SWARCO

UMSETZUNG DER KRITIS-ANFORDERUNGEN

SWARCO | The Better Way. Every Day.

SWARCOs Leitgedanke ist es, die Lebensqualität zu verbessern, indem das Reisen sicherer, schneller, bequemer und umweltschonender gestaltet wird.

Mit mehr als fünf Jahrzehnten Branchenerfahrung produziert und liefert der österreichische Verkehrstechnologiekonzern eine breite Palette von Produkten, Systemen, Dienstleistungen und schlüsselfertigen Lösungen für Straßenmarkierung, urbanes und interurbanes Verkehrsmanagement, Parken und öffentlichen Verkehr. Kooperative Systeme, Infrastruktur-zu-Fahrzeug-Kommunikation, E-Mobilität und integrierte Softwarelösungen für die lebenswerte Stadt ergänzen das zukunftsorientierte Portfolio der Gruppe.

Über 5300 Verkehrsexpert(inn)en setzen sich ein, um gemeinsam mit allen Beteiligten der Verkehrsbranche den Übergang vom konventionellen Verkehrsmanagement zu Mehrwertdiensten für die Reisenden im digitalen Zeitalter zu gestalten.

SWARCOs Produkte, Systeme und Lösungen tragen in 80 Ländern zu mehr Verkehrssicherheit und intelligentem Verkehrsmanagement bei und erwirtschaften ein Umsatzvolumen von mehr als einer Milliarde Euro.

www.swarco.com

UMSETZUNG DER KRITIS-ANFORDERUNGEN BEI SWARCO

INHALT

1 Einleitung

Als Stadt, Kommune oder Gemeinde sind Sie Betreiber kritischer Infrastrukturen und haben per Gesetz Anforderungen an deren Sicherheit.

SWARCO ist Lieferant kritischer Infrastrukturen und hat in dieser Rolle die "Umsetzungsplan KRITIS Best Practice Empfehlungen" identifiziert sowie SWARCO-intern definiert und umgesetzt. Seit 2019 sind wir DIN EN ISO/IEC 27001:2017 zertifiziert und erfüllen hierüber nicht nur normative, sondern auch zusätzliche Kundenanforderungen an Lieferanten für kritische Infrastrukturen.

Um die Zusammenarbeit zu erleichtern, den unterschiedlichen Sicherheitsanforderungen unserer Kunden gerecht zu werden (abhängig von Branche, Schutzbedarf und Auswirkungspotential) und Ihnen einen Einblick in die SWARCO-intern umgesetzten UP KRITIS Best Practice Empfehlungen zu gewähren, fassen wir unser Verständnis der Umsetzung in diesem Dokument zusammen.

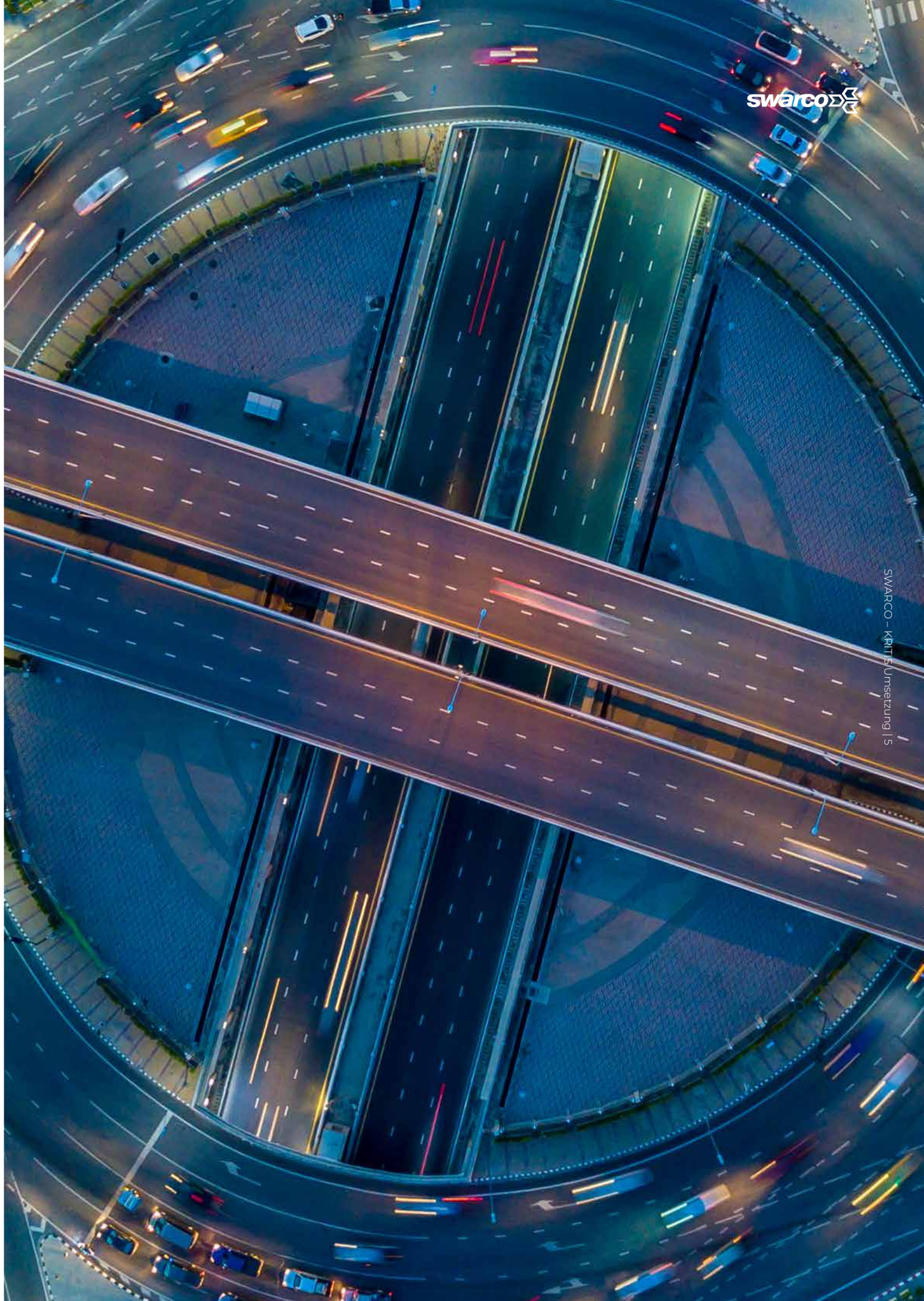
Wir verweisen in dieser Broschüre teils auf vertrauliche Richtlinien und Dokumentationen, deren aktive Umsetzung Sie als Kunde jederzeit in unserer Zentrale in Unterensingen einsehen können. Gemeinsam können wir dann Ihren individuellen Schutzbedarf ermitteln sowie dokumentieren und die wichtigsten Sicherheitsanforderungen definieren.

§ ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- 5.1 Führung und Verpflichtung
- 7.3 Bewusstsein
- A.5 Informationssicherheitsleitlinien
- A.7.2.1 Verantwortung des Managements

RELEVANTE DOKU

- LL_ISMS_Leitlinie_STS
- RL_ISMS_Personalsicherheit_STS



2 Anwendungsbereich

UNSER VERSTÄNDNIS

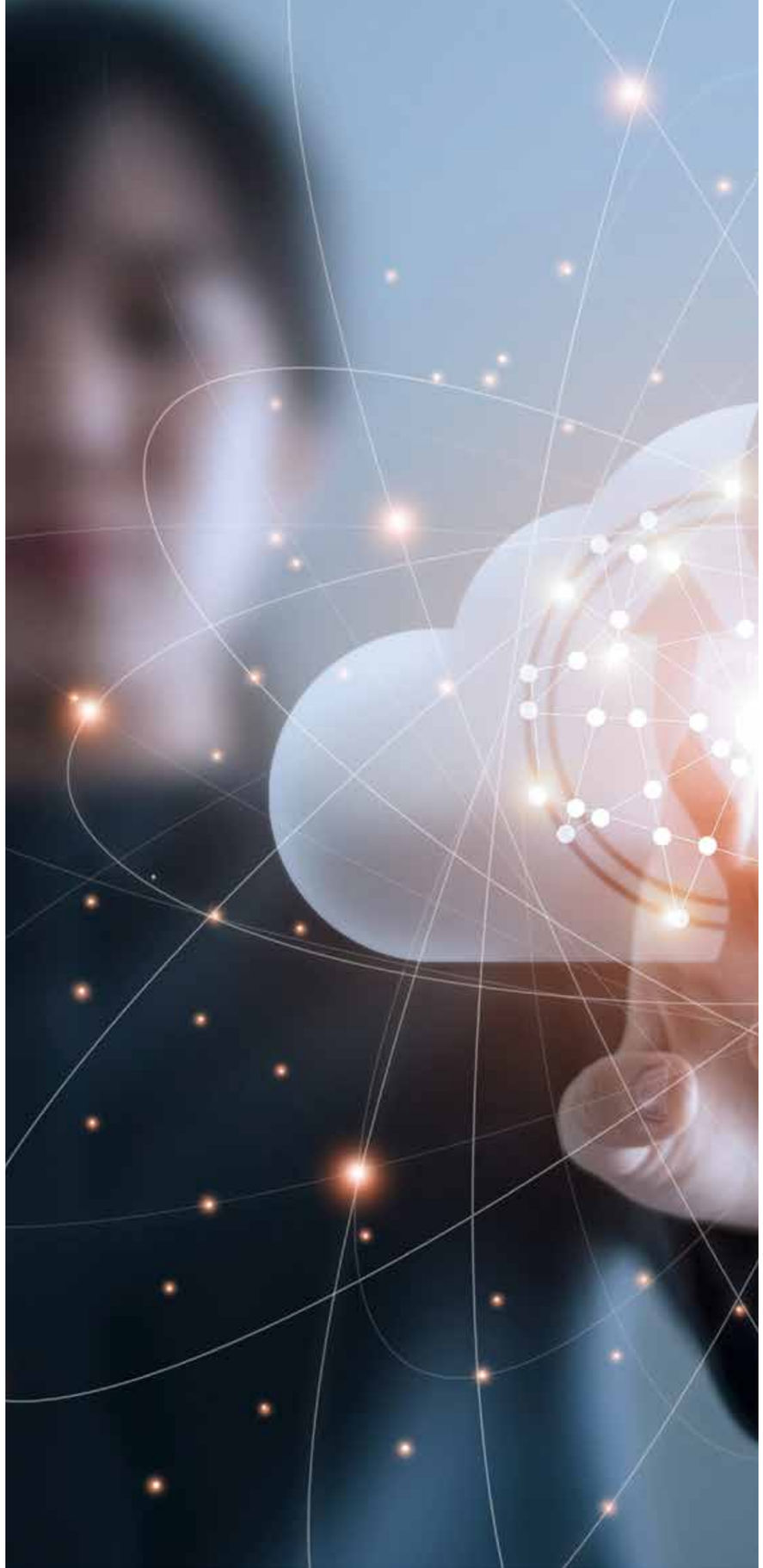
Da kritische Infrastrukturen unterschiedliche Sicherheitsanforderungen haben können, abhängig von der Branche, dem Schutzbedarf und dem Auswirkungspotential auf die Bevölkerung und das Land, legen wir gemeinsam mit den Kunden schriftlich fest, welche individuellen Sicherheitsanforderungen an unser Produkt angemessen, sinnvoll und anwendbar sind. Hierzu orientieren wir uns an den UP KRITIS Best Practice Empfehlungen. Bei Ausschluss bestimmter Sicherheitsanforderungen aus dem Anwendungsbereich dokumentieren und begründen wir diesen.

2.1. EIGENBETRIEB

UNSER UMGANG

Wir ermitteln mit Ihnen die Anforderungen, die Sie aus den folgenden Bereichen an uns stellen, auch wenn Sie den IT-Betrieb mit eigenem Personal verantworten:

- Vulnerability-Management (Schwachstellen-Management)
- Patch-Management
- Systemhärtung
- Fernzugang für Drittanbieter
- Mandantenadministration
- Anforderungen an die Softwareentwicklungsprozesse
- Einsatz von Kryptographischen Lösungen
- Dokumentation
- Benachrichtigung über sicherheitsrelevante Vorfälle
- Nicht-technische Sicherheit



2.2 BETRIEB MIT UNTERSTÜTZUNG DRITTER

UNSER UMGANG

Wir ermitteln mit Ihnen die weiterführenden Anforderungen aus folgenden Bereichen, die Sie an (dritte) Auftragnehmer stellen, die weiterführende Dienstleistungen ihres IT Betriebs erbringen:

- Informationssicherheitsprozesse / Informationssicherheitsmanagementsystem
- Zugriffsschutz und Berechtigungsvergabe
- Asset-Management
- Personalsicherheit (HR-Security)
- Physische Sicherheit und Zutrittsschutz
- Operationelle Informationssicherheits-Anforderungen (Netzwerksicherheit, Virenschutz, Logging & Monitoring, Backup & Restore, etc.)
- Sicherheit in Softwareentwicklung und Change-Prozessen / Änderungsmanagement
- Security-Incident-Management (Informationssicherheits-Management)
- Sicherheit in ausgelagerten Prozessen

§ ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- 4.3 Festlegen des Anwendungsbereichs des ISMS
- 8.1 Betriebliche Planung und Steuerung
- A.15 Lieferantenbeziehungen

RELEVANTE DOKU

- IT-Handbuch
- LL_ISMS_Leitlinie_STS
- NDAs und Geheimhaltung gemäß DSGVO/BDSG
- SWARCO_Cybersicherheits-Richtlinie_für_interne_und_externe_Nutzer

3 Rollen und Verantwortliche

3.1 ALLGEMEINE VERANTWORTUNG DES AUFTRAGGEBERS

UNSER UMGANG

Wir stellen sicher, dass alle relevanten Anforderungen bestimmt, geprüft und in einem gemeinsamen Dokument schriftlich fixiert sind (z.B. Service Level Agreement (SLA) / Dienstleistungs-Güte-Vereinbarung).

3.2 ALLGEMEINE VERANTWORTUNG DES AUFTRAGNEHMERS

UNSER UMGANG

Wir sehen unsere Verantwortung darin, die mit unseren Kunden festgelegten Anforderungen einzuhalten.
Darunter verstehen wir:

- Anerkannte Standards beachten / einsetzen
- Eskalationsprozess vereinbaren
- Kontaktinformationen festlegen (Vertrag / SLA)
- Changemanagement definieren (positiv & negativ)
- Ausreichende Ressourcen zur Verfügung stellen
- Sicherheitsanforderungen an Dienstleister / Subunternehmer definieren und überwachen

§ ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- A.12.1 Betriebsabläufe und -verantwortlichkeiten
- A.15 Lieferantenbeziehungen
- A.18 Compliance
- A.6.1 Interne Organisation
- A. 15 Lieferantenbeziehung
- A.18 Compliance
- A.12 Betriebssicherheit

RELEVANTE DOKU

- Betriebshandbücher
- IT-Handbuch
- Lizenzmanagement SWARCO Group IT
- LL_ISMS_Leitlinie_STS
- NDAs und Geheimhaltung gemäß DSGVO/ BDSG
- RL_ISMS_Compliance_ Sicherheitsanforderungen_STS
- RL_ISMS_Klassifizierung_Umgang mit Informationen_STS
- SWARCO_Cybersicherheits-Richtlinie_für_ interne_und_externe_Nutzer
- SWARCO_Cybersicherheits-Richtlinie_für_IT-Personal_und_Entwickler

4 Vulnerability-Management

UNSER VERSTÄNDNIS

Wir prüfen kontinuierlich unsere Produkte / Dienstleistungen auf Schwachstellen. Sollten von uns entwickelte Produkte / Dienstleistungen von Schwachstellen betroffen sein, melden wir diese umgehend an unsere Kunden weiter.

4.1 METHODIK UND UMFANG

UNSER UMGANG

Ermittelte Schwachstellen, die auf die Verfügbarkeit, Integrität, Vertraulichkeit von (materiellen oder immateriellen) Vermögenswerten und operierende Dienstleistungen unserer Kunden Einfluss haben, werden erfasst, auf mögliche funktionale und sicherheitsrelevante Auswirkungen hin bewertet und an die Kunden gemeldet.

4.2 VULNERABILITY-ASSESSMENT

UNSER UMGANG

Wir sichten kontinuierlich Quellen für Sicherheitsempfehlungen und bewerten diese in Bezug auf gelieferte Assets.
Bei betroffenen Komponenten führen wir eine Einstufung der Kritikalität (inklusive Reaktionszeit) durch.

4.3 BEHEBUNG VON SCHWACHSTELLEN

UNSER UMGANG

Wir erarbeiten Lösungen mit einem Best-Effort-Ansatz nach bestem Wissen. Wir haben einen implementierten Schwachstellenprozess mit festgelegten Reaktionszeiten.

4.4 KOMMUNIKATION

UNSER UMGANG

Anforderungen an die Kommunikationswege werden mit den Kunden bezüglich Art und Form vereinbart. Zur Geheimhaltung und Integrität für die Übermittlung von Mitteilungen und Dokumenten verwenden wir kryptographische Techniken nach dem Stand der Technik.

§ ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- A.16 Handhabung von Informationssicherheitsvorfällen
- A.13.2 Informationsübertragung
- A.12.6 Handhabung technischer Software
- A.17.1 Aufrechterhaltung Informationssicherheit
- A.6.2 Mobilgeräte / Telearbeit
- A.13 Kommunikationssicherheit
- A.10 Kryptographie

RELEVANTE DOKU

- Betriebshandbücher der jeweiligen Systeme
- IT-Handbuch
- Mitarbeiter Handout
- NDA und Geheimhaltung gemäß DSGVO/BDSG
- RL_ISMS Umgang mit organisatorischen Schwachstellen_STS
- RL_ISMS_Mobiles_Arbeiten
- RL_Umgang mit Schwachstellenmeldungen_ STS
- SWARCO_Cybersicherheits-Richtlinie_für_IT-Personal_und_Entwickler
- SWARCO_Cybersicherheits-Richtlinie_für_ interne_und_externe_Nutzer
- SWARCO_Cybersicherheits-Richtlinie_für_IT-Personal_und_Entwickler

5 Patch-Management

5.1 UMFANG DES PATCHINGS

UNSER UMGANG

Wir legen **vor** der Systemabnahme den Anwendungsbereich des Patchings schriftlich fest. Dazu gehören in der Regel Betriebssystem (inklusive aller Softwarepakete / Services), Tools und Applikationen (für Betrieb und Wartung), Zielapplikation (Servicelogik) und Middleware-Application-Layer, Datenbanken, Access-, Monitoring- oder Applikationsserver, die für den Service genutzt werden.

5.2 PATCH-LEVEL WÄHREND DER SYSTEMABNAHME

UNSER UMGANG

Erwartungen des Patch-Levels während der Systemabnahme: Wir stellen sicher, dass alle Systeme vor der Abnahme gepatcht und aktualisiert werden und die Patch-Level festgelegt sind. Öffentlich verfügbare und von Kunden freigegebene Patches installieren wir je nach Vereinbarung.

5.3 PATCH-MANAGEMENT NACH DER SYSTEMABNAHME

UNSER UMGANG

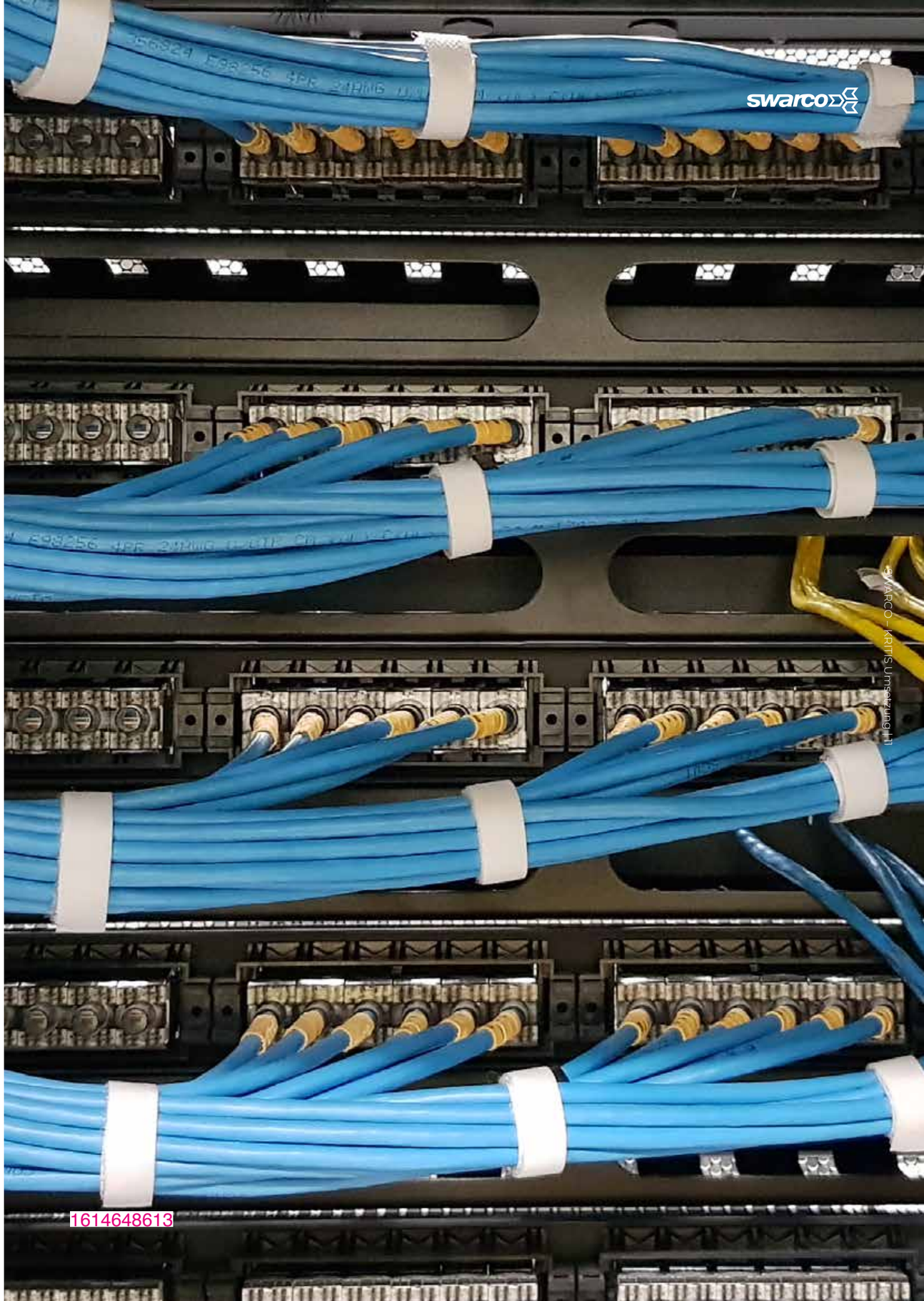
Als Anforderung an das kontinuierliche Patch-Management nach der Systemabnahme sehen wir vor, regelmäßig dem Stand der Technik entsprechende Updates und Patches zur Verfügung zu stellen, uns dabei an die individuell vereinbarten Zeiten zu halten und die Kunden darüber zu informieren.
Bei Lifecycle-Ende der von uns eingesetzten Komponenten informieren und beraten wir die Kunden dabei, angemessene und passende Alternativlösungen zu finden.
Zudem gewährleisten wir eine kontinuierliche Funktionsfähigkeit unserer gelieferten Leistung auch bei Patches der darunterliegenden Schichten anderer Systemplattformen.

§ ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- A.14.2 Sicherheit in Entwicklungs-/ Unterstützungsprozessen

RELEVANTE DOKU

- RL_ISMS_Compliance_ Sicherheitsanforderungen_STS
- SWARCO_Cybersicherheits-Richtlinie_ für_IT-Personal_und_Entwickler



6 Systemhärtung

6.1 MINIMALE INSTALLATIONSPRINZIPIEN

UNSER UMGANG

Als Standard für Betriebssysteme / Software installieren wir:

- jede Softwarekomponente, die für die Anwendung oder nach der Logik des Dienstes benötigt wird
- jede aus der Integration mit anderen Services resultierende andere Anwendung oder Softwarekomponente
- jede aus Betriebs- und Wartungsanforderungen resultierende Softwarekomponente

6.2 NETZWERKDIENSTE (NETZWERKZUGÄNGE)

UNSER UMGANG

Zusätzlich zur Dokumentation jedes Zugangs werden unnötige Netzwerkzugänge von uns deaktiviert.

6.3 KONFIGURATIONSSTANDARDS

UNSER UMGANG

Wir halten die allgemeinen/vereinbarten Konfigurationsstandards und Sicherheitsvorschriften ein.

6.4 STANDARDPASSWÖRTER

UNSER UMGANG

Jedes Standardpasswort kann in allen möglichen Fällen geändert werden.

6.5 BACKDOORS

UNSER UMGANG

Unsere Lösungen sind frei von Backdoors, die Sicherheitsmechanismen umgehen können.

6.6 KONTROLLE UND AUDIT DER IN DIESEM KAPITEL GENANNTEN KONDITIONEN

UNSER UMGANG

Wir stimmen mit unseren Kunden ab, dass wir hinsichtlich unserer Produkte geeignete Maßnahmen und Protokolle nachweisen, die alle vereinbarten Anforderungen an die Systemhärtung erfüllen.

ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- A.12.5.1 Installation von Software
- A.13.1 Netzwerksicherheitsmanagement
- A.9 Zugangssteuerung
- A.12.7 Audit von Informationssystemen

RELEVANTE DOKU

- Betriebshandbuch
- Dokumentation im Ticketsystem
- Dokumentation in Microsoft Teams / Microsoft SharePoint
- IT-Handbuch
- RL_ISMS_Personalsicherheit_STS Netzstrukturplan
- SWARCO_Cybersicherheits-Richtlinie_für_IT-Personal_und_Entwickler
- SWARCO_Cybersicherheits-Richtlinie_für_interne_und_externe_Nutzer
- Trennung von Netzwerk- und Computerbetrieb ist durch SWARCO Group IT

7 Fernzugang für Drittanbieter

7.1 ALLGEMEINE ERWARTUNGEN

UNSER UMGANG

Um bei Fernzugängen die Vertraulichkeit, Verfügbarkeit und Integrität der Assets und Services des Auftraggebers zu gewährleisten, stellen wir sicher, dass wir für alle Aktionen der Benutzerkonten mit Fernzugangsfunktion auf Systemen des Auftraggebers verantwortlich sind und eine nachträgliche Verwendung von Informationen des Zugriffs möglich ist.

7.2 USER-ACCOUNT-MANAGEMENT

UNSER UMGANG

Jeder Anwender bekommt von uns sein eigenes Benutzerkonto. Ausnahmen oder Sonderlösungen müssen von den Kunden freigegeben und schriftlich dokumentiert sein (SLA). Hierdurch garantieren wir eine komplette, revisionssichere Dokumentation der Rückverfolgbarkeit eines Accounts. Regelmäßige Prüfungen und gegebenenfalls Löschungen von Accounts inklusive Authentifizierungsverfahren und physischen Zutritte werden im SLA definiert.

ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- A.9.3 Benutzerverantwortlichkeiten
- A.9.4 Zugangssteuerung
- A.9.2 Benutzerverwaltung

RELEVANTE DOKU

- Checkliste für neue Benutzer oder Zugangssteuerungsrichtlinie
- IT-Handbuch
- Kennwortrichtlinien (gem. Empfehlungen des BSI)
- RL_ISMS_Personalsicherheit_STS
- SWARCO_Cybersicherheits-Richtlinie_für_IT-Personal_und_Entwickler
- SWARCO_Cybersicherheits-Richtlinie_für_interne_und_externe_Nutzer

8 Anforderungen an die Softwareentwicklungsprozesse

UNSER VERSTÄNDNIS

Wir haben die Anforderungen an einen sicheren Softwareentwicklungsprozess (Security by Design) definiert und dokumentiert. Unsere Softwareentwicklungsprozesse sind so ausgelegt, dass der Sicherheit der entwickelten Software angemessene Beachtung in allen wichtigen Entwicklungsphasen geschenkt wird und die Prozesse sich an den allgemein anerkannten Industriestandards und den UP KRITIS Best Practice Empfehlungen orientieren.

§ ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- A.12.5 Steuerung der Software im Betrieb
- A.14.2 Sicherheit der Entwicklungs- und Unterstützungsprozesse
- A.12.3 Datensicherung
- A.14.3 Testdaten

§ RELEVANTE DOKU

- IT-Handbuch
- RL_ISMS_Compliance_ Sicherheitsanforderungen_STS
- SWARCO_Cybersicherheits-Richtlinie_für_IT-Personal_und_Entwickler

9 Einsatz von kryptographischen Lösungen

UNSER VERSTÄNDNIS

Wir stellen sicher, dass keine veralteten und als unsicher bekannten kryptographischen Lösungen, weder in unseren Produkten, noch in unserer Kommunikation oder in der Ablage, verwendet werden. Hierzu definieren wir gemeinsam mit unseren Kunden, angepasst an den Schutzbedarf, die Vorgaben für zulässige kryptographische Algorithmen und halten diese in einer schriftlichen Richtlinie fest, die den anerkannten Richtlinien / Industriestandards entspricht. Um die Aktualität zu gewährleisten, prüfen wir die definierten Vorgaben und passen die Richtlinien an.

§ ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- A.10 Kryptographie
- A.14.1 Sicherheitsanforderungen für Informationssysteme

RELEVANTE DOKU

- IT-Handbuch
- RL_ISMS_Compliance_ Sicherheitsanforderungen_STS
- SWARCO_Cybersicherheits-Richtlinie_für_IT-Personal_und_Entwickler

10 Sicherheitsanforderungen für den IT Betrieb

UNSER VERSTÄNDNIS

Wenn wir für den IT-Betrieb oder Teile des IT-Betriebes zuständig sind, legen wir die Anforderungen an den Informationssicherheitsprozess gemeinsam mit unseren Kunden schriftlich fest.

10.1 INFORMATIONSSICHERHEITSPROZESS

UNSER UMGANG

Wir verfügen über ein Informationssicherheits-Managementsystem nach DIN EN ISO/IEC 27001:2017. Dadurch sind Prozesse und Verantwortlichkeiten definiert und dokumentiert. Alle daraus resultierenden Vorgaben werden erfüllt, ständig aktualisiert, angepasst und allen Mitarbeitern zur Verfügung gestellt. Außerdem sind hierüber Zugriffsschutz- und Berechtigungsvergabe-Prozesse sowie Kontrollen zum Zugriffsschutz und zur Berechtigungsvergabe implementiert.

10.2 ASSET-MANAGEMENT

UNSER UMGANG

Wir haben, zusätzlich zu den im Abschnitt „Nicht-technische Sicherheit - Asset Management“ definierten Anforderungen, Standards zur sicheren Löschung der Daten / Zerstörung von Datenträgern definiert, um zu vermeiden, dass die gelöschten Daten von Dritten unautorisiert wiederhergestellt werden können.

10.3 PERSONALSICHERHEIT (HR-SECURITY)

UNSER UMGANG

Zusätzlich zu den im Abschnitt „Nicht-technische Sicherheit – Human-Resources-Security“ definierten Anforderungen führen wir halbjährliche Security-Awareness-Trainings für unsere Mitarbeiter durch, die den aktuellen Erkenntnissen entsprechen.

10.4 PHYSISCHE SICHERHEIT UND ZUTRITTSSCHUTZ

UNSER UMGANG

Selbstverständlich treffen wir angemessene Vorkehrungen zur physischen Sicherheit und zum Zutrittsschutz. Diese Maßnahmen schließen Elementarschäden / -einflüsse und sonstige Notsituationen ein. Außerdem definieren wir kritische Zonen und schränken Zutritte auf autorisierte Personenkreise ein.

10.5 NETZWERKSICHERHEIT UND OPERATIONELLE SICHERHEIT

UNSER UMGANG

Netzwerksegmente mit unterschiedlichem Schutzbedarf und Sicherheitsstufen werden (durch freigegebene Firewalls) voneinander getrennt. Authentisierungsmerkmale (Passwörter, PINs) werden nur verschlüsselt über das Netzwerk übermittelt. Aus dem Internet erreichbare administrative Zugänge oder Netzwerkports für den technischen Zugriff werden abgeschaltet oder angemessen abgesichert. Zur Nachvollziehbarkeit von Angriffen oder Fehlbedienungen werden Netzwerkverbindungen, Systemzugriffe und administrative Tätigkeiten protokolliert und archiviert. Zudem wird immer ein aktueller Virenschutz implementiert und ein Datensicherungs-/ Wiederherstellungsprozess etabliert. Datenwiederherstellungstests werden regelmäßig durchgeführt. Software-Change-Prozesse für Produktivumgebungen sind etabliert und werden befolgt. Prozesse zu regelmäßigen Schwachstellenscans und zur Behebung von Schwachstellen sind etabliert und werden befolgt. Bei Benutzung von drahtlosen Netzwerken sind diese kryptographisch abgesichert.

10.6 SECURITY-INCIDENT-MANAGEMENT

UNSER UMGANG

Um auf Sicherheitsvorfälle (IT-Security-Szenarien sowie Non-IT-Security-Szenarien) schnell reagieren zu können, haben wir hierzu Prozesse und die dazugehörigen Rollen / Verantwortlichkeiten definiert, dokumentiert und adressiert.

10.7 SICHERHEIT IN AUSLAGERUNGSPROZESSEN

UNSER UMGANG

Bei Auslagerung von Betriebsleistungen oder anderen Dienstleistungen werden alle Sicherheitsanforderungen gemäß den vertraglichen Bedingungen an den Dienstleister weitergegeben und überwacht. Unser Kunde ist jederzeit über die Auslagerung informiert und gegebenenfalls in den Beauftragungsprozess involviert.

§ ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- 4.3 Festlegen des Anwendungsbereichs des ISMS
- A.5 Informationssicherheitsleitlinie
- A.8 Verwaltung von Werten
- A.17 Informationssicherheitsaspekte
- A.7 Sicherheit des Personals
- A.11 Physische und umgebungsbezogene Sicherheit
- A.9.1 Zugangssteuerung
- A.13.1 Netzwerksicherheitsmanagement
- A.14.1 Sicherheitsanforderungen für Informationssysteme
- A.8.2 Informationsklassifizierung
- A.9.2 Benutzerzugangsverwaltung
- A.12.2 Schutz vor Schadsoftware
- A.18.2 Überprüfung der Informationssicherheit
- A.7.3 Beendigung / Wechsel der Anstellung
- A.8.3 Handhabung von Datenträgern
- A.12.3 Datensicherung
- A.9.4 Zugangssteuerung für Systeme und Anwendungen
- A.16 Handhabung von Informationssicherheitsvorfällen
- A.13.2 Informationsübertragung
- A.15.2 Steuerung Dienstleistungserbringung Lieferanten
- A.18.2 Überprüfung der Informationssicherheit
- A.8 Verwaltung der Werte
- A.6.2 Mobilgeräte und Telearbeit

RELEVANTE DOKU

- AN_ISMS_Clean-Desk-Policy_STS
- AN_ISMS_physische_Sicherheitszonen_STS
- AN_Rechtevergabe_Klassifizierung_STS
- Asset-Register ISMS
- Betriebshandbuch
- Inventarisierung der Netzwerkkomponenten durch SWARCO Group IT (Wattens)
- IT-Handbuch
- LL_ISMS_Leitlinie_STS
- Microsoft Intune (MobilenGeräte)
- RL_ISMS Physische Sicherheit_STS
- RL_ISMS_Compliance_Sicherheitsan-forderungen_STS
- RL_ISMS_Klassifizierung_Umgang mit Informationen_STS
- RL_ISMS_Personalsicherheit_STS
- RL_Umgang mit Schwachstellenmeldungen_STS
- SWARCO_Cybersicherheits-Richtlinie_für_IT-Personal_und_Entwickler
- SWARCO_Cybersicherheits-Richtlinie_ für_interne_und_externe_Nutzer

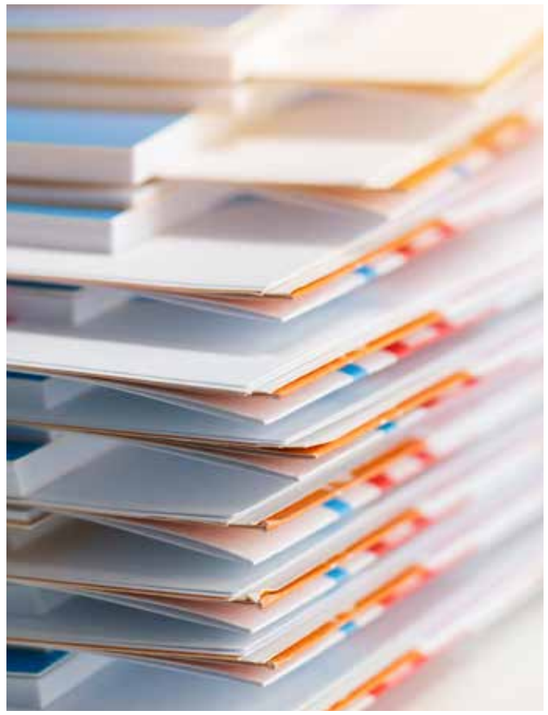
11 Dokumentation

UNSER VERSTÄNDNIS

Wir stellen jegliche Dokumentation zur Verfügung, die die Nutzung der angebotenen Lösung erleichtert oder die von unseren Kunden explizit als Teil des Liefergegenstands oder Auftrags gewünscht wird. Änderungen oder Anpassungen werden entsprechend ergänzt.

§ ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- A.8 Verwaltung der Werte
- A.6.2 Mobilgeräte und Telearbeit



12 Informationspflicht über sicherheitsrelevante Vorfälle

UNSER VERSTÄNDNIS

Gemeinsam mit unseren Kunden entwickeln wir Melde-prozesse für potentielle Sicherheitsvorfälle, die einen negativen Effekt auf materielle und immaterielle gelieferte oder auf dem Informationssystem gespeicherte Vermögenswerte haben könnten. Außerdem vereinbaren wir mit unseren Kunden Kriterien für Art, Meldeweg und Dokumentation zu Schwachstellen, bei denen diese informiert werden müssen.

§ ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- A.16 Handhabung von Informationssicherheitsvorfällen

RELEVANTE DOKU

- RL_Umgang mit Schwachstellenmeldungen_ STS

13 Nicht-technische Sicherheit

13.1 ORGANISATION DER INFORMATIONSSICHERHEIT

UNSER UMGANG

Informationen über unsere Sicherheitsorganisation in Form von Audits oder Lieferantenbewertungen, die unseren Kunden helfen, unsere Sicherheitsorganisation zu verstehen und deren Reife zu prüfen, können jederzeit geplant werden. Gerne stellen wir unseren Kunden unser DIN EN ISO/IEC 27001:2017 Zertifikat zur Verfügung.

13.2 ASSET-MANAGEMENT

UNSER UMGANG

Assets und die Verantwortung zu deren Aufrechterhaltung werden allgemein und projektbezogen identifiziert, dokumentiert und angemessen geschützt.

13.3 HUMAN-RESSOURCES-SECURITY

UNSER UMGANG

Jeder SWARCO-Mitarbeiter (und auch Subunternehmer), der über seine Tätigkeit entfernten oder lokalen Zugriff auf Informationssysteme von Kunden oder Zugriff auf kritische Daten hat, wird entsprechend der Klassifizierung (Schutzbedarf) der Daten überprüft beziehungsweise muss Informationen zu seiner Identität bereitstellen. Mitarbeiter werden nur gemäß Ihrer Freigabe und Kompetenzen bezüglich der beauftragten Leistungen geplant und eingesetzt.

13.4 AUDITS

UNSER UMGANG

Audits jeglicher Art (intern /extern / Kunde) werden regelmäßig durchgeführt. Umfang, Dauer und Art des Audits können individuell vereinbart werden. Etwaige Abweichungen oder entdeckte Verbesserungsmöglichkeiten werden dokumentiert, kommuniziert und Maßnahmen zur Umsetzung getroffen.

§ ERFÜLLT ÜBER ISO/IEC 27001 UND ANHANG DER ISO/IEC 27001

- A.6 Organisation der Informationssicherheit
- A.8 Verwaltung der Werte
- A.7 Sicherheit des Personals
- A.6.2 Mobilgeräte / Telearbeit
- A.12 Betriebssicherheit
- A.9 Zugangssteuerung
- A.12.7 Audit von Informationssystemen

RELEVANTE DOKU

- AN_Rechtevergabe_Klassifizierung
- Asset-Register ISMS
- Dokumentation in Microsoft Teams / Microsoft SharePoint
- Inventarisierung der Netzwerkkomponenten durch SWARCO Group IT (Wattens)
- ISMS_Bestellung_ISB
- LL_ISMS_Leitlinie_STS
- Microsoft Intune(mobile Endgeräte)
- Mitarbeiter Handout
- RL_ISMS_Klassifizierung_Umgang _mit_Informationen
- RL_ISMS_Mobiles_Arbeiten
- RL_ISMS_Personalsicherheit_STS
- SWARCO_Cybersicherheits-Richtlinie_ für_interne_und_externe_Nutzer