

[Name der Organisation]

ST9 Handbuch zur Identitäts- und Zugriffssteuerung

Version	1.0
Besitzer der Police	Name eingeben
Genehmigt durch	Ausschuss zur Genehmigung der Richtlinie
Datum der Genehmigung	Datum eingeben
Datum des Inkrafttretens	Datum eingeben
Nächster Überprüfungstermin	Datum eingeben
Vertraulichkeitsstufe	INTERN

Änderungsverlauf

Datum	Version	Erstellt von	Beschreibung der Änderung
26.09.24	0.91	DataGuard	Grundstruktur des Dokuments
XX.XX.24	1.00	XX	Genehmigte Version und minimale Änderungen

[Wie diese DataGuard Richtlinienvorlage zu verwenden ist:]

[DataGuard möchte Ihnen einige wichtige Hinweise zur Anwendung der bereitgestellten Richtlinienvorlage geben. Diese Vorlage soll Ihnen als Ausgangspunkt dienen, um eigene, auf Ihre Organisation zugeschnittene Richtlinien zu entwickeln. Bitte beachten Sie die folgenden Hinweise zur Verwendung der Vorlage sorgfältig.]

Verwendung der Vorlage

- **Vorlage als Ausgangspunkt:** Diese Vorlage ist sorgfältig recherchiert und von Experten zusammengestellt worden. Sie ist als Ausgangspunkt für die Erstellung Ihrer eigenen Richtlinie gedacht und bietet eine Struktur sowie Beispiele für Ihr künftiges Dokument. Bei allen Bemühungen erhebt diese Vorlage jedoch keinen Anspruch auf Passgenauigkeit und Vollständigkeit, denn die individuellen Gegebenheiten in Ihrer Organisation können abweichen.
- **Grundsatz der Effektivität:** Eine Richtlinie soll erforderlich, angemessen, passend, aufklärend und unterstützend für Ihren individuellen Unternehmenszweck wirken. Sorgen Sie dafür, dass Ihre Richtlinien stets diesem Grundsatz entsprechen.
- **Überprüfung der Inhalte:** Gehen Sie die Inhalte der Vorlage sorgfältig durch und überprüfen Sie diese im Hinblick auf die spezifischen Bedürfnisse und Anforderungen.
- **Vollständiges Verständnis erforderlich:** Stellen Sie sicher, dass Sie als Ersteller dieses Dokuments alle beschriebenen Anweisungen und Verfahren vollständig verstehen und für Ihre Organisation als anwendbar halten. Nur so können Sie fundierte Entscheidungen über Anpassungen treffen.
- **Klärung von Unklarheiten:** Sollten Sie auf Inhalte stoßen, die Sie nicht vollständig verstehen, holen Sie unbedingt weitere Informationen ein. Dies kann durch Rücksprache mit unseren DataGuard-Experten, rechtlichen Beratern oder anderen Fachexperten außerhalb oder innerhalb Ihrer Organisation geschehen.
- **Individuelle Anpassung erforderlich:** Die in der Vorlage beschriebenen Anweisungen und Verfahren sind pauschale Beispiele oder Vorschläge ohne tiefere Berücksichtigung Ihres Unternehmenskontextes. Daher ist es erforderlich, dass Sie den Inhalt der Richtlinien an die tatsächlichen Gegebenheiten und Anforderungen Ihrer Organisation anpassen.*
- **Keine ungeprüfte Übernahme:** Übernehmen Sie keine Texte oder Anweisungen aus der Vorlage, wenn diese nicht den spezifischen Anforderungen und der tatsächlichen Situation in Ihrer Organisation entsprechen. Jede Organisation ist einzigartig, und pauschale Übernahmen können zu Fehlern oder Missverständnissen führen.
- **Verantwortung der Geschäftsführung:** Beachten Sie, dass die endgültige Verantwortung für die Gestaltung und

Umsetzung von Richtlinien bei der obersten Leitung Ihrer Organisation liegt. Es ist entscheidend, dass diese alle Inhalte kritisch überprüft und eine Korrektur von unpassenden Inhalten veranlasst.]

[*] Die in dieser Vorlage gelb hinterlegten und in eckigen Klammern gesetzten Hilfstexte und Hinweise sollen nach Kenntnisnahme eliminiert oder inhaltlich angepasst werden. Beispiel: Bitte eliminieren Sie diese Seite vor Veröffentlichung der Richtlinie.]

1 Einleitung

Dieses Handbuch zur Informationssicherheit in Identitäts- und Zugriffssteuerung für [Name der Organisation] bietet einen konsolidierten Rahmen, der unsere Strategie für die effektive Verwaltung und Sicherung von Identitäten und Zugriffsrechten innerhalb unserer Organisation beschreibt. Dieses Dokument dient als umfassender Leitfaden, in dem detailliert beschrieben wird, wie unsere Organisation verschiedene Sicherheits Herausforderungen im Zusammenhang mit dem Identitäts- und Zugriffsmanagement im gesamten Anwendungsbereich des ISMS angehen wird.

Darüber hinaus dient es als übergeordnetes Dokument, das den Ansatz der Organisation für das Identitäts- und Zugangsmanagement umreißt.

1.1 Zweck und Umfang

Zweck dieser Richtlinie ist es, einen strukturierten Ansatz für das Identitäts- und Zugriffsmanagement festzulegen, um die sensiblen Informationen, die Infrastruktur und den Ruf unserer Organisation zu schützen. Durch die Einhaltung dieser Richtlinie wollen wir unsere Widerstandsfähigkeit gegen unbefugten Zugriff erhöhen und das Risiko von Datenschutzverletzungen oder des Missbrauchs von Privilegien minimieren.

1.2 Anwendbarkeit

Diese Richtlinie gilt für alle Mitarbeiter und Beteiligten und stellt sicher, dass sie sich an die festgelegten Richtlinien für das Identitäts- und Zugangsmanagement halten. Das Informationssicherheitsteam hat in Zusammenarbeit mit den zuständigen Abteilungen die Aufgabe, die Umsetzung, Pflege und kontinuierliche Verbesserung der in dieser Richtlinie beschriebenen Verfahren zu überwachen.

2 Identität und Authentifizierung

2.1 Identitätsmanagement

2.1.1 Richtlinie

Der gesamte Lebenszyklus des Identitätsmanagements muss die sichere Identifizierung von Personen und Systemen gewährleisten, die auf die Informationen des Unternehmens und andere damit verbundene Vermögenswerte zugreifen.

2.1.2 Verfahren

Das Identitätsmanagement der Organisation muss Folgendes sicherstellen:

Individuelle Verantwortlichkeit:

Jede einer Person zugewiesene Identität (Personalnummer, User-Name, E-Mail Adresse, etc.) sollte für diese Person eindeutig sein, um sie für die unter dieser Identität durchgeführten Handlungen zur Rechenschaft ziehen zu können. [Bitte beschreiben Sie, wie die Organisation diese Anforderung erfüllen wird Beispiel: Die gemeinsame Nutzung von Konten kann durch die Implementierung von Multi Factor Authentifizierung (MFA), die an einzelne Geräte gebunden ist, reduziert werden, Organisationsrichtlinie, ...]

Gemeinsame Identitäten:

Identitäten, die von mehreren Personen gemeinsam genutzt werden, sollten nur zugelassen werden, wenn dies aus geschäftlichen oder betrieblichen Gründen erforderlich ist, und müssen einer speziellen Genehmigung und Dokumentation unterliegen. [Beschreiben Sie bitte, wie die Organisation die Anforderung erfüllen wird: Genehmigungsverfahren durch den Asset Eigentümer]

Nicht-menschliche Entitäten:

Identitäten, die nicht-menschlichen Einheiten zugewiesen werden, sollten eine angemessen getrennte Genehmigung und

eine unabhängige laufende Aufsicht haben. [Bitte beschreiben Sie, wie die Organisation diese Anforderung erfüllen wird: Die Passwörter für Dienste-Accounts sollten rotieren (oder automatisch verwaltet werden) und jährlich genehmigt werden].

Rechtzeitige Beseitigung:

Identitäten sollten umgehend deaktiviert oder entfernt werden, wenn sie nicht mehr benötigt werden (z. B. wenn die zugehörigen Entitäten gelöscht oder nicht mehr verwendet werden oder wenn die mit einer Identität verbundene Person das Unternehmen verlassen oder die Rolle gewechselt hat). Wiederkehrende Überprüfungen müssen geplant werden [siehe **Aufgabenmanagement des ISMS**]. Die Löschung von Identitäten ist Teil des Offboardings und des Prozesses zum Wechsel von Verantwortlichkeiten.

Einheitliche Identitätszuordnung:

Innerhalb eines bestimmten Bereichs sollte jede Identität einer einzigen Entität zugeordnet werden, um doppelte Identitäten innerhalb desselben Kontexts zu vermeiden.

Führung von Aufzeichnungen:

Führen Sie Aufzeichnungen über alle wichtigen Ereignisse bezüglich der Verwendung und Verwaltung von Benutzeridentitäten und Authentifizierungsinformationen.

Darüber hinaus sollte das Unternehmen ein Verfahren für den Umgang mit Änderungen von Informationen im Zusammenhang mit der Benutzeridentität einrichten. Dazu könnte die erneute Überprüfung von Ausweisdokumenten zu einer Person gehören.

Bei Identitäten, die von Dritten zur Verfügung gestellt oder ausgestellt werden (z. B. Anmeldeinformationen für soziale Medien), muss das Unternehmen sicherstellen, dass diese Drittanbieter-Identitäten das erforderliche Vertrauensniveau bieten und die erforderliche Genehmigung besteht und dass alle damit verbundenen Risiken bekannt sind und angemessen behandelt werden. Dies kann sowohl Überprüfungen in Bezug auf die Anbieter, als auch Pberprüfungen in Bezug auf die zugehörigen Authentifizierungsinformationen umfassen. [Bitte beschreiben Sie die technischen oder organisatorischen Prozesse des Unternehmens, um diese Anforderungen zu erfüllen].

2.2 Informationen zur Authentifizierung

2.2.1 Richtlinie

Die Organisation muss sicherstellen, dass alle folgenden Punkte innerhalb der Organisation beachtet werden.

1. Authentifizierungsinformationen sind ein wichtiger Aspekt der Informationssicherheit.
2. Für den Zugang zu sensiblen und vertraulichen Daten müssen die Nutzer starke Authentifizierungsmethoden wie die Zwei-Faktor- oder Multi-Faktor-Authentifizierung (MFA) verwenden.
3. Die Passwörter müssen mindestens einmal jährlich oder bei Verdacht auf einen Sicherheitsvorfall geändert werden.
4. Passwörter können nicht wiederverwendet werden (z.B. Historie von mindestens 6 Passwörtern).
5. Passwörter müssen mindestens 8 Zeichen lang sein, einschließlich Zahlen, Groß- und Kleinschreibung und Sonderzeichen.
6. Häufig verwendete Passwörter oder mehr als 2 aufeinanderfolgende Zeichen sind nicht erlaubt.
7. Passwörter können nicht in Textdateien gespeichert werden; sie dürfen nur im genehmigten Passwort-Tresor gespeichert werden.
8. Die Verschlüsselung und das Hashing von Passwörtern sollte nach anerkannten kryptografischen Verfahren für Passwörter in Anwendungen und Authentifizierungssystemen erfolgen.

[Bitte ändern Sie diese Beschreibung, wenn Sie ein strengeres Passwortkriterium haben oder ein anderes Verfahren anwenden].

2.2.2 Verfahren

Das folgende Verfahren wird innerhalb der Organisation befolgt und für alle verbindlich gemacht.

Passwort-Bereitstellung:

a) Temporäre Passwörter oder PINs dürfen nicht erraten werden, sind für jeden Benutzer eindeutig und werden nach der ersten Verwendung geändert.

b) Es gibt Verfahren zur Überprüfung der Benutzeridentität, bevor neue, Ersatz- oder temporäre Authentifizierungsinformationen bereitgestellt werden.

Alle Nutzer innerhalb der Organisation müssen jährlich an die folgenden Praktiken erinnert werden:

a) Behandeln Sie geheime Authentifizierungsinformationen vertraulich und geben Sie keine persönlichen geheimen Authentifizierungsinformationen weiter. Geheime Authentifizierungsinformationen, die mit mehreren Benutzern oder nicht-personenbezogenen Einheiten verknüpft sind, sollten nur an autorisierte Personen weitergegeben werden. **[Bitte planen Sie die Benutzererinnerung in Ihrer ISMS-Aufgabenmanagement].**

b) Ändern Sie betroffene oder kompromittierte Authentifizierungsinformationen sofort nach der Benachrichtigung oder dem Hinweis auf eine Kompromittierung.

c) Wählen Sie sichere Passwörter entsprechend den Empfehlungen für bewährte Verfahren.

d) Vermeiden Sie die Verwendung derselben Passwörter für verschiedene Dienste und Systeme, bei denen kein Single Sign-On (SSO) verfügbar ist.

[Bitte bearbeiten Sie die entsprechenden Richtlinien im Mitarbeiter-Sicherheitshandbuch, in der die Anforderungen für die Erstellung von Kennwörtern festgelegt sind (z. B. ist nur die Verwendung des Passwort-Management-Tools zulässig).

2.3 Sichere Authentifizierung

2.3.1 Richtlinie

Die auf der Grundlage der Informationszugriffsbeschränkungen und der themenspezifischen Richtlinie über die Stärke der Zugriffskontrolle ausgewählten Authentifizierungsmethoden müssen der Sensibilität der Informationen entsprechen, auf die zugegriffen wird. Für den Zugriff auf hochsensible Informationen müssen starke Authentifizierungsmethoden wie MFA, digitale Zertifikate, Smartcards, Token oder biometrische Mittel eingesetzt werden.

2.3.2 Verfahren

Authentifizierungstechniken und -stärke:

Wählen Sie Authentifizierungsmethoden mit angemessener Authentifizierungsstärke, wie z. B. Passwörter, digitale Zertifikate, Smartcards, Token oder biometrische Verfahren, je nach Sensibilitätsstufe.

Multi-Faktor-Authentifizierung (MFA):

a) Identifizieren Sie kritische Informationssysteme, die eine MFA benötigen.

b) Implementieren Sie MFA-Lösungen, die mehrere Faktoren wie Passwörter, biometrische Daten oder Token kombinieren.

c) Konfigurieren Sie die Systeme so, dass unter bestimmten Umständen zusätzliche Authentifizierungsfaktoren abgefragt werden, falls erforderlich.

[Löschen, wenn nicht verwendet] Biometrische Authentifizierung:

a) Bewerten Sie die Zuverlässigkeit und die potenziellen Risiken der biometrischen Authentifizierung.

b) Einführung biometrischer Authentifizierung neben alternativen Methoden.

c) Festlegung von Verfahren zur Ungültigmachung kompromittierter biometrischer Daten und Bereitstellung alternativer Authentifizierungsmittel.

Sichere Log-On-Verfahren:

a) Stellen Sie sicher, dass sensible Informationen erst nach erfolgreichem Abschluss der Anmeldung angezeigt werden.

b) Validieren Sie die Anmeldeinformationen erst, wenn alle erforderlichen Daten eingegeben wurden.

c) Implementieren Sie Maßnahmen, um Brute-Force-Anmeldeversuche zu verhindern.

d) Konfigurieren Sie die Systeme so, dass sowohl erfolgreiche als auch erfolglose Anmeldeversuche protokolliert werden.

e) Richten Sie Warnmeldungen für potenzielle Anmeldeverletzungen und Sicherheitsereignisse ein.

h) den Nutzern nach erfolgreicher Anmeldung Einzelheiten über frühere Anmeldeversuche und Sitzungsaktivitäten zur Verfügung zu stellen.

f) Verschlüsseln Sie Passwörter bei der Eingabe und Übertragung, um unbefugten Zugriff zu verhindern.

g) Automatische Beendigung inaktiver Sitzungen nach einem bestimmten Zeitraum.

Compliance und Sicherheit:

a) Durchführung regelmäßiger Audits, um die Einhaltung der Authentifizierungsverfahren sicherzustellen.

b) Überprüfung, ob die Authentifizierungssicherheit den festgelegten Standards entspricht.

3 Physische und logische Zugangskontrolle

3.1 Zugangskontrolle

3.1.1 Richtlinie

Um sicherzustellen, dass der Zugang zu Informationen und anderen damit verbundenen Vermögenswerten in der Organisation nur befugten Personen gewährt wird und um unbefugten Zugang zu verhindern, müssen die Asset-Eigentümer die Klassifizierung der Informationsdaten und die relevanten Informationssicherheitsanforderungen in Bezug auf die Zugangskontrolle ermitteln.

3.1.2 Verfahren

Die Regeln für die Zugangskontrolle werden durch die Festlegung und Zuweisung der entsprechenden Zugangsrechte und -beschränkungen in die Praxis umgesetzt. Um die Verwaltung der Zugangskontrolle zu vereinfachen, werden Gruppen von Einheiten spezifische Rollen zugewiesen.

Definition und Implementierung von Zugangskontrollregeln:

1. Sicherstellung der Konsistenz zwischen den Zugriffsrechten und der Informationsklassifizierung.
2. Richten Sie die Zugriffsrechte an den Sicherheitsbedürfnissen und -anforderungen des physischen Perimeters aus.
3. Berücksichtigen Sie alle Arten von Verbindungen in verteilten Umgebungen, um sicherzustellen, dass Einrichtungen nur Zugang zu autorisierten Informationen und zugehörigen Ressourcen, einschließlich Netzwerken und Netzwerkdiensten, haben.
4. Elemente oder Faktoren, die für die dynamische Zugangskontrolle relevant sind, angemessen widerspiegeln.

3.2 Zugangsrechte

3.2.1 Richtlinie

Zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit innerhalb der Organisation muss der Zugang zu den Informationen so verwaltet werden, dass die Geschäftsinformationen geschützt werden.

Die den Nutzern gewährten Zugriffsrechte auf die Systeme und Ressourcen des Unternehmens müssen regelmäßig überprüft und widerrufen werden.

3.2.2 Verfahren

Die Organisation muss sicherstellen, dass das folgende Verfahren für die Zuweisung oder den Entzug von physischen und logischen Zugangsrechten eingehalten wird:

1. Einholung der Genehmigung des Asset-Eigentümers vor der Gewährung von Zugriffsrechten.
2. Berücksichtigung der geschäftlichen Anforderungen sowie der Unternehmensrichtlinien und -regeln für die Zugangskontrolle.
3. Gewährleistung der Aufgabentrennung, einschließlich der Trennung der Rollen für die Genehmigung und die Umsetzung der Zugangsrechte.
4. Entzug von Zugriffsrechten, wenn sie nicht mehr benötigt werden, insbesondere für Benutzer, die das Unternehmen verlassen haben.

5. Gewährung von zeitlich begrenzten Zugriffsrechten für einen begrenzten Zeitraum und Entzug dieser Rechte zum Ablaufdatum.
6. Überprüfung, ob die gewährte Zugriffsstufe mit den Zugriffskontrollrichtlinien übereinstimmt und mit anderen Informationssicherheitsanforderungen vereinbar ist.
7. Aktivierung der Zugriffsrechte erst nach erfolgreichem Abschluss der Autorisierungsverfahren.
8. Pflege einer zentralen Aufzeichnung der Zugriffsrechte, die einer Benutzererkennung für den Zugriff auf Assets gewährt werden.
9. Änderung der Zugriffsrechte von Benutzern, die ihre Rolle oder ihren Arbeitsplatz gewechselt haben.
10. Entfernen oder Anpassen von physischen und logischen Zugriffsrechten, was durch Entfernen, Entziehen oder Ersetzen von Schlüsseln, Authentifizierungsinformationen, Identifikationskarten oder Abonnements geschehen kann.
11. Aufzeichnung von Änderungen an den Zugriffsrechten der Benutzer.

[Prüfen und bestätigen Sie, dass dieses Verfahren korrekt ist, und konkretisieren Sie es entsprechend Ihrer Organisation]

Regelmäßige Überprüfung der physischen und logischen Zugangsrechte

1. Änderungen der Zugriffsrechte von Nutzern nach einem Wechsel innerhalb des Unternehmens (z. B. Stellenwechsel, Beförderung, Degradierung) oder nach Beendigung des Arbeitsverhältnisses.
2. Berechtigungen für privilegierte Zugriffsrechte.

Änderung oder Beendigung der Beschäftigung:

Die Zugriffsrechte eines Benutzers sollten vor jeder Änderung oder Beendigung des Beschäftigungsverhältnisses auf der Grundlage von Risikofaktoren wie z. B.: Die Beendigung oder Änderung wird vom Benutzer oder von der Geschäftsleitung veranlasst, und der Grund für die Beendigung bestimmt die Dringlichkeit der Zugangsentsorgung.

Der Zugang zu 3rd Party- und Cloud-Ressourcen muss umgehend entfernt werden.

3.3 Privilegierte Zugriffsrechte

3.3.1 Richtlinie

Privilegierte Zugriffsrechte müssen auf kontrollierte Weise zugewiesen und verwaltet werden, um das Risiko des unbefugten Zugriffs und des Missbrauchs sensibler Informationen und Systeme zu mindern.

Privilegierte Benutzer können erhebliche Änderungen an den Systemen und Daten eines Unternehmens vornehmen. Daher muss unbedingt sichergestellt werden, dass diese Konten vor unbefugter Nutzung geschützt sind. Wenn ein böswilliger Akteur privilegierten Zugriff erlangt, kann er erheblichen Schaden anrichten, einschließlich Datenverletzungen, Systemabschaltungen oder sogar die vollständige Übernahme des Netzwerks.

Die Europäische Datenschutzgrundverordnung (DSGVO) verlangt von Unternehmen, personenbezogene Daten zu schützen, was eine Begrenzung und Überwachung des privilegierten Zugriffs beinhaltet.

3.3.2 Verfahren

Identifizierung von Benutzern, die privilegierten Zugriff benötigen

1. Überprüfen Sie die Rollenstruktur und Zuständigkeiten, um Benutzer zu ermitteln, die für bestimmte Systeme oder Prozesse privilegierten Zugang benötigen.
2. Bestimmen Sie die funktionalen Rollen und Kompetenzen, die für Einzelpersonen erforderlich sind, um Aufgaben auszuführen, die einen privilegierten Zugang erfordern.

Genehmigungsverfahren:

1. Ein Genehmigungsverfahren für die Gewährung von privilegierten Zugriffsrechten einleiten und die Genehmigung der zuständigen Stelle sicherstellen.
2. Dokumentieren Sie das Genehmigungsverfahren, einschließlich der Namen der Genehmigenden und der Gründe für die Gewährung von privilegiertem Zugang.

Erteilung von privilegierten Zugriffsrechten

1. Zuteilung von privilegierten Zugriffsrechten an autorisierte Benutzer auf der Grundlage ihrer genehmigten Rollen und Verantwortlichkeiten.
2. Sicherstellung, dass privilegierte Zugriffsrechte ereignisbezogen und nach dem Grundsatz der geringsten Privilegierung gewährt werden.

Bewusstsein der Benutzer:

1. Informieren Sie die Benutzer über ihren privilegierten Zugriffsstatus und die mit dem Betrieb im privilegierten Modus verbundenen Verantwortlichkeiten.
2. Einführung von Maßnahmen, die visuell anzeigen, wenn Benutzer mit privilegiertem Zugang arbeiten.

Anforderungen an die Authentifizierung:

1. Einführung verschärfter Authentifizierungsmaßnahmen für den privilegierten Zugang, einschließlich einer erneuten Authentifizierung oder einer verstärkten Authentifizierung, falls erforderlich.
2. Sicherstellen, dass sich die Benutzer angemessen authentifizieren, bevor sie privilegierte Aufgaben ausführen.

Regelmäßige Bewertungen:

1. Durchführung regelmäßiger Überprüfungen, um festzustellen, ob die Benutzer weiterhin für privilegierte Zugangsrechte in Frage kommen.
2. Überprüfen Sie privilegierte Zugriffsrechte nach organisatorischen Änderungen, wie z. B. Rollenwechsel oder Kündigungen.

Entmutigung von generischen IDs:

1. Verboten Sie die Verwendung allgemeiner Administrator-Benutzerkennungen wie "root", "Administrator", "cisco" oder "admin".
2. Schutz der Authentifizierungsinformationen für privilegierte Identitäten, um unberechtigten Zugriff zu verhindern.

Temporärer privilegierter Zugriff:

1. Gewährung eines zeitlich begrenzten privilegierten Zugriffs für bestimmte Aufgaben oder Aktivitäten mit zeitlich begrenzten Rechten.
2. Verwenden Sie "Break-Glass"-Verfahren oder Technologien zur Verwaltung von Zugriffsrechten, um den vorübergehenden Zugang zu verwalten.
3. Verwenden Sie Passwort-Tresore und lange Passwörter (15+ Zeichen, komplexe, nicht wörterbuchartige Passwörter).

Protokollierung und Überwachung:

1. Stellen Sie sicher, dass alle privilegierten Zugriffe auf Systeme zu Prüfungs- und Überwachungszwecken protokolliert werden.
2. Überwachen Sie privilegierte Zugriffsaktivitäten auf Anomalien oder nicht autorisierte Aktionen.

Identitätsmanagement:

1. Vermeiden Sie die gemeinsame Nutzung oder Verknüpfung privilegierter Zugriffsrechte durch mehrere Personen.
2. Weisen Sie Personen, die einen besonderen privilegierten Zugang benötigen, separate Identitäten zu.

Nutzungsbeschränkungen:

Weisen Sie die Benutzer an, privilegierte Identitäten nur für Verwaltungsaufgaben und nicht für Routinetätigkeiten wie E-Mail oder Webbrowsing zu verwenden.

Dokumentation:

Dokumentieren Sie alle gewährten privilegierten Zugriffsrechte, einschließlich der Identitäten der Benutzer, der autorisierten Aufgaben und der Dauer des Zugriffs.

Schulung und Sensibilisierung:

a) Schulung der Benutzer über die ordnungsgemäße Nutzung des privilegierten Zugangs und die Bedeutung der Aufrechterhaltung von Sicherheitskontrollen.

b) Regelmäßige Übermittlung von Aktualisierungen und Erinnerungen bezüglich der Richtlinien und Verfahren für den privilegierten Zugang.

3.4 Zugang zum Quellcode

3.4.1 Richtlinie

Der Zugang zu Quellcode, Entwicklungswerkzeugen und Softwarebibliotheken muss kontrolliert werden, um die Einführung nicht autorisierter Funktionen, unbeabsichtigte oder böswillige Änderungen zu verhindern und die Vertraulichkeit wertvollen geistigen Eigentums zu wahren.

3.4.2 Verfahren

1. Mitarbeiter, die Zugang zu Quellcode, Entwicklungswerkzeugen oder Softwarebibliotheken benötigen, müssen über den dafür vorgesehenen Kanal einen formellen Zugangsantrag stellen, in dem der Grund für den Zugang und die erforderliche Dauer angegeben sind.
2. Zugriffsanträge sollten von der zuständigen Behörde auf der Grundlage der Rolle, der Verantwortlichkeiten und der geschäftlichen Anforderungen des Antragstellers genehmigt werden.

[Prüfen und bestätigen Sie, dass dieses Verfahren korrekt ist, und konkretisieren Sie es entsprechend Ihrer Organisation]

Zugangsgewährung:

1. Der Zugang zum Quellcode, zu Entwicklungswerkzeugen oder Softwarebibliotheken darf nur autorisierten Entwicklern durch den zuständigen Administrator oder das Zugangskontrollteam gewährt werden.
2. Die Zugriffsberechtigungen werden nach dem Prinzip des geringsten Privilegs konfiguriert, so dass sichergestellt ist, dass Personen nur auf die Informationen zugreifen können, die sie zur Erfüllung ihrer Aufgaben benötigen.

Prozess des Änderungsmanagements:

1. Alle Änderungen am Quellcode, an Entwicklungswerkzeugen oder Softwarebibliotheken müssen dem etablierten Änderungsmanagement/DevOps-Prozess folgen.
2. Änderungen sollten dokumentiert werden, wobei Einzelheiten wie der Grund für die Änderung, die verantwortliche(n) Person(en), Ticketnummern, Projektcode und das Datum der Umsetzung anzugeben sind.
3. Die Genehmigung für Änderungen sollte vor der Umsetzung von den entsprechenden Interessengruppen eingeholt werden.

Überwachung und Protokollierung:

1. Es sollte ein Audit-Protokoll geführt werden, in dem alle Zugriffe und Änderungen an Quellcode, Entwicklungswerkzeugen und Softwarebibliotheken festgehalten werden.
2. Das Audit-Protokoll sollte Details wie Benutzeridentitäten, Zeitstempel, zugegriffene Ressourcen und durchgeführte Aktionen erfassen.
3. Die Zugriffsprotokolle sollten regelmäßig überwacht werden, um unbefugte Zugriffsversuche oder verdächtige Aktivitäten zu erkennen.

3.5 Beschränkung des Informationszugangs

3.5.1 Richtlinie

Um sicherzustellen, dass der Zugang zu sensiblen Informationen eingeschränkt wird, muss nur der rechtmäßige Zugang ausdrücklich erlaubt werden, um den unbefugten Zugang zu sensiblen Informationen und Werten zu verhindern.

3.5.2 Verfahren

Identitätsbasierte Zugangskontrollen:

1. Zuweisung eindeutiger Benutzeridentitäten oder Rollen an Einzelpersonen oder Gruppen auf der Grundlage ihrer funktionalen Aufgaben und Zuständigkeiten.

2. Definieren Sie die den Funktionsgruppen zugeordneten Zugangsbereiche.
3. Integration der Bereitstellung und Aufhebung von physischen Zugangskontrollen in den Prozess der An- und Abmeldung von Mitarbeitern und Änderungen.

Physische und logische Zugangskontrollen:

1. Führen Sie physische Zugangskontrollen ein, wie z. B. biometrische Authentifizierung, Zugangskarten oder Schlüsselschlösser, um den physischen Zugang zu sensiblen Gütern und Einrichtungen zu beschränken.
2. Einsatz von logischen Zugangskontrollen, einschließlich Firewalls, Systemen zur Erkennung von Eindringlingen und Verschlüsselungsprotokollen, um in digitalen Systemen und Netzwerken gespeicherte Informationen zu schützen.
3. Gewährleistung der Aufgabentrennung und der Trennung von Privilegien zur Verhinderung des unbefugten Zugriffs oder Missbrauchs von Informationsbeständen.

Dokumentation und Berichterstattung:

1. Detaillierte Aufzeichnungen über Zugriffsberechtigungsentscheidungen, Zugriffskontrollkonfigurationen und Prüfungsergebnisse zu führen.
2. Erstellung regelmäßiger Berichte über Zugangskontrollaktivitäten, einschließlich Zugangsanfragen, Genehmigungen, Änderungen und Vorfälle.
3. Dokumentieren Sie alle Änderungen oder Aktualisierungen von Zugriffskontrollrichtlinien, -verfahren oder -konfigurationen für zukünftige Referenz- und Compliance-Zwecke.

4. Norm-Referenzen

4.1 Normreferenzen zu ISO27001:2022

Kapitel in diesem Dokument	Normkapitel (ISO27001:2022)
1. Einleitung	
2. Identität und Authentifizierung	
• 2.1 Identitätsmanagement	A 5.16
• 2.2 Informationen zur Authentifizierung	A 5.17; A 8.1
• 2.3 Sichere Authentifizierung	A 8.5
3. Physische und logische Zugangskontrolle	
• 3.1 Zugangskontrolle	A 5.15
• 3.2 Zugangsrechte	A 5.18
• 3.3 Privilegierte Zugriffsrechte	A 8.2
• 3.4 Zugang zu Quellcode	A 8.4
• 3.5 Beschränkung des Informationszugangs	A 8.3

4.2 Referenzen zu TISAX-ISA 6.0

Kapitel in diesem Dokument	Normkapitel (ISA-TISAX 6.0)
1. Einleitung	
2. Identität und Authentifizierung	
• 2.1 Identitätsmanagement	4.1.1
• 2.2 Informationen zur Authentifizierung	4.1.3; 4.2.1
• 2.3 Sichere Authentifizierung	4.1.2
3. Physische und logische Zugangskontrolle	
• 3.1 Zugangskontrolle	3.1.1; 4.1.2
• 3.2 Zugangsrechte	4.1.1; 4.1.3; 4.2.1
• 3.3 Privilegierte Zugriffsrechte	4.2.1
• 3.4 Zugang zu Quellcode	5.3.1
• 3.5 Beschränkung des Informationszugangs	4.1.3; 5.3.1