[Logo der Organisation]

[Name der Organisation]

Commented [27A1]: Alle mit eckigen Klammern [ ] markierte Felder in diesem Dokument müssen ausgefüllt werden.

SICHERHEITSVERFAHREN FÜR DIE IT-ABTEILUNG

Commented [27A2]: Teile dieses Dokuments, die detaillierter ausgeführt werden müssen, können als separate Dokumente (Richtlinien/Verfahren) aufgesetzt werden.

Code:	
Version:	
Datum der Version:	
Erstellt durch:	
Genehmigt durch:	
Vertraulichkeitsstufe:	

Commented [27A3]: Die Systematik für die Kodierung von Dokumenten sollte dem in der Organisation vorhandenen System zur Dokumentations-Kodierung entsprechen. Falls kein solches System vorhanden ist, kann diese Zeile gelöscht werden.

Änderungs-Historie

Datum	Version	Erstellt durch	Beschreibung der Änderung
	0.1	27001Academy	Erster Entwurf des Dokuments

Inhaltsverzeichnis

1. ZWECK, ANWENDUNGSBEREICH UND ANWENDER 3

2. REFERENZDOKUMENTE 3

3. BETRIEBSVERFAHREN FÜR INFORMATIONS- UND KOMMUNIKATIONSTECHNIK 3

3.1. ÄNDERUNGSMANAGEMENT 3
3.2. BACKUP 4
3.2.1. Backup-Prozess 4
3.2.2. Test von Backup-Kopien 4
3.3. MANAGEMENT DER NETZSICHERHEIT 4
3.4. NETZWERKDIENSTE 5
3.5. ENTSORGUNG UND VERNICHTUNG VON AUSSTATTUNG UND DATENTRÄGERN 5
3.5.1. Gerätschaften 5
3.5.2. Tragbare Speichermedien 5
3.5.3. Papier-Datenträger 5
3.5.4. Löschungs- und Vernichtungsprotokolle; Ausschuss für die Vernichtung von Daten 6
3.6. INFORMATIONSÜBERTRAGUNG 6
3.6.1. Elektronische Kommunikationswege 6
3.6.2. Beziehungen zu externen Parteien 6
3.7. SYSTEMÜBERWACHUNG 7

4. VERWALTUNG VON AUFZEICHNUNGEN, DIE ZU DIESEM DOKUMENTS ERSTELLT WURDEN 7

5. GÜLTIGKEIT UND DOKUMENTEN-HANDHABUNG 9

1. Zweck, Anwendungsbereich und Anwender

Zweck dieses Dokuments ist es sicherzustellen, dass Informations- und Kommunikations-Technologie ordnungsgemäß und sicher funktioniert.

Dieses Dokument gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS), d.h. für die gesamte Informations- und Kommunikations-Technologie sowie die verwandten Dokumentation innerhalb des Anwendungsbereiches.

Anwender dieses Dokuments sind Mitarbeiter von [Organisationseinheiten für Informations- und Kommunikations-Technologie].

2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitte A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.14.2.4
- Informationssicherheitspolitik
- [Strategie für betriebliches Kontinuitätsmanagement]
- [Richtlinie zu Mobilgeräten und Telearbeit]
- [Richtlinie zur Klassifizierung von Informationen]
- [Inventar der Werte]
- [Sicherheitspolitik für Lieferanten]

3. Betriebsverfahren für Informations- und Kommunikationstechnik

3.1. Änderungsmanagement

Jede Änderung an einem betrieblichen oder Produktiv-System muss wie folgt durchgeführt werden:

1. Die Änderung kann von [Stellenfunktionen angeben] beantragt werden
2. Die Änderung muss von [Stellenbezeichnung] genehmigt werden, der die Notwendigkeit dafür anhand der Geschäftsauswirkungen und potentiell negativen Auswirkungen auf die Sicherheit bewerten muss
3. [illegible]
4. [illegible]
5. [illegible]
6. [illegible]

Änderungsprotokolle werden wie folgt aufbewahrt: [Bezeichnung für das Formular angeben oder eine andere Methode für das Protokollieren von Änderungen angeben]

Commented [27A4]: Diesen Punkt löschen, falls Maßnahme A.12.1.2 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A5]: Diesen Punkt löschen, falls die Änderungsmanagement Richtlinie in einem separaten Dokument festgelegt ist.

Commented [27A6]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diesen Artikel:

How to manage changes in an ISMS according to ISO 27001 A.12.1.2 https://advisera.com/27001academy/blog/2015/09/14/how-to-manage-changes-in-an-isms-according-to-iso-27001-a-12-1-2/

Commented [27A7]: Es kann angegeben werden, was als mit diesem Dokument geregelte Änderung betrachtet wird und was [illegible]

Commented [27A8]: Die Schritte können auch so formuliert werden, dass die Person mit Zuständigkeit für alle weiteren Schritte im zweiten Schritt genannt wird. So muss nicht in jedem folgenden Schritt der Verantwortliche aufgeführt werden.

3.2. Backup

3.2.1. Backup-Prozess

Datensicherungen müssen für alle Systeme erstellt werden, die in der [Strategie für Betriebliches Kontinuitätsmanagement] identifiziert sind und dies muss in den ebenfalls in diesem Dokument genannten Intervallen erfolgen.

[Stellenbezeichnung] ist für den Backup-Prozess von Informationen, Software und System-Kopien verantwortlich. Daß notwendig, hier angeben welche Technologien für die Erstellung von Backup-Kopien genutzt wird, die Verantwortlichkeiten für einzelne Tätigkeiten, die Standards für die Aufbewahrung von Backup-Kopien, den physikalischen Schutz von Backup-Kopien, Verschlüsselung, Passwörter, etc. spezifizieren]

Protokolle zum Backup-Prozess werden automatisch auf den Systemen generiert, wo die Backup-Kopie erstellt wird.

3.2.2. Test von Backup-Kopien

Backup-Kopien und der Prozess für deren Rücksicherung müssen mindestens [quartalsweise] getestet werden, indem der Datenwiederherstellungsprozess auf [Angabe des Servers auf dem die Datenwiederherstellung geschieht] durchgeführt wird und geprüft wird, ob alle Daten erfolgreich wiederhergestellt wurden.

[Stellenbezeichnung] ist für den Test von Backup-Kopien verantwortlich. Protokolle zu Tests von Backup-Kopien werden wie folgt aufbewahrt: [Beschreibung der Form des Protokolls – auf Papier oder in elektronischer Form, ob eine Form vorgeschrieben ist, etc.].

3.3. Management der Netzsicherheit

[Stellenbezeichnung] ist für das Management und die Überwachung der Rechnernetze, für das Gewährleisten der Sicherheit von Informationen in Netzwerken, sowie für den Schutz der mit dem Netzwerk verbundenen Dienste vor unberechtigtem Zugang verantwortlich. Hierfür ist folgendes notwendig:

- die Trennung der operativen Verantwortung für Netzwerke und der Verantwortung für sensible Anwendungen und andere Systeme
- [der Schutz sensibler Daten im öffentlichen Netz durch (hier die zum Schutz eingesetzte Technologie beschreiben und Verantwortungsbereiche sowie Verantwortliche angeben)]
- [der Schutz sensibler Daten in drahtlosen Netzwerken durch (hier die zum Schutz eingesetzte Technologie beschreiben und Verantwortungsbereiche sowie Verantwortliche angeben)]
- [der Schutz von Geräteschaften, die sich von außerhalb Standorten mit dem Netzwerk verbinden, erfolgt durch (hier die zum Schutz eingesetzte Technologie beschreiben und Verantwortungsbereiche sowie Verantwortliche angeben)]
- [die Trennung des Datenverkehrs von Mobilgeräten, sowie das Erstellen von Firewall-Richtlinien, statischen Routen, virtuellen Lokalnetzwerken, usw.

Commented [27A9]: Diesen Punkt löschen, falls Maßnahme A.12.3.1 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A10]: Diesen Punkt löschen, falls die Backup Richtlinie in einem separaten Dokument festgelegt ist.

Commented [27A11]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diesen Artikel:

Backup policy – How to determine backup frequency
https://advisera.com/27001academy/blog/2013/05/07/backup-policy-how-to-determine-backup-frequency/

Commented [27A12]: Falls ein solches Dokument nicht vorhanden ist, müssen hier alle Systeme gelistet werden, für die ein Backup erforderlich ist, zusammen mit den Intervallen für Backups.

Commented [27A13]: Backup-Kopien sollten an Standorten

Commented [27A14]: Häufigkeit entsprechend der eingeschätzten Risiken anpassen.

Commented [27A15]: Diesen Punkt löschen, falls Maßnahme A.13.1.1 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A16]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diese Artikel:

- How to manage network security according to ISO 27001 A.13.1
https://advisera.com/27001academy/blog/2016/06/27/how-to-manage-network-security-according-to-iso-27001-a-13-1/

- Requirements to implement network segregation according to ISO 27001 control A.13.1.3
https://advisera.com/27001academy/blog/2015/11/02/requirements-to-implement-network-segregation-according-to-iso-27001-control-a-13-1-3/

- Network segregation in cloud environments according to ISO 27017
https://advisera.com/27001academy/blog/2016/09/26/network-segregation-in-cloud-environments-according-to-iso-27017/

- Using Intrusion Detection Systems and Honeypots to comply with ISO 27001 A.13.1.1 network controls
https://advisera.com/27001academy/blog/2016/07/04/using-intrusion-detection-systems-and-honeypots-to-comply-with-iso-27001-a-13-1-1-network-controls/

- How to use firewalls in ISO 27001 and ISO 27002 implementation
https://advisera.com/27001academy/blog/2015/05/25/how-to-use-firewalls-in-iso-27001-and-iso-27002-implementation/

Commented [27A17]: Oder auf Richtlinie zu Mobilgeräten und Telearbeit Bezug nehmen.

- [illegible]
- [illegible]

3.4. Netzwerkdienste

[Stellenbezeichnung] muss Sicherheitsfunktionalitäten und den erwarteten Service-Level für alle Netzwerkdienste definieren, unabhängig davon ob diese in-house oder über Outsourcing zur Verfügung gestellt werden. Falls möglich, sollten diese Anforderungen in Vereinbarungen mit den Dienstleistern dokumentiert werden.

[illegible]

3.5. Entsorgung und Vernichtung von Ausstattung und Datenträgern

Alle Daten und lizensierte Software auf tragbaren Speichermedien (z.B. auf CD, DVD, USB Stick, Speicherkarten, etc., aber auch auf Papier) und allen Gerätschaften, die Speichermedien enthalten (z.B. Rechner, Mobiltelefone, etc.), müssen gelöscht werden oder der Datenträger muss zerstört werden, bevor das Gerät entsorgt oder wiederverwendet wird.

[illegible]

3.5.1. Gerätschaften

[Stellenbezeichnung] ist für das Prüfen und Löschen von in Gerätschaften enthaltenen Daten verantwortlich, außer die Richtlinie zur Klassifizierung von Informationen schreibt hierzu etwas anderes vor. Daten müssen durch [hier die für das Löschen von Daten benutzte Technologie beschreiben] von den Datenträgern der Geräte gelöscht werden. Falls dieser Prozess, gemessen an der Sensibilität der Daten, nicht sicher genug sein sollte, muss das Speichermedium zerstört werden.

3.5.2. Tragbare Speichermedien

[Stellenbezeichnung] ist für das Löschen von Daten von tragbaren Speichermedien verantwortlich, außer die Richtlinie zur Klassifizierung von Informationen schreibt hierzu etwas anderes vor. Daten [illegible]

3.5.3. Papier-Datenträger

Mitarbeiter der Organisation, die mit der Verwaltung individueller Dokumente befasst sind, sind für die Vernichtung von Papierdokumenten verantwortlich, außer die Richtlinie zur Klassifizierung von [illegible]

Commented [27A18]: Die Häufigkeit kann genauer angegeben werden – z.B. täglich oder an bestimmten Tagen des Monats, usw.

Commented [27A19]: Die Maßnahmen können genauer spezifiziert werden – z.B. Firewall, Intrusion Detection Systeme, usw.

Commented [27A20]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diesen Artikel:

How to manage the security of network services according to ISO 27001 A.13.1.2
https://advisera.com/27001academy/blog/2017/02/13/how-to-manage-the-security-of-network-services-according-to-iso-27001-a-13-1-2/

Commented [27A21]: Diesen Punkt löschen, falls die Maßnahmen A.8.3.2 und A.11.2.7 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt werden.

Commented [27A22]: Diesen Punkt löschen, falls die Richtlinie zu Entsorgung, Vernichtung und Weiterverwendung in einem separaten Dokument festgelegt ist.

Commented [27A23]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diesen Artikel:

Secure equipment and media disposal according to ISO 27001
https://advisera.com/27001academy/blog/2015/12/07/secure-equipmentand-media-disposal-according-to-iso-27001/

Commented [27A24]: Es kann genauer ausgeführt werden, dass dies Aufbewahrung in der eigenen Organisation und/oder Übergabe an eine andere Organisation (z.B. Verkauf, Spende, Versand zur Reparatur, usw.) bedeuten kann.

Commented [27A25]: Es kann genauer angegeben werden, dass dies die Weitergabe an einen anderen Benutzer, usw. bedeutet.

Commented [27A26]: Löschen, falls Maßnahme A.8.1.1 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A27]: Löschen, falls eine solche Richtlinie nicht vorhanden ist.

Commented [27A28]: z.B. Auflistung spezieller Werkzeuge die [illegible]

Commented [27A29]: Dies kann z.B. eine Festplatte in einem Server sein.

Commented [27A30]: Löschen, falls eine solche Richtlinie nicht vorhanden ist.

Commented [27A31]: Löschen, falls eine solche Richtlinie nicht vorhanden ist.

Commented [27A32]: Oder eine andere Methode angeben.

3.5.4. Löschungs- und Vernichtungsprotokolle; Ausschuss für die Vernichtung von Daten

Für alle Daten mit der Klassifizierung "Eingeschränkt" und "Vertraulich" müssen Löschungs-/ Vernichtungsprotokolle geführt werden. Die Protokolle müssen folgende Informationen enthalten: Information über den Datenträger, Datum der Löschung/Vernichtung, Methode der Löschung/Vernichtung, Durchführender des Vorgangs.

[redacted]

3.6. Informationsübertragung

3.6.1. Elektronische Kommunikationswege

Informationen der Organisation können über folgende elektronische Kommunikationswege ausgetauscht werden: E-Mail, Downloads von Dateien aus dem Internet, Übertragung von Daten via [hier die Bezeichnungen spezieller Kommunikationssysteme angeben], Telefone, Faxgeräte, der Versand von SMS Textnachrichten, tragbare Medien, sowie Foren und soziale Netzwerke.

[redacted]

3.6.2. Beziehungen zu externen Parteien

Der Begriff Externe Parteien umfasst verschiedene Dienstleister, Firmen für Hardware- und Software-Wartung, Firmen die Transaktionen oder Datenverarbeitung durchführen, Kunden, etc.

[redacted] Die Vereinbarung kann in Papierform oder in elektronischer Form bestehen (z.B. Zustimmung zu Allgemeinen Geschäftsbedingungen) und muss Klauseln entsprechend der Risikoeinschätzung enthalten, mindestens jedoch die Nachfolgenden:

- Methode zur Identifizierung der anderen Partei
- Zugangsberechtigungen zu Informationen
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Commented [27A33]: An die in der Organisation verwendeten Vertraulichkeitsstufen anpassen.

Commented [27A34]: Diesen Punkt löschen, falls die Richtlinie zur Informationsübertragung in einem separaten Dokument festgelegt ist.

Commented [27A35]: Diesen Punkt löschen, falls die Maßnahme A.13.2.1 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A36]: Das betreffende Datenträger kann genauer spezifiziert werden.

Commented [27A37]: Die betreffenden Foren und sozialen Netzwerke können genauer spezifiziert werden.

Commented [27A38]: Hier Kommunikationswege entsprechend der Risikoeinschätzung und der üblicherweise genutzten Kanäle hinzufügen oder löschen.

Commented [27A39]: Dieser Text kann durch eine direkte Festlegung der Daten und Kommunikationswege, der Einschränkungen und verbotenen Tätigkeiten ersetzt werden.

Commented [27A40]: Löschen, falls eine solche Richtlinie nicht vorhanden ist.

Commented [27A41]: Diesen Punkt löschen, falls die Maßnahme A.13.2.2 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Verträge/Vereinbarungen mit externen Partien müssen sich an den Vorschriften der [Sicherheitspolitik für Lieferanten] orientieren.

3.7. Systemüberwachung

Auf Basis der Ergebnisse der Risikoeinschätzung entscheidet [Stellenbezeichnung], welche Protokolldateien auf welchen Systemen und für welche Systeme geführt werden und wie lange diese gespeichert werden. Protokolle müssen für alle Administratoren und Systembediener von sensiblen Systemen geführt werden.

[Stellenbezeichnung] ist für die tägliche Überwachung der Protokolle zu automatischen Fehlermeldungen verantwortlich. Ebenso ist er für die Registrierung von Fehlern zuständig, die von

4. Verwaltung von Aufzeichnungen, die zu diesem Dokuments erstellt wurden

Name der Aufzeichnung	*Aufbewahrungs-Ort*	*Verantwortlicher für Aufbewahrung*	*Maßnahme zum Schutz der Aufzeichnung*	*Aufbewahrungs-Dauer*
[Name des Änderungsprotokolls] – in elektronischer Form	[Name des Intranet Ordners]	[Stellen-bezeichnung]	Nach der Erstellung kann das Protokoll nicht mehr nachträglich geändert werden	3 Jahre
[Entscheidungen zu Kommunikations-Wegen für spezifische Informationsarten, Einschränkungen, verbotene Tätigkeiten] – elektronische Form	[Name des Intranet Ordners]	[Stellen-bezeichnung]	Nach der Erstellung kann das Protokoll nicht mehr nachträglich geändert	3 Jahre

Commented [27A42]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diesen Artikel:

Logging and monitoring according to ISO 27001 A.12.4 https://advisera.com/27001academy/blog/2015/11/23/logging-and-monitoring-according-to-iso-27001-a-12-4/

Commented [27A43]: Die Protokolle können

Commented [27A44]: Diesen Text löschen, falls Maßnahme A.12.4.1 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A45]: Diesen Text löschen, falls Maßnahme A.12.4.3 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A46]: Diesen Text löschen, falls Maßnahme A.12.4.1 und A.12.4.3 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt werden.

Commented [27A47]: Es kann angegeben werden, dass dies z.B. die Prüfung von E-Mail oder anderer Kommunikation beinhalten kann, was jedoch der gültigen Gesetzeslage entsprechen muss.

Commented [27A48]: Falls notwendig, kann dies detaillierter festgelegt werden, z.B. in Tabellenform – welche Systeme überprüft werden, wie häufig, usw.

Commented [27A49]: Diesen Text löschen, falls Maßnahme A.12.4.1 und A.12.4.3 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt werden.

Commented [27A50]: Bitte ändern Sie diese Aufzeichnungen derart, dass sie zu denen passen, die Sie bereits in Ihrem Unternehmen haben. Sollten Sie keine ähnlichen Aufzeichnungen haben, können Sie neue Aufzeichnungen in einem neuen Format erstellen, welches Ihnen am besten zusagt.

			werden	
[Protokolle zum Backup-Prozess] – elektronische Form	System auf dem der Backup-Prozess ausgeführt wird	[Stellen-bezeichnung]	Die Aufzeichnungen werden nur mit Lesezugriffs-Berechtigung versehen; sie können weder gelöscht noch bearbeitet werden.	Protokolle werden für die Dauer von 1 Jahr aufbewahrt
[Protokolle zum Test von Backup-Kopien] – elektronische oder Papierform	[Name des Aktenordners/ Schranks]	[Stellen-bezeichnung]	Nur [Stellen-bezeichnung] hat die Berechtigung für den Zugang zu solchen Aufzeich-nungen	Aufzeichnungen werden für die Dauer von 1 Jahr aufbewahrt
[Sicherheitsfunktionalitäten und erwartete Service-Levels für Netzwerkdienste] - elektronische und Papierform	Rechner von [Stellenbezeichnung], [Name des Aktenordners/Schranks]	[Stellen-bezeichnung]	Nur [Stellen-bezeichnung] hat die Berechtigung für den Zugang zu solchen Aufzeich-nungen	5 Jahre über das Ende der Vereinbarung oder des geleisteten Service hinaus
[Löschungs-/Vernichtungs-Protokolle] - in Papierform	[Name des Aktenordners/Schranks]	[Stellen-bezeichnung]	Der Schrank ist verschlossen, die Schlüssel werden von [Stellen-funktionen] verwahrt	Protokolle werden für die Dauer von 5 Jahren aufbewahrt
[Aufzeichnungen zur Überprüfung von Protokoll-Dateien] -	Rechner von [Stellenbezeichnung], [Name des	[Stellen-bezeichnung]	Nur [Stellen-bezeichnung] hat die	Aufzeichnungen werden für die Dauer von

elektronische und Papierform	Aktenordners/Schranks]		Berechtigung für den Zugang zu solchen Aufzeich-nungen	5 Jahren aufbewahrt

5. Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab [Datum]

Der Eigentümer des Dokuments ist [Stellenbezeichnung], der das Dokument mindestens einmal jährlich prüfen und gegebenenfalls aktualisieren muss.

Commented [27A51]: Dies ist lediglich eine Empfehlung; Häufigkeit gegebenenfalls anpassen.

Für die Auswertung des Dokuments auf Wirksamkeit und Angemessenheit müssen folgende Kriterien berücksichtigt werden:

- [illegible]
- [illegible]

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [27A52]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.