeiten im Bereich Informationssicherheit sind klar definiert, dokumentiert und organisatorisch verankert. Entscheidungs-, Kontroll- und Eskalationswege sind verbindlich geregelt, sodass sicherheitsrelevante Aufgaben eindeutig zugeordnet, umgesetzt und überwacht werden.

Durch organisatorische und technische Maßnahmen ist eine wirksame Trennung kritischer Aufgaben, insbesondere zwischen Entwicklung, Freigabe und Betrieb, umgesetzt. Diese Aufgabentrennung reduziert das Risiko von Fehlbedienungen, Interessenkonflikten und Missbrauch.

Risikomanagement und Einbindung von Lieferanten

Informationssicherheitsrisiken werden systematisch identifiziert, bewertet, dokumentiert und behandelt. Dies umfasst auch Risiken aus der Zusammenarbeit mit Lieferanten, Dienstleistern und weiteren externen Parteien. Für externe Partner gelten definierte Sicherheitsanforderungen, die vertraglich festgelegt, regelmäßig überprüft und bei Bedarf angepasst werden. Dadurch ist der Schutz von Kundeninformationen entlang der gesamten Lieferkette sichergestellt.

Umgang mit Sicherheitsvorfällen

Strukturierte Prozesse zur Meldung, Bewertung, Behandlung und Nachverfolgung von Informationssicherheitsvorfällen sind implementiert. Zuständigkeiten, Eskalationsmechanismen und Kommunikationswege sind klar definiert. Sicherheitsvorfälle werden dokumentiert, analysiert und mit geeigneten Maßnahmen zur Schadensbegrenzung und Ursachenvermeidung adressiert. Erkenntnisse fließen systematisch in die Weiterentwicklung der Sicherheitsorganisation ein.

Rechtliche, regulatorische und vertragliche Anforderungen

Rechtliche, regulatorische und vertragliche Anforderungen in Bezug auf Informationssicherheit und Datenschutz werden systematisch erfasst, bewertet und eingehalten. Die Umsetzung relevanter Vorgaben, insbesondere im Hinblick auf Datenschutz und Kundenanforderungen, wird regelmäßig überprüft und dokumentiert. Dadurch wird sichergestellt, dass Kundenanforderungen sowie gesetzliche Verpflichtungen zuverlässig erfüllt werden.

Notfall- und Wiederanlaufmanagement

Für wesentliche Geschäftsprozesse bestehen dokumentierte Notfall- und Wiederanlaufpläne. Backup-Konzepte, Redundanzen und Wiederherstellungsverfahren sind implementiert und werden regelmäßig getestet. Die Betriebsfähigkeit kritischer Systeme und Services wird auch im Störungsfall gewährleistet.

A.6 – Personalsicherheit

Mitarbeitende sind ein zentraler Faktor für die Informationssicherheit. Durch klar definierte Prozesse, verbindliche Verpflichtungen, strukturierte Rollensteuerung und kontinuierliche Sensibilisierung wird das Risiko von Sicherheitsvorfällen durch menschliche Fehler, Fahrlässigkeit oder Missbrauch wirksam reduziert.

Sicherheitsüberprüfung bei Neueinstellungen

Vor der Einstellung werden, abhängig von der jeweiligen Position und dem Schutzbedarf, Qualifikation, Identität, Integrität und Vertrauenswürdigkeit von Bewerbenden geprüft. Die Durchführung erfolgt im Rahmen der geltenden rechtlichen Vorgaben.

Alle Mitarbeitenden unterzeichnen Vertraulichkeits- und Sicherheitsvereinbarungen und verpflichten sich zur Einhaltung der geltenden Informationssicherheitsrichtlinien und internen Regelwerke.

Vertrags- und Verpflichtungsregelungen

Arbeitsverträge und begleitende Vereinbarungen enthalten verbindliche Regelungen zu Informationssicherheit, Datenschutz, Vertraulichkeit und zum Schutz geschäftskritischer Informationen.
Diese Verpflichtungen gelten sowohl während des Beschäftigungsverhältnisses als auch über dessen Beendigung hinaus.

Onboarding, Rollenwechsel und Offboarding

Die Vergabe, Änderung und der Entzug von Rollen und Zugriffsrechten erfolgen über definierte, dokumentierte Prozesse mit klar benannten Verantwortlichkeiten und Genehmigungsstufen.

Berechtigungen werden nach dem Need-to-know-Prinzip vergeben und regelmäßig überprüft.
Bei Rollenwechseln oder dem Ausscheiden von Mitarbeitenden werden Zugriffsrechte zeitnah angepasst oder entzogen, Unternehmensressourcen zurückgeführt und relevante Sicherheitsmaßnahmen abgeschlossen.

Verantwortungsbewusstsein und verbindliches Verhalten

Alle Mitarbeitenden sind zur Einhaltung der geltenden Informationssicherheitsvorgaben verpflichtet. Dies umfasst insbesondere die Informationssicherheitspolitik, IT-Nutzungsrichtlinien, Datenschutzregelungen sowie weitere relevante interne Vorgaben.
Verstöße gegen Sicherheitsregelungen unterliegen definierten disziplinarischen Maßnahmen und werden nachvollziehbar dokumentiert.

Kontinuierliche Sensibilisierung und Schulung

Regelmäßige Schulungs- und Awareness-Programme sind etabliert, um ein dauerhaft hohes Sicherheitsbewusstsein sicherzustellen. Schulungen decken unter anderem folgende Themen ab:

- Social Engineering und Phishing
- Passwort- und Zugangssicherheit
- Datenschutz und Schutz personenbezogener Daten
- Sicherer Umgang mit sensiblen und vertraulichen Informationen
- Sicherheitsanforderungen im Arbeitsalltag und im mobilen Arbeiten

Neue Mitarbeitende erhalten im Rahmen des Onboardings eine verpflichtende Einführung in relevante Sicherheits- und Datenschutzanforderungen.

Sicheres Arbeiten und Remote-Work-Regelungen

Für mobiles Arbeiten und Remote-Zugriffe gelten definierte Sicherheitsvorgaben. Technische und organisatorische Maßnahmen stellen sicher, dass Informationen auch außerhalb der Unternehmensstandorte geschützt sind. Mitarbeitende sind verpflichtet, Sicherheitsanforderungen auch im Mobiles Arbeiten oder bei externen Tätigkeiten einzuhalten.

Meldung von Sicherheitsereignissen
Mitarbeitende sind aktiv in das Sicherheitsmanagement eingebunden und kennen die vorgesehenen Meldewege für Sicherheitsereignisse und verdächtige Aktivitäten.
Meldungen können niedrigschwellig, vertraulich und ohne negative Konsequenzen erfolgen. Hinweise und Vorfälle werden strukturiert bewertet und in die kontinuierliche Verbesserung der Sicherheitsmaßnahmen einbezogen.

Schutz vor Insider-Risiken und Missbrauch

Maßnahmen zur Reduzierung von Insider-Risiken sind implementiert. Dazu zählen unter anderem das Vier-Augen-Prinzip, Aufgabentrennung, Zugriffsbeschränkungen, Monitoring-Mechanismen sowie regelmäßige Überprüfungen kritischer Berechtigungen.

A.7 – Asset-Management und Physische Sicherheit

Informationswerte (Assets) werden systematisch identifiziert, klassifiziert, dokumentiert und über ihren gesamten Lebenszyklus hinweg geschützt. Dies umfasst physische und digitale Informationswerte, IT-Systeme, Datenträger sowie Kundeninformationen. Zuständigkeiten für Assets sind klar definiert und Schutzmaßnahmen sind risikobasiert umgesetzt.

Asset-Inventarisierung und Verantwortlichkeiten

Alle relevanten Informationswerte werden in einem zentralen Asset-Verzeichnis geführt. Eigentümer und Verantwortliche für Assets sind benannt. Der Status, Standort, Schutzbedarf und Lebenszyklus der Assets werden dokumentiert und regelmäßig überprüft, um eine vollständige Nachvollziehbarkeit sicherzustellen.

Klassifizierung und Schutz von Informationen

Informationen werden gemäß ihrem Schutzbedarf klassifiziert. Auf dieser Grundlage sind abgestufte organisatorische, technische und physische Schutzmaßnahmen definiert und implementiert, um Vertraulichkeit, Integrität und Verfügbarkeit sicherzustellen.
Die Klassifizierung wird bei Erstellung, Verarbeitung, Speicherung, Übertragung und Archivierung konsequent berücksichtigt.

Kontrolle des physischen Zugangs

Geschäftsräume, Serverräume und besonders schützenswerte Bereiche sind durch elektronische Zutrittssysteme, Schließsysteme und Besuchermanagement gesichert.
Zutritt erhalten ausschließlich autorisierte Personen. Zutrittsrechte werden regelmäßig überprüft, dokumentiert und bei Bedarf angepasst oder entzogen. Besucher werden registriert, begleitet und kontrolliert.

Schutz vor Umwelt- und Störfaktoren

Technische Infrastrukturen und Rechenzentren sind gegen physische Risiken abgesichert. Dazu zählen redundante Stromversorgung, Brandschutzsysteme, Klimatisierung, Temperatur- und Feuchtigkeitsüberwachung, Alarmanlagen sowie Videoüberwachung.
Diese Maßnahmen schützen vor Feuer, Wasser, Stromausfällen, Umweltgefahren, Sabotage und unbefugtem Zugriff und sichern den stabilen Betrieb kritischer Systeme.

Geräteschutz, Nutzung und sichere Entsorgung

IT-Geräte und Datenträger werden physisch gesichert, inventarisiert und so betrieben, dass Manipulation und Diebstahl verhindert werden. Mobile Endgeräte sind verschlüsselt und durch technische Sicherheitsmechanismen geschützt.

Backups werden gesichert gespeichert und vor unbefugtem Zugriff geschützt.
Ausgemusterte Hardware und Datenträger werden gemäß definierten, dokumentierten Verfahren datenschutzkonform gelöscht oder zerstört. Die ordnungsgemäße Entsorgung wird nachvollziehbar dokumentiert.

Sichere Nutzung von Arbeitsplätzen und Clear-Desk-Regeln

Arbeitsplätze unterliegen verbindlichen Clean-Desk- und Clean-Screen-Regeln. Vertrauliche Informationen werden vor unbefugter Einsicht geschützt.
Technische Maßnahmen wie automatische Bildschirmsperren, Sitzungs-Timeouts und Zugangssicherungen sind umgesetzt, um Informationsabflüsse zu verhindern.

Umgang mit mobilen Assets und externen Arbeitsorten

Für mobile Geräte und Mobiles Arbeiten gelten definierte Sicherheitsvorgaben. Der Schutz von Informationen wird auch außerhalb der Unternehmensstandorte durch Verschlüsselung, Zugriffskontrollen und verbindliche Nutzungsrichtlinien sichergestellt.

Sichere Lagerung, Transport und Archivierung

Physische und digitale Informationswerte werden geschützt gelagert, sicher transportiert und revisionssicher archiviert. Zugriff auf Archive und sensible Datenträger ist beschränkt, protokolliert und regelmäßig überprüft.

Schutz vor Verlust, Diebstahl und unbefugter Nutzung

Maßnahmen zur Verhinderung von Verlust, Diebstahl, Sabotage und Missbrauch von Assets sind implementiert. Dazu zählen Kennzeichnung, Zugriffskontrollen, Monitoring, Alarmmechanismen sowie definierte Melde- und Reaktionsprozesse bei Verlust oder Sicherheitsvorfällen.

A.8 – Zugriffskontrolle und technische Maßnahmen

Technische und organisatorische Maßnahmen zur Zugriffskontrolle sind implementiert, um sicherzustellen, dass der Zugriff auf Informationen, Systeme und Anwendungen ausschließlich autorisierten Personen entsprechend ihrer Rolle und Aufgabe gewährt wird. Zugriffsrechte folgen dem Prinzip der minimalen Rechtevergabe (Least Privilege) und werden nachvollziehbar verwaltet.

Identitäts- und Zugriffsmanagement

Ein zentrales Identitäts- und Berechtigungsmanagement steuert die Vergabe, Änderung und den Entzug von Benutzerrechten. Rollenbasierte Zugriffskonzepte stellen sicher, dass Mitarbeitende ausschließlich auf die für ihre Tätigkeit erforderlichen Ressourcen zugreifen können. Berechtigungen sind dokumentiert, genehmigungspflichtig und revisionsfähig.

Endpunkt- und Gerätemanagement

Alle Endgeräte werden zentral verwaltet, sicher konfiguriert und regelmäßig aktualisiert. Sicherheitsrichtlinien werden technisch durchgesetzt, um den Schutz von Unternehmens- und Kundendaten sicherzustellen.
Der Zugriff auf interne Ressourcen ist ausschließlich autorisierten, konformen und vertrauenswürdigen Geräten gestattet.

Regelmäßige Überprüfung und Kontrolle von Zugriffsrechten

Zugriffsrechte werden in festgelegten Intervallen überprüft, um ihre Notwendigkeit, Angemessenheit und Aktualität sicherzustellen. Veraltete oder nicht mehr benötigte Berechtigungen werden zeitnah entzogen.
Diese Maßnahmen reduzieren das Risiko unbefugter Zugriffe auf kundenbezogene und geschäftskritische Informationen.

Privilegierte Zugänge und Administrationskonten

Administrative und besonders privilegierte Konten unterliegen strengen Genehmigungs-, Kontroll- und Überwachungsprozessen. Der Einsatz privilegierter Zugriffe ist auf das erforderliche Minimum beschränkt.
Administrative Aktivitäten werden protokolliert, überwacht und regelmäßig ausgewertet, um Missbrauch, Fehlkonfigurationen und Sicherheitsvorfälle frühzeitig zu erkennen.

Sichere Authentisierung und Sitzungssteuerung

Moderne Authentisierungsmechanismen sind implementiert, darunter Multi-Faktor-Authentisierung, sichere Passwortrichtlinien, Schutz vor Brute-Force-Angriffen sowie zeitlich begrenzte Sitzungen.
Automatische Sperrmechanismen, Timeout-Regelungen und Wiederanmeldepflichten erhöhen den Schutz vor unbefugtem Zugriff.

Logging, Monitoring und Anomalieerkennung

Sicherheitsrelevante Ereignisse werden zentral protokolliert, korreliert und analysiert. Ein strukturiertes Monitoring erkennt ungewöhnliche Aktivitäten, Abweichungen und potenzielle Sicherheitsvorfälle frühzeitig.
Erkannte Auffälligkeiten werden bewertet, eskaliert und in Incident-Response-Prozesse überführt.

Schutz vor Schadsoftware und Bedrohungen

Mehrstufige Schutzmaßnahmen gegen Malware sind implementiert, einschließlich moderner Endpoint-Protection-Lösungen, EDR-Systeme, E-Mail-Sicherheitsmechanismen und Web-Filter.
Signaturbasierte und verhaltensbasierte Erkennungsmethoden reduzieren das Risiko von Schadsoftware, Phishing und gezielten Angriffen.

Sichere Konfiguration und Systemhärtung

IT-Systeme, Server, Anwendungen und Netzkomponenten werden nach anerkannten Sicherheitsstandards gehärtet und sicher konfiguriert. Standardpasswörter, unnötige Dienste und unsichere Protokolle sind deaktiviert.
Konfigurationsänderungen unterliegen definierten Freigabe- und Dokumentationsprozessen.

Sichere Softwareentwicklung und Umgebungs-Trennung

Sicherheitsanforderungen sind in den Softwareentwicklungsprozess integriert. Dazu gehören Bedrohungsanalysen, Code-Reviews, automatisierte Sicherheitstests sowie definierte Freigabeprozesse.
Entwicklungs-, Test- und Produktionsumgebungen sind organisatorisch und technisch voneinander getrennt, um Risiken durch unbeabsichtigte Änderungen oder Datenabflüsse zu vermeiden.

Patch- und Schwachstellenmanagement

Sicherheitsupdates und Patches werden strukturiert bewertet, priorisiert und zeitnah eingespielt. Schwachstellen werden regelmäßig identifiziert, analysiert und behandelt.
Kritische Sicherheitslücken werden risikobasiert adressiert und nachvollziehbar dokumentiert.

Backup, Wiederherstellung und Redundanz

Regelmäßige Backups geschäftskritischer Daten und Systeme werden erstellt, geschützt und überwacht. Wiederherstellungsverfahren sind dokumentiert und werden regelmäßig getestet.
Redundante Systeme und Verfügbarkeitsmechanismen sichern den stabilen Betrieb und minimieren Ausfallzeiten.

Kryptografische Maßnahmen

Daten werden sowohl im Ruhezustand als auch bei der Übertragung verschlüsselt. Kryptografische Verfahren entsprechen anerkannten Sicherheitsstandards.
Schlüssel werden nach definierten Sicherheitsrichtlinien erzeugt, gespeichert, verwaltet und ausgetauscht. Der Zugriff auf kryptografische Schlüssel ist streng kontrolliert und protokolliert.

Netzwerksicherheit und Segmentierung

Netzwerke sind segmentiert und durch Firewalls, Intrusion-Detection- und Prevention-Systeme sowie Zugriffskontrollen geschützt. Der Datenverkehr zwischen Netzzonen wird überwacht und auf das erforderliche Maß beschränkt.

5 Anhänge und Verweise

Titel des Anhangs / Verweis	Beschreibung

6 Änderungshistorie

Datum	Bearbeiter	Beschreibung der Änderung
30.04.2018	KLV, RIA	Anlage des Dokuments
18.08.2020	KLS, KLV	Überarbeitung
23.04.2021	KLV	Überprüfung der Aktualität
26.04.2022	KLV	Technische und organisatorische Maßnahmen überarbeitet
22.02.2023	KLV	Technische und organisatorische Maßnahmen überarbeitet
10.09.2024	KLV	Technische und organisatorische Maßnahmen überarbeitet
15.11.2024	KLS	Inhalt in aktuelles Dokumenten-Design überführt. Link für die Sub-unternehmer eingefügt.
30.12.2025	KLV	Überarbeitung / Aufnahme ISO27001:2024

Noch Fragen? Kein Problem!
Wir sind für Sie da:

Per E-Mail:

datenschutz@bex.ag

Telefonisch:

+49 7361 999 39 10

(Mo-Fr: 8-16 Uhr)

Oder jederzeit unter:

www.bex.ag

BEX Components AG

Gartenstraße 97

73430 Aalen