[Name der Organisation]

ST12 Handbuch zum Management der Geschäftskontinuität

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 Geschäftskontinuität für[Name der Organisation] bietet einen konsolidierten Rahmen, der unsere Strategie zur Gewährleistung eines ununterbrochenen Betriebs und zur Abschwächung potenzieller Störungen beschreibt. Es dient als umfassender Leitfaden, in dem detailliert beschrieben wird, wie unsere Organisation plant, die verschiedenen Herausforderungen im Zusammenhang mit der Wahrung unserer Geschäftskontinuität in unserem gesamten Betrieb zu bewältigen. Darüber hinaus wird darin der Ansatz der Organisation für das Management der Geschäftskontinuität dargelegt.

1.1 Zweck und Umfang

Das Hauptziel der Richtlinien in diesem Handbuch ist es, einen strukturierten Ansatz für das Management der Geschäftskontinuität zu entwickeln, um den Betrieb, die sensiblen Informationen, die Vermögenswerte und den Ruf unserer Organisation zu schützen. Durch die Einhaltung dieser Richtlinie wollen wir unsere Widerstandsfähigkeit gegen Störungen erhöhen und das Risiko von Betriebsausfällen oder -verlusten minimieren.

1.2 Anwendbarkeit

DieseRichtlinie gilt für alle Mitarbeiter und Beteiligten und stellt sicher, dass sie die festgelegten Richtlinien für das Management der Geschäftskontinuität einhalten.

Die Abteilung für Geschäftskontinuität [Bitte ändern Sie die Rollenbezeichnung ab, wenn Sie eine andere Abteilung, z. B. die IT-Abteilung mit dieser Rolle beauftragen] ist in Zusammenarbeit mit den relevanten Abteilungen für die Beaufsichtigung der Umsetzung, Pflege und kontinuierlichen Verbesserung der in diesem Handbuch beschriebenen Verfahren verantwortlich.

2 Kapazitäts- und Redundanzmanagement

2.1 Kapazitätsmanagement

2.1.1 Richtlinie

Das IT-Kapazitätsmanagement, der Beschaffungsbereich, das Liegenschaftsmanagement, sowie der Personalbereich müssen sicherstellen, dass der Organisation ausreichend Ressourcen zur Verfügung gestellt werden, um den aktuellen und künftigen Bedarf zu decken.

2.1.2 Verfahren

[Das Kapazitätsmanagement im Bereich der Informationssicherheit umfasst die Sicherstellung, dass Systeme, Netzwerke und Ressourcen angemessen dimensioniert und zugewiesen werden, um aktuelle und zukünftige Anforderungen zu erfüllen und gleichzeitig Sicherheitsmaßnahmen zum Schutz vor potenziellen Bedrohungen und Schwachstellen aufrechtzuerhalten. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen].

Identifizierung des Kapazitätsbedarfs:

1. Regelmäßige Bewertung des Kapazitätsbedarfs für verschiedene Ressourcen, einschließlich Informationsverarbeitungseinrichtungen, Personal, Büros und andere Einrichtungen.

2. Zusammenarbeit mit den relevanten Interessengruppen, um die Kritikalität von Systemen und Prozessen zu bestimmen und die Ressourcenzuweisung entsprechend zu priorisieren.

Überwachung und Anpassung:

1. Implementierung von Überwachungsinstrumenten und -mechanismen zur kontinuierlichen Überwachung der Ressourcennutzung in allen relevanten Bereichen.

2. Regelmäßige Überprüfung der Metriken zur Ressourcennutzung, um kapazitätsbezogene Probleme oder Trends zu erkennen, die eine Anpassung erfordern.

Systemabstimmung und -optimierung:

1. Durchführung regelmäßiger Systemabstimmungs- und Optimierungsmaßnahmen zur Maximierung der Ressourceneffizienz und Leistung.

2. Implementierung von Best Practices und Optimierungen, um sicherzustellen, dass die Systeme ihr volles Potenzial ausschöpfen und keine unnötigen Ressourcen verbrauchen.

Stresstests und Leistungsvalidierung:

1. Durchführung regelmäßiger Stresstests, um die Systemkapazität und -leistung unter Spitzenlastbedingungen zu überprüfen.

2. Analyse der Stresstestergebnisse zur Ermittlung von Engpässen oder verbesserungswürdigen Bereichen der Ressourcennutzung.

Durchführung von Identifizierungsmaßnahmen:

1. Einsatz von Maßnahmen zur Identifikation von Kapazitätsengpässen, z. B. Überwachungsregeln und Warnmeldungen, um ressourcenbezogene Probleme in Echtzeit zu erkennen.

2. Einrichtung von Eskalationsverfahren zur unverzüglichen Behebung festgestellter Anomalien oder kapazitätsbezogener Probleme.

Projektion des künftigen Bedarfs:

1. Zusammenarbeit mit Stakeholdern bei der Prognose künftiger Kapazitätsanforderungen auf der Grundlage von Wachstumsprognosen und technologischen Fortschritten.

2. Nutzung von historischen Daten und Trendanalysen, um den künftigen Ressourcenbedarf genau vorherzusagen.

Überwachung der Ressourcenverwendung und Berichterstattung:

1. Regelmäßige Überwachung der Metriken zur Ressourcennutzung und Erstellung umfassender Berichte, um Trends zu verfolgen und potenzielle Kapazitätsengpässe zu erkennen.

2. Weitergabe von Nutzungsberichten an relevante Interessengruppen, um eine fundierte Entscheidungsfindung und Ressourcenplanung zu erleichtern.

2.2 Redundanz der Informationsverarbeitungseinrichtungen

2.2.1 Richtlinie

Um einen kontinuierlichen Betrieb zu gewährleisten und die Verfügbarkeitsanforderungen zu erfüllen sowie die Verfügbarkeit kritischer Geschäftsdienste und Informationssysteme aufrechtzuerhalten, sind Redundanzen zwischen den Verarbeitungseinrichtungen erforderlich, um Ausfallzeiten zu minimieren und einen ununterbrochenen Betrieb zu gewährleisten.

2.2.2 Verfahren

[Redundanz von Informationsverarbeitungseinrichtungen bedeutet die Einrichtung von Ersatz-Systemen zur Aufrechterhaltung eines reibungslosen Betriebs bei Ausfällen oder Katastrophen, zur Sicherung der Datenintegrität und der Dienste sowie zur Aufrechterhaltung von Sicherheitsmaßnahmen zur Risikominimierung. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen].

Identifizierung von Verfügbarkeitsanforderungen:

1. Identifizierung von Verfügbarkeitsanforderungen für kritische Geschäftsdienste und Informationssysteme auf der Grundlage von Service Level Agreements (SLAs), Business Impact Analysis (BIA) und der Einhaltung gesetzlicher Vorschriften.

Planung von Redundanzmaßnahmen:

1. Entwurf einer Systemarchitektur mit Redundanzmaßnahmen, die geeignet sind, die ermittelten Verfügbarkeitsanforderungen zu erfüllen.

2. Bestimmung des erforderlichen Redundanzgrads für jede Komponente der Informationsverarbeitungseinrichtungen unter Berücksichtigung von Faktoren wie Kritikalität, Auswirkungen und Budgetbeschränkungen.

Auswahl der Redundanzmechanismen:

1. Auswahl von Redundanzmechanismen auf der Grundlage der ermittelten Verfügbarkeitsanforderungen und der Infrastruktur des Unternehmens, einschließlich:

- Duplizierung von Informationsverarbeitungseinrichtungen (z. B. Ersatzkomponenten, gespiegelte Systeme).
- Verträge mit mehreren Lieferanten für kritische Einrichtungen.
- Verwendung redundanter Netze und geografisch getrennter Datenzentren.
- Verwendung von redundanten Stromversorgungen oder -quellen.
- Implementierung von redundanten Instanzen von Software- und Hardware-Komponenten.

Festlegung von Aktivierungsverfahren:

1. Die Aktivierung von redundanten Komponenten und Verarbeitungseinrichtungen, unabhängig davon, ob die Aktivierung automatisch oder manuell erfolgt, muss vom Business/Asset Owner genehmigt werden.

2. Redundante Komponenten müssen die gleiche Sicherheitsstufe wie die primären Komponenten aufweisen.

Einführung von Überwachungsmechanismen:

1. Überwachung der Informationsverarbeitungsanlagen auf Ausfälle oder Leistungsminderungen.

2. Einrichtung von Warnungen und Benachrichtigungen, um Probleme, die die Verfügbarkeit beeinträchtigen könnten, sofort zu erkennen und darauf zu reagieren.

Redundante Systeme testen:

1. Durchführung regelmäßiger Tests von redundanten Systemen und Ausfallsicherungsmechanismen zur Überprüfung der Funktionalität und der Bereitschaft für Notfälle.

2. In den Testszenarien sind verschiedene Ausfallszenarien zu simulieren, um die Wirksamkeit der Redundanzmaßnahmen zu bewerten und etwaige Schwachstellen oder Anfälligkeiten zu ermitteln.

Integration mit Strategien für die Geschäftskontinuität

1. Sicherstellen, dass die Redundanzmaßnahmen mit den Geschäftskontinuitäts-Strategien und -Lösungen der Organisation abgestimmt werden, um die IKT-Bereitschaft für die Geschäftskontinuität zu verbessern.

2. Koordination mit dem Geschäftskontinuitätsteam, um Redundanzanforderungen in die gesamte Kontinuitätsplanung einzubeziehen.

3 IKT-Bereitschaft für die Geschäftskontinuität

3.1 Informationssicherheit bei Unterbrechungen

3.1.1 Richtlinie

Die Festlegung von Informationssicherheitsmaßnahmen bei Unterbrechungen dient der Aufrechterhaltung eines angemessenen Niveaus der Informationssicherheit. Sie zielt darauf ab, die Entwicklung, Umsetzung, Erprobung, Überprüfung und Bewertung von Plänen zur Aufrechterhaltung oder Wiederherstellung der Sicherheit von Informationen im Zusammenhang mit kritischen Geschäftsprozessen nach Unterbrechungen oder Ausfällen festzulegen.

3.1.2 Verfahren

[Vergewissern Sie sich, dass das folgende Verfahren genau der Vorgehensweise entspricht, die Ihr Unternehmen bei Störungen der Informationssicherheit anwendet. Beispiele für solche Ereignisse können sein:

- Naturkatastrophen wie Erdbeben, Wirbelstürme, Überschwemmungen oder Waldbrände.
- Cyberangriffe wie Ransomware, Malware-Infektionen oder Denial-of-Service-Angriffe.
- Stromausfälle oder Ausfälle der Infrastruktur.
- Menschliche Fehler oder versehentliche Datenverletzungen.
- Pandemien oder Gesundheitskrisen mit Auswirkungen auf die Verfügbarkeit von Arbeitskräften.
- Politische Unruhen oder Terroranschläge, die die physische oder digitale Infrastruktur betreffen.
- Geräteausfälle oder Fehlfunktionen der Hardware.
- Unterbrechungen der Lieferkette, die sich auf kritische Technologiekomponenten oder -dienste auswirken.
- Regulatorische Änderungen oder Probleme mit der Einhaltung von Vorschriften, die sich auf den Umgang mit Daten und Sicherheitsmaßnahmen auswirken.
- System-Upgrades oder Wartungsarbeiten, die zu vorübergehenden Unterbrechungen der Dienste führen].

Risikobewertung und Folgenanalyse

1. Führen Sie eine umfassende Risikobewertung durch, um potenzielle Bedrohungen und Schwachstellen zu ermitteln, die die Informationssicherheit bei Störfällen beeinträchtigen könnten.
2. Führen Sie eine Auswirkungsanalyse durch, um die möglichen Folgen dieser Störungen für die Informationssicherheit des Unternehmens zu verstehen.

Anforderungen für die Anpassung von Informationssicherheitskontrollen

1. Das Unternehmen legt seine spezifischen Anforderungen für die Anpassung der Informationssicherheitskontrollen bei Störfällen fest, die sowohl technologische als auch verfahrenstechnische Aspekte umfassen.
2. Die Anforderungen müssen der Notwendigkeit Rechnung tragen, die Sicherheit der Informationen während der gesamten Dauer der Störung und in der Wiederherstellungsphase aufrechtzuerhalten.

Integration der Informationssicherheit in das Management der Geschäftskontinuität

Die Anforderungen an die Informationssicherheit sind nahtlos in die Prozesse des Geschäftskontinuitäts-Managements zu integrieren, um die Abstimmung und Koordinierung zwischen der Sicherheit und den allgemeinen Bemühungen um die Widerstandsfähigkeit des Unternehmens zu gewährleisten.

Planung und -umsetzung

1. Es sind Pläne zu entwickeln, umzusetzen, zu testen, zu überprüfen und zu bewerten, um die Sicherheit von Informationen, die sich auf kritische Geschäftsprozesse beziehen, nach einer Unterbrechung oder einem Ausfall aufrechtzuerhalten oder wiederherzustellen.
2. Die Wiederherstellung der Informationssicherheit muss innerhalb des erforderlichen Niveaus und der vorgegebenen Fristen erfolgen, die durch die Risikotoleranz der Organisation und die gesetzlichen Verpflichtungen bestimmt werden.

3.2 IKT-Bereitschaft für die Geschäftskontinuität

3.2.1 Richtlinie

Das Unternehmen hat sich gegenüber seinen interessierten Parteien verpflichtet, einen Zustand der Bereitschaft für die Geschäftskontinuität aufrechtzuerhalten, um die Widerstandsfähigkeit kritischer Abläufe und Dienste im Falle störender Vorfälle oder Notfälle zu gewährleisten.

Vorrangiges Ziel ist es, die Verfügbarkeit der Informationen und der damit verbundenen Vermögenswerte der Organisation im Falle von Störungen zu gewährleisten.

Die IT-Bereitschaft für die Geschäftskontinuität umfasst die Durchführung einer Business-Impact-Analyse (BIA), um die potenziellen Auswirkungen von Unterbrechungen der Geschäftsaktivitäten zu ermitteln und anhand dieser Analyse das Wiederherstellungszeitziel (Recovery Time Objective, RTO) und das Wiederherstellungspunktziel (Recovery Point Objective, RPO) für priorisierte Aktivitäten und Ressourcen zu bestimmen.

Das Unternehmen muss darauf vorbereitet sein, seine Ziele auch während einer Störung zu erreichen, indem es die Verfügbarkeit seiner Informationen und anderer zugehöriger Vermögenswerte aufrechterhält.

3.2.2 Verfahren

[IKT-Bereitschaft für die Geschäftskontinuität in der Informationssicherheit bedeutet, dass IT-Systeme und -Netzwerke darauf vorbereitet sind, Unterbrechungen zu überstehen, und dass robuste Sicherungs- und Wiederherstellungsmechanismen vorhanden sind. Dazu gehören regelmäßige Tests, die Aktualisierung von Sicherheitsprotokollen und das Vorhandensein von Notfallplänen zur Aufrechterhaltung des Betriebs in Notfällen, zur Minimierung von Ausfallzeiten und Datenverlusten. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen].

Das Unternehmen muss sicherstellen, dass eine angemessene Struktur vorhanden ist, um sich auf eine Störung vorzubereiten, diese abzumildern und darauf zu reagieren. Dazu gehören IT-Kontinuitätspläne, die regelmäßig bewertet und von der Geschäftsleitung genehmigt werden. Diese Pläne müssen Leistungs- und Kapazitätsspezifikationen, RTOs für jeden priorisierten IT-Dienst und RPOs für die priorisierten IT-Ressourcen enthalten, einschließlich:

Identifizierung von kritischen Vorgängen:

Identifizierung und Überprüfung kritischer Geschäftsprozesse und der entsprechenden Systeme und Dienste, die für den Betrieb der Organisation wesentlich sind.

Genehmigung:

Einholung der Unterstützung und Genehmigung der Geschäftsleitung.

[Beispiel: durch Erläuterung des geschäftlichen Nutzens der Bereitschaft, einschließlich der rechtlichen und regulatorischen Vorteile, die sich aus dem Nachweis der Bereitschaft ergeben].

Bestimmung von RPO und RTO von Geschäftsprozessen:

Ermittlung und Dokumentation von RTO und RPO von Geschäftsprozessen, die von der entsprechenden IT-Infrastruktur und Anwendung unterstützt werden.
[Beispiel: RTO/RPO Stufe 1: 0-4h, Stufe 2: 5-24h, Stufe 3: 25-96h. Stufe 4: mehr als 97h
Beispiel - [Name der Organisation] wird sich in erster Linie auf die Ebenen 1 und 2 konzentrieren].

4 IKT-Backup-Management

4.1 Sicherung von Informationen

4.1.1 Richtlinie

Die Sicherung von Daten und Systemen muss auf die Datenaufbewahrungs- und Sicherheitsanforderungen des Unternehmens als Teil des Geschäftskontinuitäts-Programms zugeschnitten sein.

4.1.2 Verfahren

[Bei der Datensicherung werden kritische Daten regelmäßig auf sekundären Speichersystemen dupliziert, um die Datenintegrität und -verfügbarkeit im Falle von Datenverlust, Korruption oder Systemausfällen zu gewährleisten. Dieser Prozess umfasst die Festlegung von Backup-Zeitplänen, die Überprüfung der Backup-Integrität und die Implementierung sicherer Speicherverfahren, um eine effiziente Datenwiederherstellung bei Störungen zu ermöglichen. Ändern Sie diesen Abschnitt, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen].

Identifizierung des Sicherungsbedarfs:

1. Bewerten Sie die Anforderungen des Unternehmens an die Datenaufbewahrung, die Ziele der Geschäftskontinuität und die Einhaltung gesetzlicher Vorschriften, um den Backup-Bedarf zu ermitteln.

2. Identifizieren Sie kritische Systeme, Anwendungen und Daten, die regelmäßig gesichert werden müssen, um das Risiko eines Datenverlusts zu verringern.

Entwicklung eines Sicherungsplans:

1. Entwickeln Sie detaillierte Backup-Pläne, in denen Häufigkeit, Umfang und Methodik der Backups auf der Grundlage

der Wiederherstellungspunktziele (RPOs) und Wiederherstellungszeitziele (RTOs) des Unternehmens festgelegt werden.

2. Dokumentieren Sie die Sicherungspläne, einschließlich des Zeitplans für Vollsicherungen, inkrementelle Sicherungen und differenzielle Sicherungen, soweit zutreffend.

Auswahl von Backup-Einrichtungen und Infrastruktur:

1. Wählen Sie geeignete Backup-Einrichtungen und -Infrastrukturen zur Unterstützung der Backup-Anforderungen des Unternehmens aus.

2. Stellen Sie sicher, dass die Sicherungslösungen skalierbar und zuverlässig sind und die Sicherungsdaten sicher an entfernten Standorten gespeichert werden können.

Backup-Speicherung und Sicherheitsimplementierung:

1. Richten Sie sichere Speicherorte für Sicherungskopien ein, entweder vor Ort oder außerhalb des Unternehmens, und mit angemessenen physischen und umwelttechnischen Schutzmaßnahmen. [Beispiel: Rechenzentrumsübergreifende Sicherung].

2. Implementieren Sie Verschlüsselungsmechanismen zum Schutz von Sicherungsdaten während der Speicherung und Übertragung in Übereinstimmung mit Sicherheitsanforderungen und gesetzlichen Vorschriften.

Prüfung und Validierung von Sicherungsverfahren:

1. Führen Sie regelmäßig Tests durch, um die Integrität und Zuverlässigkeit der Sicherungsverfahren zu überprüfen.

2. Führen Sie Testwiederherstellungen von Sicherungsdaten auf Testsystemen durch, um die Wirksamkeit der Sicherungs- und Wiederherstellungsprozesse zu überprüfen.

3. Dokumentieren Sie die Testergebnisse und gehen Sie auf alle während der Tests festgestellten Probleme oder Mängel ein.

Überwachung und Beaufsichtigung:

1. Bestimmen Sie das Personal, das für die Überwachung der Backup-Vorgänge und die Beaufsichtigung der geplanten Backup-Aktivitäten zuständig ist.

2. Implementieren Sie Überwachungsinstrumente und -verfahren, um sicherzustellen, dass die Backups gemäß den festgelegten Zeitplänen und Anforderungen durchgeführt werden.

3. Beheben Sie etwaige Backup-Ausfälle oder -Unterbrechungen umgehend, um Datenverluste zu minimieren und die Backup-Bereitschaft aufrechtzuerhalten.

Sicherungsmaßnahmen für kritische Systeme:

1. Entwickeln Sie spezielle Sicherungsmaßnahmen für kritische Systeme und Dienste auf der Grundlage ihrer Bedeutung für den Geschäftsbetrieb.

2. Stellen Sie eine umfassende Backup-Abdeckung für kritische Systeme, einschließlich aller notwendigen Informationen, Anwendungen und Daten, die für die Systemwiederherstellung erforderlich sind, sicher.

Überlegungen zur Sicherung von Cloud-Diensten:

1. Bei der Nutzung von Cloud-Diensten muss sichergestellt werden, dass Sicherungskopien der Unternehmensdaten in der Cloud-Umgebung oder über zugelassene Cloud-Sicherungslösungen erstellt werden.

2. Überprüfen Sie die Einhaltung von Sicherungsanforderungen und Datenschutzstandards bei der Nutzung von Cloud-basierten Sicherungsdiensten von Drittanbietern.

Verwaltung der Aufbewahrungsfrist und Löschung der Daten:

1. Bestimmen Sie die Aufbewahrungsfristen für Sicherungsdaten auf der Grundlage von gesetzlichen Vorschriften, rechtlichen Verpflichtungen und Geschäftsanforderungen.

2. Legen Sie Verfahren für die sichere Löschung von Sicherungsdaten nach Ablauf der Aufbewahrungsfristen fest, um die Einhaltung der Datenschutzgesetze und -vorschriften zu gewährleisten.

Dokumentation und Compliance Management:

1. Führen Sie eine detaillierte Dokumentation der Backup-Verfahren, Zeitpläne und Aktivitäten zu Prüfungs- und Compliance-Zwecken.

2. Gewährleisten Sie die Einhaltung einschlägiger Normen und Richtlinien, wie z. B. ISO/IEC 27040, und regelmäßige Aktualisierung der Sicherungsdokumentation, um Änderungen in der Technologie und den Vorschriften zu berücksichtigen.

5. Norm-Referenzen

5.1 Normreferenzen zu ISO27001:2022

Kapitel in diesem Dokument	Normkapitel (ISO27001:2022)
1. **Einleitung**	
2. **Kapazitäts- und Redundanzmanagement**	
• 2.1 Kapazitätsmanagement	A 8.6
• 2.2 Redundanz von Informationsverarbeitungseinrichtungen	A 8.14
3. **IKT-Bereitschaft für die Geschäftskontinuität**	
• 3.1 Informationssicherheit bei Unterbrechungen	A 5.29
• 3.2 IKT-Bereitschaft für die Geschäftskontinuität	A 5.30
4. **IKT-Backup-Management**	
• 4.1 Sicherung von Informationen	A 8.13

5.2 Referenzen zu TISAX-ISA 6.0

Kapitel in diesem Dokument	Normkapitel (ISA-TISAX 6.0)
1. **Einleitung**	
2. **Kapazitäts- und Redundanzmanagement**	
• 2.1 Kapazitätsmanagement	5.2.1
• 2.2 Redundanz von Informationsverarbeitungseinrichtungen	5.3.2
3. **IKT-Bereitschaft für die Geschäftskontinuität**	
• 3.1 Informationssicherheit bei Unterbrechungen	1.3.4; 1.6.3; 5.2.3; 5.2.8
• 3.2 IKT-Bereitschaft für die Geschäftskontinuität	5.2.8

4. **IKT-Backup-Management**	
• 4.1 Sicherung von Informationen	5.2.9