[Name der Organisation]

ST10 Handbuch zur physischen Sicherheit

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 Ihre 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 Kennnisnahme eliminiert oder inhaltlich angepasst werden. Beispiel: Bitte eliminieren Sie diese Seite vor Veröffentlichung der Richtlinie.]

1 Einleitung

Das Handbuch zum Management der physischen Sicherheit für [Name der Organisation] stellt einen konsolidierten Rahmen dar, der unsere Strategie für die wirksame Verwaltung und Sicherung unserer physischen Sicherheitsmaßnahmen umreißt. Es dient als umfassender Leitfaden, in dem detailliert dargelegt wird, wie unsere Organisation verschiedene Sicherheitsherausforderungen im Zusammenhang mit der physischen Sicherheit in unserem gesamten Betrieb angehen wird. Darüber hinaus dient es als übergeordnetes Dokument, das den Ansatz der Organisation für das Management der physischen Sicherheit umreißt.

[**Hinweis:** In diesem Handbuch werden mehrere Richtlinien behandelt, die einen direkten Einfluss auf das Mitarbeiter-Sicherheitshandbuch haben. Berücksichtigen Sie daher bei Ihren Anpassungen stets auch erforderliche Anpassungen im Mitarbieterhandbuch Informationssicherheit (DataGuard Policy-Vorlage ST4)]

1.1 Zweck und Umfang

Das Hauptziel dieses Richtlinienpakets besteht darin, einen strukturierten Ansatz für das Management der physischen Sicherheit festzulegen, um die sensiblen Informationen, Vermögenswerte und den Ruf unserer Organisation zu schützen. Durch die Einhaltung dieser Richtlinie wollen wir unsere Widerstandsfähigkeit gegen Sicherheitsverletzungen erhöhen und das Risiko von Störungen oder Kompromittierungen innerhalb unserer physischen Sicherheitsinfrastruktur minimieren.

1.2 Anwendbarkeit

Diese Richtlinie gilt für alle Mitarbeiter und Beteiligten und stellt sicher, dass sie sich an die festgelegten Richtlinien für das physische Sicherheitsmanagement halten. Die Sicherheitsabteilung hat in Zusammenarbeit mit den zuständigen Abteilungen die Aufgabe, die Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung der in diesem Richtlinienpaket beschriebenen Verfahren zu überwachen.

2 Physische Sicherheitsbedingungen und Einrichtungen

2.1 Physische Sicherheitsperimeter

2.1.1 Richtlinie

Um die Informationen der Organisation und die damit verbundenen Vermögenswerte vor unbefugtem physischem Zugriff, Beschädigung und Störung zu schützen, ist es unerlässlich, robuste physische Sicherheitsperimeter um unsere Einrichtungen zu gestalten.

2.1.2 Verfahren

[Prüfen Sie, dass dieses Verfahren mit Ihrer Organisation übereinstimmt und konkretisieren es ggf. In diesem Verfahren geht es darum, wie Sie sicherstellen, dass die Sicherheitsbereiche geschützt werden]

Festlegung von Sicherheitsperimetern:

1. Führen Sie eine Bewertung durch, um Bereiche zu ermitteln, die sensible Informationen enthalten.
2. Legen Sie auf der Grundlage der Bewertung die Sicherheitsgrenzen um sensible Bereiche fest.
3. Berücksichtigen Sie bei der Festlegung der Grenzen eines jeden Bereichs die Anforderungen an die Informationssicherheit im Zusammenhang mit den Vermögenswerten innerhalb dieses Bereichs. [Beispiele hierfür sind Räumlichkeiten, die Konfigurationsinformationen zu Verschlüsselung und Datenmaskierung enthalten. Wenn solche Anforderungen an Räume gestellt werden, sollen sie sich wahrscheinlich innerhalb der Grenzen befinden, in denen Sicherheitsmaßnahmen implementiert werden. Weitere Beispiele sind Server-Räume, Buchhaltungsabteilungen, Personalabteilungen und Archive].

4. Dokumentieren Sie die festgelegten Grenzen und teilen Sie sie allen Beteiligten mit.
   [Bitte erstellen Sie zur Dokumentation einen entsprechenden Plan, aus dem die jeweiligen Bereichsgrenzen innerhalb Ihrer Liegenschaften, sowie deren Klassifikationen ersichtlich werden]

Baulicher Schutz von Sicherheitsbereichen:

1. Vergewissern Sie sich, dass die Außendächer, Wände, Decken und Fußböden der Räumlichkeiten solide gebaut sind.
2. Installieren Sie an allen Außentüren geeignete Kontrollmechanismen, um unbefugten Zugang zu verhindern. Diese Mechanismen können Gitter, Alarme oder Schlösser umfassen.
3. Führen Sie eine Mitarbeiterrichtlinie ein, die sicherstellt, dass alle Türen und Fenster verschlossen sind, wenn sie unbeaufsichtigt sind. [Ist Bestandteil des Mitarbeiter-Sicherheitshandbuchs]
4. Bringen Sie einen Außenschutz für die Fenster an, insbesondere für die ebenerdigen.
5. Sichern Sie alle Lüftungsöffnungen, um unbefugtes Eindringen zu verhindern.
6. Regelmäßige Inspektion des physischen Zustands der Abgrenzungen und Durchführung der erforderlichen Wartungsarbeiten.

Alarmüberwachung und -prüfung:

1. Installieren Sie Alarmsysteme an allen Grenztüren zu Sicherheitsbereichen.
2. Überwachen und testen Sie die Alarme regelmäßig, achten Sie auf die Stärke der Wände, um den erforderlichen Widerstandsgrad zu ermitteln.
3. Stellen Sie sicher, dass die Alarmsysteme ausfallsicher arbeiten. Für den Fall, dass ein System ausfällt, soll ein Backup-System vorhanden sein.
4. Dokumentieren Sie alle Alarmtests und alle als Reaktion auf die Testergebnisse ergriffenen Maßnahmen.
5. Schulen Sie das Personal entsprechend der richtigen Reaktion auf Alarmauslösungen.

2.2 Physischer Zugang

2.2.1 Richtlinie

Zugangspunkte wie Liefer- und Ladebereiche und andere Punkte, an denen Unbefugte das Gelände betreten können, sollen kontrolliert und, wenn möglich, von den Informationsverarbeitungseinrichtungen getrennt werden, um unbefugten Zugang zu verhindern.

Besuche sollen dokumentiert werden, Besucher sollen sich entsprechend ausweisen und beaufsichtigt und angewiesen werden, welches Verhalten erwartet wird (unter anderem Unterlassung von Ton- Bild und Datenaufnahmen). Anlieferungs- und Ladebereiche sollen nur für befugtes Personal zugänglich sein.

2.2.2 Verfahren

[Prüfen Sie, dass dieses Verfahren mit Ihrer Organisation übereinstimmt und konkretisieren es ggf. In diesem Verfahren geht es darum, wie Sie verwalten wollen, wer wann Zugang zu was hat, angefangen von Mitarbeitern der Organisation bis hin zu Besuchern/Gästen.]

Personalzugang:

1. Beschränken Sie den Zugang zu Standorten und Gebäuden auf befugtes Personal. Verwalten Sie Zugangsrechte durch Erteilung, regelmäßige Überprüfung, Aktualisierung und Entzug von Berechtigungen und dokumentieren dies entsprechend.
2. Führen und überwachen Sie ein physisches Logbuch oder einen elektronischen Prüfpfad für alle Zugriffe. Schützen Sie alle Protokolle und sensiblen Authentifizierungsdaten.
3. Implementieren Sie ein Verfahren und technischer Mechanismen für die Verwaltung des Zugangs zu Bereichen ein, in denen Informationen verarbeitet oder gespeichert werden. Verwenden Sie zur Authentifizierung Zugangskarten, biometrische Daten oder eine Zwei-Faktor-Authentifizierung. Erwägen Sie doppelte Sicherheitstüren für den Zugang zu sensiblen Bereichen.
4. Richten Sie einen personell oder anderweitig überwachten Empfangsbereich ein, um den physischen Zugang zum Gelände oder Gebäude zu kontrollieren.

5. Kontrollieren Sie persönliche Gegenstände des Personals und interessierter Parteien beim Betreten und Verlassen (Speichermedien, Kameras, Aufnahmegeräte).
6. Verlangen Sie von allen Mitarbeitern und Interessenten einen sichtbaren Ausweis. Verlangen Sie von allen, dass unmittelbare Information erfolgt, wenn Besucher ohne Begleitung sind und über Personen, die keinen sichtbaren Ausweis tragen.
7. Gewähren Sie dem Personal des Lieferanten nur bei Bedarf beschränkten Zugang zu Sicherheitsbereichen oder Informationsverarbeitungseinrichtungen. Dieser Zugang soll genehmigt und überwacht werden.
8. Achten Sie besonders auf die Sicherheit des physischen Zugangs zu Gebäuden, in denen sich Vermögenswerte für mehrere Organisationen befinden.
9. Planen Sie physische Sicherheitsmaßnahmen, die verstärkt werden, wenn die Wahrscheinlichkeit physischer Zwischenfälle steigt.
10. Sichern Sie andere Zugänge wie Notausgänge vor unbefugtem Zugriff.
11. Führen Sie eine dokumentierte Schlüsselverwaltung, um die Steuerung von physischen Schlüsseln oder Authentifizierungsinformationen sicherzustellen. Führen Sie ein Logbuch und machen Sie eine jährliche physische Schlüsselprüfung.

Besucherzugang:

1. Sorgen Sie für eine Authentifizierung der Identität der Besucher durch ein geeignetes Mittel.
2. Notieren Sie das Datum und die Uhrzeit des Zutritts und des Verlassens von Besuchern.
3. Gewähren Sie Besuchern nur zu bestimmten, genehmigten Zwecken. Geben Sie Besuchern Anweisungen zu den Sicherheitsanforderungen des Bereichs und zu entsprechendem Verhalten bei Notfällen.
4. Beaufsichtigen Sie alle Besucher, es sei denn, es wird eine ausdrückliche Ausnahme gewährt.

Zugang zu Liefer- und Ladebereichen:

1. Beschränken Sie den Zugang zu Liefer- und Ladebereichen von außerhalb des Gebäudes auf bestimmtes und befugtes Personal.
2. Gestalten Sie die Anlieferungs- und Ladebereiche so, dass Lieferungen ein- und ausgeladen werden können, ohne dass das Lieferpersonal unbefugten Zugang zu anderen Gebäudeteilen erhält.
3. Sichern Sie die Außentüren von Liefer- und Ladebereichen, wenn die Türen zu Sicherheitsbereichen geöffnet werden.
4. Prüfen und untersuchen Sie eingehende Lieferungen auf Sprengstoffe, Chemikalien oder andere gefährliche Stoffe, bevor sie aus den Liefer- und Ladebereichen weitergeleitet werden.
5. Registrieren Sie eingehende Lieferungen gemäß den Verfahren der Warenwirtschaft bei der Ankunft am Standort.
6. Trennen Sie eingehende und ausgehende Sendungen, soweit möglich, physisch voneinander.

Untersuchen Sie eingehende Lieferungen auf Anzeichen von Manipulationen während des Transports. Werden Manipulationen entdeckt, sollen sie sofort gemeldet werden.

2.3 Sicherung von Büros, Räumen und Anlagen.

2.3.1 Richtlinie

Um unbefugten physischen Zugang, Beschädigung und Beeinträchtigung der Informationswerte der Organisation und anderer zugehöriger Vermögenswerte in Büros, Räumen und Einrichtungen zu verhindern, müssen physische Sicherheitskontrollen zur Sicherung von Büros, Räumen und Einrichtungen durchgeführt werden.

2.3.2 Verfahren

[Prüfen Sie, dass dieses Verfahren mit Ihrer Organisation übereinstimmt und konkretisieren es ggf. Dieses Verfahren bezieht sich speziell auf die Verwaltung von physischen Räumen wie Büros, Aufenthaltsräumen und anderen Einrichtungen in der Organisation.]

Standortwahl für kritische Einrichtungen:

1. Ermitteln Sie kritische Einrichtungen innerhalb der Organisation, die eine erhöhte physische Sicherheit erfordern.
2. Wählen Sie Standorte für diese Einrichtungen, die der Öffentlichkeit nicht zugänglich sind, um das Risiko eines unbefugten Eindringens oder einer Störung zu minimieren.

Wirkung des Gebäudes und Beschilderung:

1. Stellen Sie sicher, dass Gebäude, in denen kritische Einrichtungen untergebracht sind, unauffällig sind und nicht offen auf ihren Zweck hinweisen.
2. Vermeiden Sie die Verwendung von Schildern, sowohl außerhalb als auch innerhalb des Gebäudes, die auf die Anwesenheit von Informationsverarbeitungstätigkeiten hinweisen.
3. Überprüfen und aktualisieren Sie die Beschilderung regelmäßig, um sicherzustellen, dass sie mit dieser Richtlinie übereinstimmt.

Beschaffenheit der Einrichtungen:

1. Ergreifen Sie Maßnahmen, um zu verhindern, dass vertrauliche Informationen oder Aktivitäten von außen sichtbar oder hörbar sind. Dazu gehören Fensterverkleidungen, Schalldämmung und die sichere Entsorgung vertraulicher Abfälle.
2. Berücksichtigen Sie den Bedarf an elektromagnetischer Abschirmung in Abhängigkeit von der Art der in der Einrichtung verarbeiteten Informationen.

Kontrolle von Informationen über Einrichtungen:

1. Schränken Sie die Verfügbarkeit von Verzeichnissen, internen Telefonverzeichnissen und digitalen Gebäudeplänen ein, auf denen die Standorte von Einrichtungen zur Verarbeitung vertraulicher Informationen verzeichnet sind.
2. Beschränken Sie den Zugriff zu diesen Informationen nur auf befugtes Personal.
3. Überprüfen Sie regelmäßig die Zugriffsrechte auf diese Informationen und widerrufen Sie sie, falls erforderlich.

Zusätzliche Sicherheitsmaßnahmen:

1. Führen Sie auf der Grundlage von Risikobewertungen je nach Bedarf zusätzliche Sicherheitsmaßnahmen ein. Dazu könnten Videoüberwachung, Zugangskontrollsysteme, Alarmsysteme usw. gehören.
2. Stellen Sie sicher, dass diese Maßnahmen mit der Art und Sensibilität der in der Einrichtung verarbeiteten Informationen und dem bestehenden Kontrollumfeld in Einklang stehen.

2.4 Überwachung der physischen Sicherheit

2.4.1 Richtlinie

Das Unternehmen muss den unbefugten physischen Zugang zu den Räumlichkeiten der Organisation ständig Überwachen und schützen.

Verfahren

[Bitte prüfen Sie, dass dieses Verfahren mit Ihrer Organisation übereinstimmt und konkretisieren es ggf. Dieses Verfahren regelt, wie Sie Sicherheitsbereiche permanent überwachen. Meist erfolgt das durch Videoüberwachung. Es bestehen aber auch andere Methoden. Dieses Verfahren regelt auch die Wartung und Verwaltung der Videoüberwachungsanlagen, da diese mit eigenen Risiken wie Ausfallzeiten oder Störungen verbunden sind].

Installation und Einrichtung von Überwachungsanlagen:

1. Identifizieren Sie kritische Bereiche innerhalb und außerhalb der Räumlichkeiten der Organisation, die überwacht werden müssen. Beraten Sie sich mit der Personalabteilung über erfasste Bereiche und Umsetzung der Aufzeichnung.
2. Installieren Sie Überwachungskameras an strategischen Orten, um Zugänge, sensible Bereiche und Umzäunungen zu überwachen.
3. Stellen Sie eine korrekte Ausrichtung und Konfiguration der CCTV (Closed Circuit Television)-Kameras für eine optimale Abdeckung und Aufzeichnung sicher.
4. Testen Sie die Funktionalität von CCTV-Systemen, um den ordnungsgemäßen Betrieb und die Videoaufzeichnungsmöglichkeiten zu überprüfen.

Einsatz von Einbruchmeldeanlagen:

1. Bestimmen Sie erforderliche Einbruchmeldeanlagen auf der Grundlage der Risikobewertung und der Sicherheitsanforderungen.
2. Installieren Sie Kontaktmelder an Fenstern, Türen und anderen Eingängen, um bei unbefugtem Zutritt einen Alarm auszulösen.
3. Einsatz von Bewegungsmeldern mit Infrarottechnologie zur Erkennung von Bewegungen und Auslösung von Alarmen in bestimmten Bereichen.
4. Installieren Sie Sensoren, die auf das Geräusch von zerbrechendem Glas reagieren, um einen Alarm auszulösen und das Sicherheitspersonal im Falle eines versuchten Einbruchs zu alarmieren.
5. Achten Sie auf die richtige Platzierung und Kalibrierung der Alarmkomponenten, um Fehlalarme zu minimieren und die Erkennungsgenauigkeit zu maximieren.

Alarmanlagen-Bedienelemente:

1. Bringen Sie die Bedienfelder der Alarmanlage an sicheren und alarmgesicherten Orten an, um unbefugten Zugang oder Manipulationen zu verhindern.
2. Bringen Sie die Schalttafeln so an, dass sie für befugtes Personal leicht zugänglich sind.
3. Implementieren Sie manipulationssichere Mechanismen an Schalttafeln und Meldern, um eine Manipulation oder Deaktivierung des Systems zu verhindern.
4. Testen Sie regelmäßig die Funktionstüchtigkeit der Alarmanlagenzentralen, um sicherzustellen, dass sie ordnungsgemäß funktionieren und auf ausgelöste Alarme reagieren.

CCTV-Überwachungsmaßnahmen:

1. Beauftragen Sie geschultes Personal oder Sicherheitspersonal mit der Überwachung von Live-Übertragungen der Videoüberwachung und der Reaktion auf Alarmmeldungen.
2. Kontinuierliche Überwachung von Zugangspunkten, sensiblen Bereichen und Perimetern auf Anzeichen von unbefugten Aktivitäten oder Eindringlingen.
3. Aufzeichnung und Aufbewahrung des Überwachungsmaterials gemäß den geltenden Gesetzen und Vorschriften, Gewährleistung der ordnungsgemäßen Handhabung und Speicherung der aufgezeichneten Videodaten.
4. Einführung von Verfahren zur Überprüfung und Analyse von Überwachungsmaterial als Reaktion auf Sicherheitsvorfälle oder Untersuchungen.

Regelmäßige Wartung und Prüfung:

1. Führen Sie routinemäßige Wartungen an Überwachungssystemen, CCTV-Kameras und Einbruchmeldeanlagen durch, um eine optimale Leistung sicherzustellen.
2. Führen Sie Planmäßige Tests von Alarmkomponenten, einschließlich Kontaktmeldern, Bewegungssensoren und Glasbruchsensoren, um die Funktionalität und Reaktionsfähigkeit zur Überprüfung durch.
3. Beheben Sie festgestellte Probleme oder Fehlfunktionen umgehend durch Reparaturen, Austausch oder Anpassungen, um die Wirksamkeit des Überwachungssystems aufrechtzuerhalten.

Einhaltung der Vorschriften und Dokumentation:

1. Stellen Sie die Einhaltung der einschlägigen Gesetze, Vorschriften und Organisationsrichtlinien für die Überwachung von Räumlichkeiten und Überwachungsaktivitäten sicher.
2. Führen Sie zu Dokumentations- und Prüfungszwecken genaue Aufzeichnungen über die Konfiguration von Überwachungssystemen, Alarmsystemtests, Wartungsaktivitäten und Reaktionen auf Vorfälle.
3. Regelmäßige Überprüfung und Aktualisierung der Verfahren in Übereinstimmung mit Änderungen der Sicherheitsanforderungen, technologischen Fortschritten oder gesetzlichen Vorgaben.

Schulung und Sensibilisierung:

1. Führen Sie umfassende Schulung des Personals durch, das für die Überwachung und Verwaltung von Überwachungssystemen, Einbruchalarmanlagen und Sicherheitsmaßnahmen zuständig ist.
2. Sensibilisieren Sie Mitarbeiter für die Bedeutung der physischen Sicherheit und die Rolle der Überwachung bei der

Abschreckung von unbefugtem Zutritt und dem Schutz der Vermögenswerte der Organisation.

3. Führen Sie regelmäßige Schulungen und Übungen durch, um die Bereitschaft und Wirksamkeit des Sicherheitspersonals bei der Reaktion auf Sicherheitsvorfälle und Alarme zu testen.

Reaktion auf Zwischenfälle und Eskalation:

1. Legen Sie klare Verfahren für die Reaktion auf Sicherheitsvorfälle fest, die durch Überwachungssysteme oder ausgelöste Alarme festgestellt werden.

2. Definieren Sie Eskalationspfade und Kommunikationsprotokolle für die Benachrichtigung des zuständigen Personals, einschließlich der Sicherheitsteams, der Geschäftsleitung und der Strafverfolgungsbehörden, soweit erforderlich. [Verweisen Sie hier auf Ihre bestehenden Richtlinien für die Vorfallbehandlung (DataGuard Policy-Vorlage ST8) hin.]

Dokumentieren und melden Sie Sicherheitsvorfälle, einschließlich versuchter Sicherheitsverletzungen oder unbefugten Zugriffs, in Übereinstimmung mit den festgelegten Verfahren zur Reaktion auf Vorfälle und den gesetzlichen Anforderungen.

2.5 Schutz vor physischen und umweltbedingten Bedrohungen.

2.5.1 Richtlinie

Das Unternehmen muss seine Informationen schützen, indem es sich gegen physische und umweltbedingte Gefahren absichert, um die potenziellen Auswirkungen zu verringern. Zu den Risiken gehören Naturkatastrophen und geplante Angriffe bis hin zu unbeabsichtigten Ereignissen.

Verfahren

[Bitte prüfen Sie, ob dieses Verfahren Ihren offiziellen Geschäftsprozessen entspricht und konkretisieren es ggf. In diesem Verfahren wird erläutert, wie Sie Risikobewertungen vornehmen und physische Bedrohungen wie Feuer, Überschwemmungen, Wirbelstürme usw. behandeln.]

Risikobewertung:

1. Führen Sie initial und wiederkehrend umfassende Risikobewertungen von physischen Standorten durch, bevor Sie an ihnen kritische Vorgänge durchführen.

2. Identifizieren Sie potenzielle physische und umweltbedingte Bedrohungen, einschließlich Naturkatastrophen, vorsätzlicher Angriffe und unbeabsichtigter Zwischenfälle.

3. Bewerten Sie potenzielle Folgen der festgestellten Bedrohungen für die Infrastruktur, die Informationsverarbeitungssysteme und das Personal.

Fachliche Beratung:

1. Lassen Sie sich von Fachleuten oder Experten aus den entsprechenden Gebieten beraten, um die mit physischen und ökologischen Bedrohungen verbundenen Risiken zu verstehen und zu bewältigen.

2. Holen Sie Anleitung zur Durchführung geeigneter Kontrollen und Maßnahmen zur wirksamen Minderung der festgestellten Risiken ein.

Kontrolle der Umsetzung:

1. Führen Sie auf der Grundlage der Ergebnisse der Risikobewertung und der Beratung durch Fachleute die erforderlichen Sicherheitsvorkehrungen und Kontrollen ein, um die festgestellten Bedrohungen zu mindern.

2. Stellen Sie sicher, dass die Kontrollen auf die spezifischen Risiken zugeschnitten und für das betriebliche Umfeld der Organisation geeignet sind.

[Im Folgenden finden Sie einige Beispiele für die Durchführung von Kontrollen. Stellen Sie sicher, dass Sie das Risiko (z. B. Überschwemmungen) und die zur Verringerung dieses Risikos eingerichteten Maßnahmen (z. B. Hochwassererkennungssysteme) erläutern.

1. *Feuer:*

- *Installieren und konfigurieren Sie Brandmeldesysteme, die eine Früherkennung ermöglichen.*
    - *Einrichtung von automatischen Alarmauslösungsmechanismen und Brandbekämpfungssystemen.*
    - *Regelmäßige Prüfung und Wartung der Brandmelde- und Brandbekämpfungsanlagen.*

1. *Überschwemmung:*
    a. *Installation von Hochwassermeldesystemen in gefährdeten Gebieten. Bereitstellung von Wasserpumpen oder gleichwertigen Mitteln zur Bewältigung von Überschwemmungen.*
    b. *Festlegung von Verfahren zur Reaktion auf Hochwasserwarnungen und zur wirksamen Bewältigung von Hochwasserereignissen.*
2. *Elektrische Überspannung:*
    a. *Einsatz von Überspannungsschutzgeräten für kritische Informationssysteme und -geräte.*
    b. *Regelmäßige Durchführung von Wartungskontrollen der Überspannungsschutzsysteme.*
    c. *Schulung des Personals im Erkennen und Reagieren auf Überspannungsereignisse.*
3. *Sprengstoffe und Schusswaffen:*
    a. *Durchführung von Sicherheitsmaßnahmen, wie z. B. Personen- und Fahrzeugkontrollen, an den Zufahrten zu Einrichtungen.*
    b. *Durchführung von Stichprobenkontrollen auf das Vorhandensein von Sprengstoff oder Waffen im Rahmen der Sicherheitsprotokolle.]*

Einhaltung und Überwachung:

1. Stellen Sie sicher, dass das gesamte Personal die etablierten Kontrollen und Verfahren zum Umgang mit physischen und umweltbedingten Bedrohungen kennt und einhält.
2. Überwachen Sie regelmäßig die Wirksamkeit der durchgeführten Kontrollen und deren regelmäßige Überprüfung, um neu auftretende Bedrohungen oder Änderungen im betrieblichen Umfeld zu berücksichtigen.

Dokumentation und Aufbewahrung von Unterlagen:

1. Führen Sie eine Dokumentation der Risikobewertungen, der Beratungen mit Fachleuten und der Durchführung von Kontrollen.
2. Führen Sie Aufzeichnungen über die Bewertung der Wirksamkeit von Kontrollen, über Vorfälle und über alle Aktualisierungen oder Überarbeitungen von Verfahren.

Schulung und Sensibilisierung:

1. Schulen Sie Personal im Erkennen, Reagieren und Entschärfen von physischen und umweltbedingten Bedrohungen.
2. Sensibilisieren Sie Personal für die Bedeutung der Einhaltung der festgelegten Verfahren und der Wachsamkeit gegenüber potenziellen Bedrohungen.

3 Besondere physische Arbeitsumgebungen

3.1 Arbeiten in Sicherheitsbereichen

3.1.1 Richtlinie

Zum Schutz der Informationen muss das Unternehmen Sicherheitsmaßnahmen für das in Sicherheitsbereichen arbeitende Personal festlegen, um die Informationen und die damit verbundenen Werte vor Schäden und unbefugten Eingriffen zu schützen.

Verfahren

[Bitte prüfen Sie, dass dieses Verfahren mit Ihrer Organisation übereinstimmt und konkretisieren es ggf. In diesem Verfahren wird erläutert, wie Sie Ihre Organisation davor schützen, dass das Personal in den Sicherheitsbereichen, die Sie in Abschnitt 2.1 eingerichtet haben, arbeiten muss; dies reicht von der Frage, welchen Zugang sie haben sollen, bis hin zur Frage, wie es mit Objekten wie Türen und Schränken umgehen soll. Es gibt auch Hinweise darauf, welche Informationen sie kennen sollen und welche Geräte sie in diesen Sicherheitsbereichen nicht benutzen dürfen (z. B. Mobiltelefone).]

Zugangskontrolle:

1. Der Zugang zu Sicherheitsbereichen soll nur befugtem Personal vorbehalten sein.

2. Das Personal muss einen gültigen Ausweis oder Zugangsausweis vorlegen, bevor es die Sicherheitsbereiche betritt.
3. Die Zugriffsberechtigungen sollen regelmäßig überprüft und bei Bedarf aktualisiert werden.

Erfordernis von genereller Kenntnis:

1. Die Information über das Vorhandensein von oder die Aktivitäten in Sicherheitsbereichen sollen nur an Mitarbeiter weitergegeben werden, die davon Kenntnis haben müssen.
2. Das entsprechende Personal soll über die Sensibilität von Informationen in Sicherheitsbereichen und die Bedeutung der Wahrung der Vertraulichkeit unterrichtet werden.

Beaufsichtigung:

1. Arbeitstätigkeiten in Sicherheitsbereichen sollen überwacht werden, um die Einhaltung der Sicherheitsmaßnahmen zu gewährleisten.
2. Die Vorgesetzten sollen das Verhalten des Personals überwachen und eingreifen, wenn verdächtige oder unbefugte Aktivitäten beobachtet werden.

Verschluss und durchzuführende Inspektionen:

1. Sicherheitsbereiche, einschließlich Türen, Schränke und Lagereinheiten, sollen verschlossen werden, wenn sie nicht benutzt werden.
2. Regelmäßige Inspektionen der Sicherheitsbereiche sollen durchgeführt werden, um sicherzustellen, dass die physischen Sicherheitsmaßnahmen intakt sind und ordnungsgemäß funktionieren.

Verbotene Geräte:

1. Dem Personal ist es untersagt, Foto-, Video-, Audio- oder sonstige Aufnahmegeräte ohne Genehmigung in die Sicherheitsbereiche mitzubringen.
2. Die Endgeräte der Benutzer, z. B. Mobiltelefone und Laptops, sollen bei ihrem Eintreffen überprüft werden, um die Einhaltung der Richtlinien zur Gerätekontrolle sicherzustellen.

Verfahren für Notfälle:

1. In den Sicherheitsbereichen sollen an gut sichtbarer Stelle Notfallprozeduren ausgehängt werden, die die Evakuierungswege, Kontaktinformationen für Notfälle und Anweisungen für die Reaktion auf Sicherheitsvorfälle enthalten.
2. Das Personal soll sich mit den Notfallverfahren vertraut machen und etwaige Unregelmäßigkeiten oder Zwischenfälle umgehend melden.

Ausbildung:

1. Das gesamte Personal, das in Sicherheitsbereichen arbeitet, soll eine Schulung über Sicherheitsmaßnahmen, einschließlich Zugangskontrolle, Vertraulichkeit und Notfallverfahren, erhalten.
2. Vor dem erstmaligen Betreten eines Sicherheitsbereichs und in anschießenden regelmäßigen Abständen sollen Schulungen durchgeführt werden, um das Sicherheitsbewusstsein zu stärken.

Überwachung der Einhaltung der Vorschriften:

1. Die Einhaltung der Sicherheitsmaßnahmen soll durch regelmäßige Inspektionen, Audits und Beobachtungen überwacht werden.
2. Das Sicherheitspersonal kann Stichprobenkontrollen und Überwachungen durchführen, um die Einhaltung der Sicherheitsprotokolle zu gewährleisten.

Meldung von Vorfällen:

1. Das Personal soll alle Sicherheitsvorfälle, Verstöße oder Bedenken unverzüglich den zuständigen Behörden oder dem Sicherheitspersonal melden.
2. Berichte über Vorfälle sollen dokumentiert und umgehend untersucht werden, um die Risiken zu mindern und künftige Vorfälle zu verhindern.

3.2 Aufgeräumte Arbeitsbereiche

[Es gibt Maßnahmen, die sicherstellen, dass physische Daten wie Papier ordnungsgemäß aufbewahrt werden und nicht auf dem Schreibtisch liegen, wenn sie benötigt werden, bis hin zu einer korrekten Einrichtung des Schutzes für den PC-Bildschirm, einschließlich Antivirus und Verwaltung von Pop-ups. Da Phishing eines der größten Risiken für ein Unternehmen darstellt, ist es von entscheidender Bedeutung, dass Sie so viele dieser Kontrollen wie möglich in Betracht ziehen. Bitte prüfen Sie, dass dieses Verfahren mit Ihrer Organisation übereinstimmt und konkretisieren es ggf.]

3.2.1 Richtlinie

Zum Schutz der Informationen muss das Unternehmen klare Schreibtischregeln für Papiere und Wechseldatenträger sowie klare Bildschirmregeln für Informationsverarbeitungsgeräte aufstellen, um die Risiken des unbefugten Zugriffs, des Verlusts und der Beschädigung von Informationen während und außerhalb der normalen Arbeitszeiten zu verringern.

3.2.2 Verfahren

Verschluss sensibler Informationen:

1. Mitarbeiter, die für sensible oder kritische Geschäftsinformationen verantwortlich sind, sollen sicherstellen, dass diese Informationen sicher aufbewahrt werden, wenn sie nicht gebraucht werden.
2. Verwenden Sie Tresore, Schränke oder andere sichere Aufbewahrungsmöglichkeiten, um Papierdokumente und Wechseldatenträger mit vertraulichen Informationen wegzuschließen.
3. Bevor Sie Ihr Büro oder Ihren Arbeitsplatz verlassen, muss sichergestellt werden, dass alle sensiblen Informationen sicher aufbewahrt werden und für Unbefugte unzugänglich sind.

Schutz von Endpunktgeräten:

1. Sobald Endpunktgeräte der Benutzer nicht benutzt werden oder unbeaufsichtigt sind, soll das Personal sie mit Schlüsselschlössern oder anderen Sicherheitsmechanismen abschließen.
2. Stellen Sie sicher, dass die Endgeräte der Benutzer an sicheren Orten aufbewahrt werden, um unbefugten Zugriff oder Manipulationen zu verhindern.
3. Das Personal soll darin geschult werden, verdächtige Aktivitäten im Zusammenhang mit Benutzerendgeräten zu erkennen und zu melden.

Bildschirmsperrung und Abmeldung:

1. Die Endpunktgeräte der Benutzer sollen abgemeldet oder mit einem durch Benutzerauthentifizierung gesteuerten Bildschirm- und Tastatursperrmechanismus gesperrt werden, wenn sie unbeaufsichtigt sind.
2. Konfigurieren Sie alle Computer und Systeme mit einer Timeout- oder automatischen Abmeldefunktion, um einen unbefugten Zugriff bei Inaktivität zu verhindern.
3. Die Mitarbeiter sollen es sich zur Gewohnheit machen, ihre Geräte abzumelden oder zu sperren, sobald sie ihren Arbeitsplatz verlassen.

Druckernutzung:

1. Mitarbeiter, die Drucker verwenden, sollen ihre Druckerzeugnisse sofort aus Druckern oder Multifunktionsgeräten abholen.
2. Stellen Sie sicher, dass die Drucker mit Authentifizierungsfunktionen ausgestattet sind, um den Zugriff auf die Ausdrucke auf befugtes Personal zu beschränken.
3. Das Personal soll wachsam sein und alle unbefugten Versuche, auf Ausdrucke oder andere Ausgaben zuzugreifen, melden.

Sichere Lagerung und Entsorgung:

1. Bewahren Sie Dokumente und Wechseldatenträger mit sensiblen Informationen in ausgewiesenen sicheren Aufbewahrungsbereichen auf.
2. Wenn sensible Informationen nicht mehr benötigt werden, entsorgen Sie sie durch sichere Entsorgungsmechanismen wie Schreddern oder elektronisches Löschen.
3. Führen Sie Aufzeichnungen über die Entsorgungsaktivitäten in Übereinstimmung mit den organisatorischen Richtlinien und gesetzlichen Vorschriften.

Konfiguration von Bildschirm-Pop-up-Fenstern:

1. Das Personal soll Pop-up-Einstellungen auf Bildschirmen vornehmen, um die Anzeige sensibler Informationen in öffentlichen Bereichen oder bei Präsentationen/geteilten Bildschirmansichten zu minimieren.

2. Stellen Sie sicher, dass die Popup-Einstellungen so angepasst sind, dass ein unbefugtes Ansehen von E-Mails, Nachrichten oder anderen sensiblen Inhalten verhindert wird.

Gereinigte Whiteboards und Displays:

1. Das Personal soll sensible Informationen von Whiteboards und anderen Displays entfernen, wenn sie nicht mehr benötigt oder beaufsichtigt werden.

2. Verwenden Sie geeignete Löschmethoden, um die vollständige Entfernung von Informationen von Tafeln und Bildschirmen sicherzustellen.

3. Ermuntern Sie Ihr Personal, bei der Verwendung von Whiteboards und Bildschirmen für Diskussionen oder Präsentationen, eine angemessene Vorsicht und Diskretion walten zu lassen.

Schulung und Sensibilisierung:

1. Schulen Sie Personal in den in diesem Dokument beschriebenen Verfahren bei Eintritt in die Organisation und danach in regelmäßigen Abständen.

2. Sensibilisieren Sie Personal für die Relevanz aufgeräumter Schreibtisch- und Bildschirmmaßnahmen.

Verfahren bei Auflösung/Endreinigung von Einrichtungen:

1. Führen Sie eine abschließende Durchsuchung des Arbeitsbereichs durch, um sicherzustellen, dass alle sensiblen Informationen und Vermögenswerte ordnungsgemäß gesichert sind, bevor Sie die Räumlichkeiten verlassen.

2. Schauen Sie hinter Schubladen, unter Schreibtischen und in anderen versteckten Bereichen nach, um sicherzustellen, dass keine Dokumente oder Speichermedien zurückgelassen wurden.

3. Melden Sie den entsprechenden internen Stellen oder dem Sicherheitspersonal alle bei der Endreinigung entdeckten Sicherheitsbedenken oder Anomalien.

4 Ausstattung und Verkabelung

4.1 Standortwahl und Schutz von Ausstattung

4.1.1 Richtlinie

Um Informationswerte zu schützen, muss das Unternehmen dafür sorgen, dass Ausstattung sicher untergebracht und geschützt sind, um Risiken durch physische und umweltbedingte Bedrohungen sowie durch unbefugten Zugriff und Beschädigung zu mindern.

4.1.2 Verfahren

[Bitte prüfen Sie, ob dieses Verfahren Ihren offiziellen Geschäftsprozessen entspricht und konkretisieren es ggf. Dieses Verfahren regelt, wo Ausstattung bzw. Geräte aufbewahrt werden, wenn sie nicht in Gebrauch sind (z. B. Laptops, die über Nacht an einem sicheren Ort aufbewahrt werden), und wie man sich in der Nähe dieser Geräte verhält - z. B. nicht rauchen in der Nähe von brennbaren Gegenständen].

Sichere Platzierung der Ausstattung:

1. Bestimmen Sie geeignete Standorte für die Platzierung der Ausstattung, um den unnötigen Zugang zu den Arbeitsbereichen zu minimieren und den unbefugten Zugang zu verhindern.

2. Stellen Sie sicher, dass die Geräte in sicheren Bereichen aufgestellt werden, die von stark frequentierten Bereichen oder Bereichen, die für Unbefugte erreichbar sind, entfernt sind.

3. Verwenden Sie ggf. physische Barrieren oder Zugangskontrollen, um den Zugang zu den Geräten zu beschränken.

Schutz von Einrichtungen zur Informationsverarbeitung:

1. Platzieren Sie Informationsverarbeitungsanlagen, in denen sensible Daten verarbeitet werden, sorgfältig, um das Risiko einer unbefugten Einsichtnahme während der Nutzung zu minimieren.

2. Implementieren Sie Zugangskontrollen, wie z. B. Kartenleser oder biometrische Authentifizierung, um den Zugang zu

Einrichtungen mit sensiblen Informationen zu beschränken.

3. Überprüfen Sie Zutrittsprotokolle und führen Sie regelmäßige Audits durch, um die Einhaltung der Zugriffskontrollrichtlinien zu gewährleisten.

Minimierung der physischen und umweltbedingten Bedrohungen:

1. Implementieren Sie Maßnahmen, um Risiken durch physische und umweltbedingte Bedrohungen wie Diebstahl, Feuer, Wasserschäden, Staub, Vibrationen und Vandalismus zu mindern.

2. Installieren Sie Sicherheitskameras, Alarme und Überwachungssysteme, um unbefugten Zugang oder böswillige Aktivitäten zu erkennen und zu verhindern.

3. Überprüfen Sie Geräte und Einrichtungen regelmäßig auf Anzeichen von Schäden oder Manipulationen und beheben Sie etwaige Schwachstellen umgehend.

Richtlinien für Essen, Trinken und Rauchen:

1. Stellen Sie Richtlinien auf, die das Essen, Trinken und Rauchen in der Nähe von Informationsverarbeitungsanlagen verbieten, um Schäden durch Verschütten oder Beschädigung durch schädliche Substanzen zu vermeiden.

2. Stellen Sie außerhalb der Sicherheitsbereiche ausgewiesene Bereiche zur Verfügung, in denen das Personal gefahrlos Speisen und Getränke zu sich nehmen oder rauchen kann.

Überwachung der Umwelteinflüsse:

1. Setzen Sie Systeme zur Überwachung von Temperatur, Luftfeuchtigkeit und anderen Faktoren, die sich auf die Leistung der Geräte auswirken können ein.

2. Legen Sie Schwellenwerte für akzeptable Umgebungsbedingungen fest und setzen Sie Warnungen oder Benachrichtigungen bei Abweichungen von diesen Schwellenwerten um.

3. Ergreifen Sie Korrekturmaßnahmen, wie z. B. die Anpassung von Heizung, Lüftung, Klimatechnik (HLK)-Einstellungen oder die Installation von Feuchtigkeitsbarrieren, um optimale Umgebungsbedingungen zu erhalten.

Blitzschutz:

1. Installieren Sie Blitzschutzmaßnahmen, einschließlich Blitzableitern und Überspannungsschutzvorrichtungen, an Gebäuden, in denen sich Geräte befinden, um Schäden durch Blitzeinschläge zu minimieren. Berücksichtigen Sie das lokale Risiko des Auftretens von Blitzen.

2. Installieren Sie Blitzschutzfilter an den eingehenden Strom- und Kommunikationsleitungen, um zu verhindern, dass Überspannungen die Geräte beschädigen.

Besondere Schutzmethoden:

1. Beurteilen Sie den Bedarf an speziellen Schutzmethoden, wie z. B. Tastaturmembranen oder robusten Gehäusen, auf der Grundlage der Betriebsumgebung und der potenziellen Gefahren.

2. Beschaffen und installieren Sie bei Bedarf spezielle Geräte oder Schutzmaßnahmen, um die Geräte vor Umweltverschmutzungen oder physischen Schäden zu schützen.

Schutz von vertraulichen Informationen:

1. Implementierung von Verschlüsselungs- und Zugangskontrollen, um Geräte, die vertrauliche Informationen verarbeiten, vor unbefugtem Zugriff oder Abhören zu schützen.

2. Führen Sie regelmäßige Sicherheitsbewertungen und Audits zur Ermittlung und Behebung von Schwachstellen in Geräten durch, die sensible Daten verarbeiten.

Räumliche Trennung der Einrichtungen:

1. Trennen Sie von der Organisation verwaltete Informationsverarbeitungseinrichtungen physisch von denen, die nicht von der Organisation verwaltet werden, um unbefugten Zugang oder Eingriffe zu verhindern.

2. Führen Sie Zugangskontrollen, Absperrungen oder Trennwände ein, um Sicherheitsbereiche abzugrenzen und den Zugang auf befugtes Personal zu beschränken.

4.2 Sicherheit von Vermögenswerten außerhalb von Geschäftsräumen

4.2.1 Richtlinie

Um Informationen zu schützen, muss das Unternehmen den Schutz von externen Ressourcen sicherstellen, um den Verlust, die Beschädigung, den Diebstahl oder die Kompromittierung von Geräten zu verhindern, die außerhalb des Unternehmensgeländes verwendet werden, und um die Unterbrechung des Unternehmensbetriebs zu minimieren.

Verfahren

[Bitte prüfen Sie, ob dieses Verfahren Ihren offiziellen Geschäftsprozessen entspricht und konkretisieren es ggf. Dieses Verfahren erklärt, wie Sie Ihre Vermögenswerte schützen, wenn sie sich nicht an ihrem üblichen Standort befinden (d. h. Laptops, wenn sie nicht im Büro sind).]

Autorisierung der Nutzung von Geräten außerhalb des Standorts:

1. Holen Sie die Genehmigung der Geschäftsleitung ein, bevor Sie Geräte außerhalb des Unternehmensgeländes, einschließlich unternehmenseigener Geräte und privater Geräte, die im Auftrag des Unternehmens verwendet werden (BYOD), zur Speicherung oder Verarbeitung von Informationen außerhalb des Unternehmensgeländes nutzen.
2. Stellen Sie sicher, dass nur zugelassene Geräte für organisatorische Zwecke außerhalb des Betriebsgeländes verwendet werden.

Schutz von Off-Site-Geräten:

1. Vermeiden Sie es, Geräte und Speichermedien an öffentlichen oder ungesicherten Orten unbeaufsichtigt zu lassen, um Verlust, Diebstahl oder unbefugten Zugriff zu verhindern.
2. Halten Sie sich an die Anweisungen des Herstellers zum Schutz der Geräte vor Umwelteinflüssen wie elektromagnetischen Feldern, Wasser, Hitze, Feuchtigkeit und Staub.
3. Verwenden Sie Schutztaschen oder -hüllen für Geräte, um Schäden durch versehentliches Fallenlassen oder Verschütten zu minimieren.

Nachweis lückenloser Überwachung:

1. Führen Sie ein Protokoll, um die Aufbewahrung für Geräte außerhalb des Firmengeländes aufzuzeichnen, wenn sie zwischen verschiedenen Personen oder interessierten Parteien übertragen werden.
2. Dokumentieren Sie die Namen und Organisationen der Personen, die bei jeder Verbringung für die Ausstattung verantwortlich sind.
3. Löschen Sie vor der Übertragung alle unnötigen Informationen vom Gerät, um die Datensicherheit zu gewährleisten.

Autorisierung und Aufzeichnungen:

1. Holen Sie Genehmigungen für die Entfernung von Geräten und Datenträgern aus den Räumlichkeiten der Organisation ein, wenn dies notwendig und praktisch ist.
2. Führen Sie Aufzeichnungen über alle Geräte und Medien, einschließlich des speziellen Zwecks, des Datums und der beteiligten autorisierten Personen, um einen Nachweis zu erhalten.
3. Bewahren Sie die Aufzeichnungen über den Umzug von Geräten an einem sicheren Ort auf, zu dem nur befugtes Personal Zugang hat.

Schutz vor Einsichtnahme in Informationen:

1. Vermeiden Sie die Einsichtnahme in sensible Informationen auf externen Geräten an öffentlichen Orten oder in öffentlichen Verkehrsmitteln, um unbefugten Zugriff oder "Shoulder Surfing"-Angriffe zu verhindern. Schulen Sie Personals zur Wachsamkeit gegen "Shoulder Surfing".
2. Verwenden Sie Sichtschutzfilter oder passen Sie die Helligkeit des Bildschirms oder nehmen Sie andere Maßnahmen vor, um das Risiko zu minimieren, dass Informationen von Unbefugten eingesehen werden können.

Standortverfolgung und Fernlöschung:

1. Aktivieren Sie die Standortverfolgung und Fernlöschfunktionen auf mobilen Geräten, um die Rückverfolgung im Falle von Verlust oder Diebstahl zu erleichtern.
2. Führen Sie Verfahren zur Fernlöschung ein, um den unbefugten Zugriff auf sensible Daten zu verhindern, die auf verlorenen oder gestohlenen Geräten gespeichert sind.

Schutz von fest installierten Geräten:

1. Führen Sie physische Sicherheitsmaßnahmen wie Schlösser, Absperrungen und Überwachungskameras zum Schutz von fest installierten Geräten ein, die sich außerhalb der Räumlichkeiten der Organisation befinden.
2. Führen Sie regelmäßige Inspektionen und Wartungsarbeiten an fest installierter Ausstattung durch, um deren Integrität und Funktionalität zu gewährleisten.
3. Überwachen Sie die Umgebungsbedingungen, um potenzielle Risiken für fest installierte Ausstattung zu erkennen, wie z. B. Wetterschäden oder Umweltgefahren.

4.3 Speichermedien

4.3.1 Richtlinie

Sicherstellung der ordnungsgemäßen Verwaltung von Speichermedien während des gesamten Lebenszyklus, einschließlich Erwerb, Verwendung, Transport und Entsorgung, in Übereinstimmung mit dem Klassifizierungsschema der Organisation und den Handhabungsanforderungen. Diese Richtlinie zielt darauf ab, die unbefugte Offenlegung, Änderung, Entfernung oder Zerstörung von auf Speichermedien gespeicherten Informationen zu verhindern.

Verfahren

[Bitte prüfen Sie, ob dieses Verfahren Ihren offiziellen Geschäftsprozessen entspricht und konkretisieren es ggf. Dieses Verfahren erklärt, wie Ihre Organisation die Speicherung von Medien (z. B. Festplatten/SSDs) aufrechterhalten wird.]

Autorisierung und Erwerb:

1. Holen Sie die Genehmigung des Leiters der IT-Abteilung und des Leiters der Sicherheitsabteilung ein, bevor Sie Wechseldatenträger für den betrieblichen Gebrauch erwerben.
2. Stellen Sie sicher, dass die erworbenen Speichermedien dem Klassifizierungsschema der Organisation und den Handhabungsanforderungen entsprechen.

Sichere Lagerung und Handhabung:

1. Bewahren Sie alle Speichermedien entsprechend ihrer Informationsklassifizierung in ausgewiesenen Sicherheitsbereichen auf.
2. Schützen Sie die Speichermedien gemäß den Herstellerangaben vor Umwelteinflüssen wie Hitze, Feuchtigkeit, elektronischen Feldern und Alterung.
3. Implementieren Sie physische Zugangskontrollen, um den unbefugten Zugriff auf Speichermedien zu verhindern.
4. Behandeln Sie Speichermedien mit Sorgfalt, um physische Schäden oder Datenbeschädigungen während des Gebrauchs zu vermeiden.

Genehmigung zur Mitnahme:

1. Verlangen Sie, dass das Personal eine Genehmigung einholen muss, bevor es Speichermedien aus den Räumlichkeiten der Organisation entfernt.
2. Führen Sie Aufzeichnungen über alle genehmigten Mitnahmen, um einen Nachweis zur Rechenschaft zu erstellen.

Transfer- und Transportsicherheit:

1. Stellen Sie sicher, dass die Übertragung von Informationen auf Wechselspeichermedien sicher und in Übereinstimmung mit den Unternehmensrichtlinien und -verfahren erfolgt.
2. Führen Sie Sicherheitsmaßnahmen zum Schutz von Speichermedien während des physischen Transports ein, z. B. durch die Nutzung sicherer Postdienste oder Kuriere.

Sichere Wiederverwendung oder Beseitigung:

1. Löschen Sie vor der Wiederverwendung von Speichermedien die Daten sicher oder formatieren Sie die Medien, um alle vertraulichen Informationen zu entfernen.
2. Entsorgen Sie Speichermedien, die vertrauliche Informationen enthalten, auf sichere Art und Weise, z. B. durch Vernichtung, Schreddern oder sichere Datenlöschung.

3. Identifizieren Sie Speichermedien, die aufgrund ihrer Sensibilität und Klassifizierung sicher entsorgt werden müssen.
4. Wählen Sie externe Anbieter von Entsorgungsdienstleistungen sorgfältig aus und stellen Sie sicher, dass diese über angemessene Kontrollen und Erfahrung im sicheren Umgang mit sensiblen Informationen verfügen.
5. Protokollieren Sie alle Entsorgungsaktivitäten, um einen Prüfpfad für Entsorgungsaktionen zu erhalten und die Verantwortlichkeit zu gewährleisten.

Risikobewertung für beschädigte Geräte:

1. Führen Sie eine Risikobewertung für beschädigte Speichermedien mit sensiblen Daten durch, um die geeignete Vorgehensweise zu bestimmen, z. B. die physische Zerstörung oder die sichere Entsorgung.

Schulung und Sensibilisierung:

1. Schulen Sie für die Verwaltung von Speichermedien zuständiges Personal im Hinblick auf die in diesem Dokument beschriebenen Verfahren.
2. Sensibilisieren Sie das gesamte Personal für die Bedeutung einer sicheren Verwaltung von Speichermedien, um eine unbefugte Weitergabe oder den Verlust von Informationen zu verhindern.

4.4 Sicherheit der Verkabelung

4.4.1 Richtlinie

Der Schutz von Kabeln, die Strom, Daten oder Telekommunikation übertragen, vor Abhörung, Störung oder Beschädigung muss den Verlust, die Beschädigung, den Diebstahl oder die Beeinträchtigung von Informationen und zugehörigen Vermögenswerten sowie die Unterbrechung des Betriebs der Organisation im Zusammenhang mit der Strom- und Kommunikationsverkabelung verhindern.

Verfahren

[Bitte prüfen Sie, ob dieses Verfahren Ihren offiziellen Geschäftsprozessen entspricht und konkretisieren es ggf. Schützen Sie alle Kabel, die nicht nur Daten, sondern auch Strom oder andere Dienste transportieren.]

Unterirdische Installation und Schutz:

1. Ermitteln Sie Bereiche, in denen Strom- und Telekommunikationsleitungen verlegt werden müssen, wobei die Verlegung unterirdischer Leitungen Vorrang haben soll, sofern dies möglich ist.
2. Stellen Sie sicher, dass unterirdische Kabel durch Kabelkanäle oder andere geeignete Methoden angemessen vor versehentlichen Schnitten oder Beschädigungen geschützt sind.
3. Untersuchen Sie Erdkabel regelmäßig auf Anzeichen von Schäden oder Beeinträchtigungen und beheben Sie umgehend Schwächen.

Trennung von Kabeln:

1. Trennen Sie Strom- und Kommunikationskabel ausreichend räumlich voneinander, um das Risiko von Störungen zu minimieren.
2. Stellen Sie sicher, dass Strom- und Kommunikationskabel getrennt verlegt werden und sich die Wege innerhalb der Informationsverarbeitungseinrichtungen nicht kreuzen.

Zusätzliche Kontrollen für empfindliche Systeme:

1. Identifizieren Sie sensible oder kritische Systeme, die einen zusätzlichen Schutz der Verkabelungsinfrastruktur erfordern.
2. Installieren Sie stabile Kabelkanäle und verschließen Sie Räume oder Boxen und Alarmanlagen an den Inspektions- und Endpunkten für empfindliche Verkabelung.
3. Implementieren Sie eine elektromagnetische Abschirmung, um Kabel vor externen Störungen zu schützen und die Datenintegrität zu gewährleisten.
4. Führen Sie regelmäßig technische und physische Kontrollen durch, um nicht zugelassene Geräte, die an den Kabeln angebracht sind, zu entdecken und zu entfernen.
5. Kontrollieren Sie den Zugang zu Patchpanels und Kabelräumen mit mechanischen Schlüsseln oder PINs, um

unbefugten Zugriff zu vermeiden.

Verwendung von Glasfaserkabeln:

1. Wenn nicht vorhanden, prüfen Sie die Eignung von Glasfaserkabeln für den Einsatz in kritischen Systemen, in denen erhöhte Sicherheits- und Datenübertragungsfunktionen erforderlich sind.
2. Installieren Sie Glasfaserkabel als Alternative zu herkömmlichen Kupferkabeln in sensiblen Bereichen, wo dies möglich ist.

Kabelbeschriftung:

1. Beschriften Sie die Kabel an beiden Enden mit eindeutigen Quell- und Zielangaben, um die physische Identifizierung und Überprüfung zu erleichtern.
2. Vergewissern Sie sich, dass die Etiketten sicher an den Kabeln befestigt sind und für die Wartung und Fehlersuche gut lesbar sind.

Fachliche Beratung:

1. Konsultieren Sie Fachleute oder einschlägige Experten, um eine Anleitung für die Bewältigung von Risiken im Zusammenhang mit Zwischenfällen oder Fehlfunktionen bei der Verkabelung zu erhalten.
2. Lassen Sie sich bei der Umsetzung geeigneter Abhilfemaßnahmen auf der Grundlage der spezifischen Anforderungen und Herausforderungen der Organisation beraten.

Gemeinsame Koordinierung der Ressourcen:

1. Arbeiten Sie zusammen mit anderen Organisationen, die an einem gemeinsamen Standort untergebracht sind, um die Verwaltung und den Schutz der gemeinsamen Verkabelungsinfrastruktur zu koordinieren.
2. Richten Sie klare Kommunikationskanäle und Verfahren für die Behandlung von Fragen der gemeinsamen Verkabelung und die Gewährleistung der gegenseitigen Einhaltung von Sicherheitsmaßnahmen ein.

4.5 Wartung der Ausstattung

4.5.1 Richtlinie

Die Ausstattung muss so gewartet werden, dass die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und zugehörigen Vermögenswerten aufgrund von Verlust, Beschädigung, Diebstahl oder Kompromittierung von Informationen und Unterbrechung des Betriebs der Organisation aufgrund unangemessener Wartungspraktiken gewährleistet werden kann.

Verfahren

[Bitte prüfen Sie, ob dieses Verfahren Ihren offiziellen Geschäftsprozessen entspricht und konkretisieren es ggf. Dieses Verfahren wird Ihnen helfen, sicherzustellen, dass Ihre Ausstattung korrekt gewartet wird und dass Sie im Falle von Problemen Fehler melden und die Ausstattung wieder in Betrieb nehmen, um sicherzustellen, dass die Vertraulichkeit, Verfügbarkeit und Integrität geschützt ist.]

Wartungsplan für die Ausstattung:

1. Erstellen Sie einen umfassenden Wartungsplan auf der Grundlage der Empfehlungen des Lieferanten und der organisatorischen Anforderungen.
2. Identifizieren Sie spezifische Wartungsaufgaben, Häufigkeit und verantwortliches Personal für jedes Gerät.
3. Dokumentieren Sie den Wartungsplan an einem zentralen Ort, der dem zuständigen Personal zugänglich ist.

Autorisiertes Wartungspersonal:

1. Stellen Sie sicher, dass nur geschultes und autorisiertes Personal Wartungsarbeiten an der Ausstattung durchführen darf.
2. Führen Sie eine Liste des autorisierten Instandhaltungspersonals und dessen Qualifikationen oder Bescheinigungen.
3. Führen Sie regelmäßige Schulungen durch, um das Wartungspersonal auf den neuesten Stand der Wartungsverfahren und -protokolle zu bringen.

Störungsmeldungen und Aufzeichnungen:

1. Legen Sie Verfahren fest zur unverzüglichen Meldung vermuteter oder tatsächlicher Gerätefehler.
2. Dokumentieren Sie alle gemeldeten Fehler, einschließlich der Einzelheiten des Problems, der zur Lösung ergriffenen Maßnahmen und des Ergebnisses.
3. Führen Sie ein zentrales Fehlerprotokoll zur Verfolgung und Überwachung der Geräteleistung und der Wartungshistorie.

Planmäßige Wartungskontrollen:

1. Koordinieren Sie geplante Wartungsarbeiten mit internem Personal oder externen Dienstleistern, falls erforderlich.
2. Implementieren Sie Kontrollen, um die Einhaltung von Wartungsplänen zu gewährleisten und Betriebsunterbrechungen zu minimieren.
3. Verlangen Sie von externem Wartungspersonal die Unterzeichnung von Vertraulichkeitsvereinbarungen, bevor Sie Wartungsaufgaben durchführen.

Beaufsichtigung der Wartung vor Ort:

1. Beauftragen Sie einen bestimmten Vorgesetzten mit der Überwachung der Wartungsarbeiten vor Ort und der Einhaltung der Sicherheitsprotokolle.
2. Führen Sie regelmäßige Inspektionen während der Wartung durch, um die Einhaltung der Wartungsverfahren und Sicherheitsstandards zu überprüfen.

Berechtigung zur Fernwartung:

1. Holen Sie für Fernwartungstätigkeiten eine ordnungsgemäße Genehmigung ein, um den unbefugten Zugriff auf sensible Geräte und Daten zu verhindern.
2. Implementieren Sie sichere Maßnahmen für den Fernzugriff, wie verschlüsselte Verbindungen und Multi-Faktor-Authentifizierung, um sich vor Cyber-Bedrohungen zu schützen.

Sicherheitsmaßnahmen für die Wartung außerhalb von Gebäuden:

1. Implementieren Sie Sicherheitsprotokolle für Geräte, die zur Wartung außer Haus gebracht werden, einschließlich sicherer Transport- und Lagerungsvorkehrungen.
2. Stellen Sie sicher, dass das externe Wartungspersonal die Sicherheitsrichtlinien und -verfahren der Organisation einhält, wenn es sich außerhalb des Standorts aufhält.

Inspektion nach Instandhaltung:

1. Inspizieren Sie gründlich die Ausstattung nach der Wartung, um die ordnungsgemäße Funktion und Integrität sicherzustellen.
2. Vergewissern Sie sich vor der Wiederinbetriebnahme, dass keine Manipulationen am Gerät vorgenommen wurden und dass es gemäß den Spezifikationen funktioniert.

Verfahren zur sicheren Entsorgung oder Wiederverwendung:

1. Legen Sie Verfahren für die sichere Entsorgung oder Wiederverwendung von Geräten fest, die nicht mehr verwendet werden.
2. Stellen Sie sicher, dass sensible Daten vor der Entsorgung oder Wiederverwendung sicher von den Geräten gelöscht werden.
3. Entsorgen Sie die Geräte in Übereinstimmung mit den geltenden Vorschriften und Umweltrichtlinien.

Überwachung der Einhaltung der Vorschriften:

1. Überwachen Sie regelmäßig die Einhaltung von Wartungsverfahren und -protokollen für die Ausstattung.
2. Führen Sie Audits durch und Überprüfen Sie Instandhaltungsaufzeichnungen und -aktivitäten, um verbesserungswürdige Bereiche zu ermitteln und die Einhaltung von Richtlinien zu gewährleisten.

4.6 Sichere Entsorgung oder Wiederverwendung von Ausstattung

4.6.1 Richtlinie

Das Unternehmen muss sicherstellen, dass Ausstattungsgegenstände, die Speichermedien enthalten, überprüft werden, um sicherzustellen, dass sensible Daten und lizenzierte Software vor der Entsorgung oder Wiederverwendung entfernt werden. Diese Richtlinie soll die Weitergabe vertraulicher Informationen verhindern und geistiges Eigentum vor unberechtigtem Zugriff oder Offenlegung schützen.

4.6.2 Verfahren

[Bitte prüfen Sie, ob dieses Verfahren Ihren offiziellen Geschäftsprozessen entspricht und konkretisieren es ggf. Prüfen Sie, wenn Ihre Organisation Geräte wie Medien (z. B. Festplatten) entsorgen muss und wenn Sie Geräte haben, die weitergegeben werden müssen (z. B. eine Festplatte in einem Laptop, die an eine andere Person weitergegeben werden muss, wenn ein Mitarbeiter die Organisation verlassen hat).]

Verifizierung von Speichermedien:

1. Führen Sie vor der Entsorgung oder Wiederverwendung von Geräten eine gründliche Inspektion durch, um das Vorhandensein von Speichermedien, einschließlich Festplatten, Solid-State-Laufwerken, Speicherkarten oder anderen Wechseldatenträgern, zu überprüfen.

2. Dokumentieren Sie die Ergebnisse des Überprüfungsprozesses, einschließlich der Art und Kapazität der ermittelten Speichermedien.

Sicheres Entfernen von Daten:

1. Für Geräte, die Speichermedien enthalten:

    a. Ermitteln Sie, wie sensibel die Daten sind, die gespeichert sind, und ob es notwendig ist, die Daten sicher zu entfernen oder zu überschreiben.

    b. Wenn sensible Daten vorhanden sind, leiten Sie den Prozess des sicheren Überschreibens der Speichermedien ein, um die ursprünglichen Daten unwiederbringlich zu machen.

    c. Verwenden Sie zugelassene Überschreibungswerkzeuge oder -methoden, die für die jeweilige Speichermedientechnologie und den Geheimhaltungsgrad der Informationen empfohlen werden.

    d. Ist ein Überschreiben nicht möglich oder ist das Gerät beschädigt, müssen die Speichermedien physisch vernichtet werden, um eine Datenwiederherstellung zu verhindern.

Entfernung von Identifikationsmerkmalen:

1. Vor der Entsorgung, dem Weiterverkauf oder der Spende von Geräten sind alle Etiketten und Kennzeichnungen zu entfernen, die auf die Organisation, das Eigentum, die Klassifizierung, das System oder das Netz hinweisen.

2. Vergewissern Sie sich, dass alle verbleibenden Markierungen oder Aufkleber vollständig unkenntlich gemacht werden, um eine Verbindung mit der Organisation zu verhindern.

Rückbau von Sicherheitskontrollen:

1. Bewerten Sie die Notwendigkeit, Sicherheitseinrichtungen wie Zugangskontrollen oder Überwachungsanlagen auf der Grundlage von Mietverträgen und Risikominderungsstrategien zu entfernen.

2. Wenn Sicherheitskontrollen abgeschafft werden sollen, ist dafür zu sorgen, dass angemessene Verfahren eingehalten werden, um den unbefugten Zugang zu sensiblen Informationen oder die Gefährdung von Sicherheitsmaßnahmen zu verhindern.

Risikobewertung für beschädigte Geräte:

1. Führen Sie eine Risikobewertung für beschädigte Geräte mit Speichermedien durch, um das geeignete Vorgehen zu bestimmen.

2. Wenn das Risiko eines unbefugten Zugriffs auf sensible Informationen als hoch eingestuft wird, ist der physischen Zerstörung der Speichermedien Vorrang vor einer Reparatur oder Entsorgung einzuräumen.

Implementierung der Festplattenverschlüsselung:

1. Stellen Sie sicher, dass die Geräte vollständig verschlüsselt sind, um das Risiko der Offenlegung vertraulicher Informationen bei der Entsorgung oder Neuverwendung zu verringern.

2. Vergewissern Sie sich, dass die Verschlüsselungsprozesse die gesamte Festplatte abdecken, starke kryptografische

Schlüssel verwenden und die kryptografischen Schlüssel vor unbefugtem Zugriff schützen.

Überprüfung der Überschreibungswerkzeuge:

1. Überprüfen Sie die Auswahl geeigneter Überschreibungswerkzeuge oder -methoden auf der Grundlage der Speichermedientechnologie und der Klassifizierungsstufe der gespeicherten Informationen.
2. Stellen Sie sicher, dass die ausgewählten Überschreibungswerkzeuge die Speichermedien wirksam bereinigen können und die Originaldaten nicht wiederherstellbar sind.

Überwachung der Einhaltung der Vorschriften:

1. Überwachen Sie regelmäßig die Einhaltung der in diesem Dokument beschriebenen Verfahren, um die Einhaltung der Maßnahmen zur sicheren Entsorgung und Wiederverwendung zu gewährleisten.
2. Führen Sie regelmäßige Audits oder Inspektionen durch, um zu überprüfen, ob die Verfahren zur Entsorgung und Wiederverwendung von Geräten mit den Unternehmensrichtlinien und Industriestandards übereinstimmen.

5 Versorgung

5.1 Versorgungssicherheit.

5.1.1 Richtlinie

Um den Schutz der Informationsverarbeitungseinrichtungen vor Stromausfällen und anderen Störungen zu gewährleisten, die zum Verlust, zur Beschädigung oder zur Kompromittierung von Informationen und zugehörigen Vermögenswerten führen, müssen die Versorgungseinrichtungen den Unternehmensanforderungen entsprechen.

5.1.2 Verfahren

[Bitte prüfen Sie, ob dieses Verfahren Ihren offiziellen Geschäftsprozessen entspricht und konkretisieren es ggf. Bei diesem Verfahren geht es darum, sicherzustellen, dass Sie über Betriebsmittel verfügen, um zu gewährleisten, dass Sie die CIA (vor allem die Verfügbarkeit) von Geräten aufrechterhalten können. Dies reicht von Geräten, die sicherstellen, dass die Stromversorgung bei Stromausfällen aufrechterhalten werden kann, bis hin zu einer regelmäßigen Überprüfung dieser Geräte. Es geht auch um Netzwerkunterbrechungen, um sicherzustellen, dass Anlagen, die immer Internetzugang benötigen, diesen so weit wie möglich aufrechterhalten können].

Konfiguration und Wartung der Ausstattung:

1. Stellen Sie sicher, dass die Geräte zur Unterstützung der Versorgungseinrichtungen gemäß den Spezifikationen des Herstellers konfiguriert, betrieben und gewartet werden.
2. Führen Sie regelmäßige Inspektionen und Wartungen der Versorgungseinrichtungen durch, um deren ordnungsgemäße Funktion zu gewährleisten und mögliche Probleme zu erkennen.

Kapazitätsplanung:

1. Planen Sie die regelmäßige Bewertung der Kapazität der Versorgungsunternehmen zur Bewältigung des Geschäftswachstums und der Interaktionen mit anderen unterstützenden Versorgungsunternehmen.
2. Planen Sie bei Bedarf die Aufrüstung oder Erweiterung der Versorgungsinfrastruktur, um eine angemessene Kapazität zu erhalten.

Inspektion und Prüfung:

1. Führen Sie einen Plan für die regelmäßige Inspektion und Prüfung von Versorgungseinrichtungen, um Zuverlässigkeit und Leistung zu gewährleisten.
2. Dokumentieren Sie alle Inspektions- und Testaktivitäten, einschließlich aller festgestellten Probleme und ergriffenen Abhilfemaßnahmen.

Alarmanlagen:

1. Installieren Sie Alarmsysteme, um Störungen in der Versorgungsinfrastruktur rechtzeitig zu erkennen.
2. Stellen Sie sicher, dass die Alarmsysteme ordnungsgemäß konfiguriert und getestet werden, um eine rechtzeitige Benachrichtigung über Versorgungsausfälle zu gewährleisten.

Redundanzmaßnahmen:

1. Stellen Sie sicher, dass die Versorgungsunternehmen über mehrere Einspeisungen mit unterschiedlicher physischer Streckenführung verfügen, um die Auswirkungen von Störungen zu minimieren.
2. Überprüfen Sie regelmäßig die Redundanzmaßnahmen zur Anpassung an Änderungen der Versorgungsinfrastruktur oder der Geschäftsanforderungen und passen sie ggf. an.

Netzsegmentierung:

1. Stellen Sie sicher, dass die Geräte zur Unterstützung der Versorgungseinrichtungen in einem separaten Netz von den Einrichtungen zur Informationsverarbeitung betrieben werden, falls sie an ein Netz angeschlossen sind.
2. Implementieren Sie eine Netzwerksegmentierung, um die Versorgungsinfrastruktur von sensiblen Informationssystemen zu isolieren und unbefugten Zugriff zu verhindern.

Sichere Internetverbindung:

1. Verbinden Sie Geräte, die Versorgungseinrichtungen unterstützen, nur dann mit dem Internet, wenn es notwendig ist, und sorgen Sie für sichere Verbindungen, um Cyber-Bedrohungen abzuschwächen.
2. Implementieren Sie Firewalls, Intrusion-Detection-Systeme und andere Sicherheitsmaßnahmen zum Schutz der Versorgungseinrichtungen vor unbefugtem Zugriff und Cyberangriffen.

Vorbereitung auf den Notfall:

1. Stellen Sie Notbeleuchtung und Kommunikationssysteme bereit, um die Reaktionsfähigkeit bei Versorgungsausfällen zu erleichtern.
2. Installieren Sie Notschalter und -ventile in der Nähe von Notausgängen oder Geräteräumen, um in Notfällen Strom, Wasser, Gas oder andere Versorgungseinrichtungen abzuschalten.
3. Halten Sie die Kontaktdaten für Notfälle auf dem neuesten Stand und stellen Sie sie dem Personal zur Verfügung, um eine schnelle Kommunikation und Koordination bei Ausfällen zu ermöglichen.

Zusätzliche Redundanzmaßnahmen:

1. Richten Sie mehrere Versorgungsstränge von mehr als einem Versorgungsunternehmen ein, um die Widerstandsfähigkeit gegen Störungen zu erhöhen.
2. Arbeiten Sie mit Energieversorgern zusammen, um zusätzliche Redundanzoptionen zu prüfen und Maßnahmen zur Minimierung von Ausfallzeiten bei Energieversorgungsausfällen zu ergreifen.

6. Norm-Referenzen

6.1 Normreferenzen zu ISO27001:2022

Kapitel in diesem Dokument	Normkapitel (ISO27001:2022)
1. **Einleitung**	
2. **Physische Sicherheitsperimeter**	
• 2.1 Physische Sicherheitsperimeter	A 7.1
• 2.2 Physischer Zugang	A 7.2
• 2.3 Sicherung von Büros, Räumen und Anlagen	A 7.3
• 2.4 Überwachung physischer Sicherheit	A 7.4

• 2.5 Schutz vor physischen und umweltbedingten Bedrohungen	A 7.5
3. **Besonders schützenswerte physische Arbeitsumgebungen**	
• 3.1 Arbeiten in Sicherheitsbereichen	A 7.6
• Aufgeräumte Arbeitsbereiche	A 7.7
4. **Ausstattung und Verkabelung**	
• 4.1 Standortwahl und Schutz von Ausstattung	A 7.8
• 4.2 Sicherheit von Vermögenswerten außerhalb von Geschäftsräumen	A 7.9
• 4.3 Speichermedien	A 7.10
• 4.4 Sicherheit der Verkabelung	A 7.12
• 4.5 Wartung der Ausstattung	A 7.13
• 4.6 Sichere Entsorgung oder Wiederverwendung von Ausstattung	A 7.14
5. Versorgung	
• 5.1 Versorgungssicherheit	A 7.11

6.2 Referenzen zu TISAX-ISA 6.0

Kapitel in diesem Dokument	**Normkapitel (ISA-TISAX 6.0)**
1. **Einleitung**	
2. **Physische Sicherheitsperimeter**	
• 2.1 Physische Sicherheitsperimeter	3.1.1
• 2.2 Physischer Zugang	3.1.1
• 2.3 Sicherung von Büros, Räumen und Anlagen	3.1.1
• 2.4 Überwachung physischer Sicherheit	3.1.1

• 2.5 Schutz vor physischen und umweltbedingten Bedrohungen	5.2.8
3. **Besonders schützenswerte physische Arbeitsumgebungen**	
• 3.1 Arbeiten in Sicherheitsbereichen	3.1.1
• Aufgeräumte Arbeitsbereiche	2.1.3
4. **Ausstattung und Verkabelung**	
• 4.1 Standortwahl und Schutz von Ausstattung	3.1.1
• 4.2 Sicherheit von Vermögenswerten außerhalb von Geschäftsräumen	3.1.4
• 4.3 Speichermedien	3.1.3; 3.1.4
• 4.4 Sicherheit der Verkabelung	3.1.1
• 4.5 Wartung der Ausstattung	3.1.3
• 4.6 Sichere Entsorgung oder Wiederverwendung von Ausstattung	3.1.3
5. Versorgung	
• 5.1 Versorgungssicherheit	5.2.8