[Logo der Organisation]

[Name der Organisation]

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

IT-SICHERHEITSPOLITIK

Commented [27A2]: Für Anleitungen zur Struktur dieses Dokuments lesen Sie diesen Artikel:

How to structure the documents for ISO 27001 Annex A controls https://advisera.com/27001academy/blog/2014/11/03/how-to-structure-the-documents-for-iso-27001-annex-a-controls/

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

Der Zweck dieses Dokuments ist die Festlegung klarer Regeln für den Gebrauch von Informationssystemen und anderer Informationswerte bei [Name der Organisation].

Dieses Dokument gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS), d.h. für alle Informationssysteme und andere Informationswerte innerhalb des ISMS Anwendungsbereiches.

Anwender dieses Dokuments sind alle Mitarbeiter von [Name der Organisation].

2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitte A.6.2.1, A.6.2.2, A.8.1.2, A.8.1.3, A.8.1.4, A.9.3.1, A.11.2.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.2.1, A.12.3.1, A.12.5.1, A.12.6.2, A.13.2.3, A.18.1.2
- Informationssicherheitspolitik
- [Richtlinie zur Klassifizierung von Informationen]
- [Verfahren zum Umgang mit Informationssicherheits-Vorfällen]
- [Inventar der Werte]
- [Sicherheitsverfahren für die IT-Abteilung]
- [Richtlinie zur Übertragung von Informationen]

3. Zulässiger Gebrauch von Informationswerten

Commented [27A4]: Es muss auf Basis der Ergebnisse der Risikoeinschätzung entschieden werden, inwieweit die aufgelisteten Punkte notwendig sind.

Diese Schulung wird Ihnen dabei helfen, das Sicherheitsbewusstsein zu steigern und das Wissen Ihrer Mitarbeiter zu verfolgen: https://training.advisera.com/awareness-session/security-awareness-training/

3.1. Definitionen

Informationssystem – schließt alle Server und Arbeitsplatzrechner, Netzwerk-Infrastruktur, [illegible] den Verantwortungsbereich der Organisation fallen. Der Gebrauch eines Informationssystems [illegible]

[illegible] Mobiltelefone, tragbare Computer, Speichermedien, usw. angewendet.

3.2. Zulässiger Gebrauch

[illegible]

3.3. Verantwortlichkeiten für Werte

Commented [27A5]: Diesen Punkt löschen, falls Maßnahme A.8.1.2 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Jedem Informationswert ist im Inventar der Werte ein Eigentümer zugeordnet. Der Eigentümer des

3.4. Untersagte Aktivitäten

Es ist untersagt, Informationswerte auf eine Art und Weise zu nutzen, die unnötigerweise

- Bild- oder Video-Dateien herunterzuladen, die nicht geschäftlichen Zwecken dienen, E-Mail-
-
-
- durch [Stellenbezeichnung] ausdrücklich genehmigt
-
-
- von Daten (z.B. USB Sticks) ohne ausdrückliche Genehmigung durch [Stellenbezeichnung] zu

3.5. Entfernung von Werten aus dem Standort

Ausstattung, Information oder Software darf ohne vorherige schriftliche Genehmigung durch

von der Person beaufsichtigt werden, welche die Erlaubnis für ihre Mitnahme erhalten hat.

3.6. Rückgabe von Werten bei Beendigung eines Vertrages

diesbezüglichen Informationswerte an [Stellenbezeichnung) zurückgeben.

3.7. Backup-Verfahren

3.8. Virenschutz

3.9. Berechtigungen zur Nutzung von Informationssystemen

Commented [27A6]: Löschen, falls Maßnahme A.12.5.1 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A7]: Löschen, falls keine solche Richtlinie vorhanden ist.

Commented [27A8]: Diesen Punkt löschen, falls Maßnahme A.11.2.5 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A9]: Hier sollte angegeben werden ob eine

Commented [27A10]: Diesen Punkt löschen, falls Maßnahme A.8.1.4 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A11]: Diesen Punkt löschen, falls Maßnahme A.12.3.1 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A12]: Hier ist sicherzustellen, dass dies nicht

Commented [27A13]: 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 [27A14]: Sofern eine

Commented [27A15]: Diesen Punkt löschen, falls Maßnahme A.12.2.1 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

sind, also für welche sie die Zugangsberechtigung erhalten haben.

Anwender dürfen keine Tätigkeiten ausführen die für eine Umgehung der Sicherheitsmaßnahmen

3.10. Benutzerkonto Verantwortlichkeiten

Der Benutzer darf weder direkt noch indirekt anderen Personen die Benutzung seiner/ihrer

Commented [27A16]: Löschen, falls Maßnahme A.9.3.1 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Der Eigentümer eines Benutzerkontos ist dessen Anwender, der für die Benutzung des

3.11. Passwort Verantwortlichkeiten

Commented [27A17]: Diesen Punkt löschen, falls die Passwort-Richtlinie in einem separaten Dokument festgelegt ist.

Commented [27A18]: Diesen Punkt löschen, falls Maßnahme A.9.3.1 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

anwenden:

-
-
- sichere Methode zugelassen
- Vom Anwender erstellte Passworte dürfen auf keinem Weg verbreitet werden (mündlich,
-
- gemeldet werden
- Sichere Passworte müssen folgendermaßen gewählt werden:
  -
  -
  -
  -
  - das Passwort darf nicht in einem Wörterbuch enthalten sein, darf kein Wort im Dialekt oder in der Umgangssprache irgendeiner Sprache oder irgendein solches
  -
  -
- Passworte müssen alle 3 Monate geändert werden
-

- Passworte dürfen nicht in einem System zur automatischen Anmeldung gespeichert werden
- [illegible]

3.12. Richtlinie zum aufgeräumten Arbeitsplatz und leeren Bildschirm

Jegliche Information mit der Klassifizierung "Interner Gebrauch", "Eingeschränkt" und "Vertraulich" [illegible]

3.12.1. Richtlinie zum aufgeräumten Arbeitsplatz

[illegible] verhindern.

Solche Dokumente und Datenträger müssen entsprechend der Richtlinie zur Klassifizierung von [illegible]

3.12.2. Richtlinie zum leeren Bildschirm

Falls die berechtigte Person nicht an ihrem Arbeitsplatz ist, dürfen keine sensiblen Informationen auf [illegible]

[illegible] durch Abmelden von allen Systemen oder Sperren des Bildschirms mit einem Passwort umgesetzt. Falls die Person für einen längeren Zeitraum abwesend ist (mehr als 30 Minuten), wird die Richtlinie [illegible]

3.12.3. Schutz gemeinsam genutzter Einrichtungen und Gerätschaften

Dokumente, die sensible Information beinhalten, müssen umgehend von Druckern, Faxgeräten und [illegible]

[illegible] berechtigten Person angeben – z.B. Absperren der Einrichtung, usw.].

[illegible] z.B. Absperren der Einrichtung, usw.].

[illegible]

Commented [27A19]: Diesen Punkt löschen, falls die Richtlinie zum aufgeräumten Arbeitsplatz und leeren Bildschirm in einem separaten Dokument festgelegt ist.

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

Clear desk and clear screen policy – What does ISO 27001 require? https://advisera.com/27001academy/blog/2016/03/14/clear-desk-and-clear-screen-policy-what-does-iso-27001-require/

Commented [27A21]: Diesen Punkt löschen, falls Maßnahme A.11.2.9 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A22]: Diesen Punkt löschen, falls Maßnahme A.11.2.9 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A23]: An das in der Organisation gebräuchliche Schema anpassen.

Commented [27A24]: Diesen Punkt löschen, falls Maßnahme A.11.2.8 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

folgendermaßen verhindert: [hier angeben wie - z.B. Absperren der Einrichtung, Einsatz von PIN-

3.13. Internetnutzung

Auf das Internet darf nur über das lokale Netzwerk der Organisation mit geeigneter Infrastruktur und

Benutzergruppen oder für alle Mitarbeiter der Organisation sperren. Falls der Zugang zu bestimmten Webseiten gesperrt ist, kann der Anwender die Berechtigung für den Zugriff auf diese Seiten

werden nachdem ihre Authentizität und Korrektheit bestätigt wurde.

3.14. E-Mail und andere Verfahren für den Nachrichtenaustausch

Andere Verfahren zum Austausch von Nachrichten, abgesehen von elektronischer Post, sind auch

Gemäß [den Sicherheitsverfahren für die IT-Abteilung / der Richtlinie zur Übertragung von

darf. Ebenso legt er mögliche Beschränkungen fest, wem es gestattet ist diese Kommunikations-

verleumderischen oder anderen inakzeptablen oder illegalen Inhalten zu versenden. Nutzer dürfen keine Massenmails an Personen versenden, zu denen keine Geschäftsbeziehung besteht oder an

der Richtlinie zur Klassifizierung von Informationen schützen.

Commented [27A25]: Diesen Punkt löschen, falls Maßnahme A.13.2.3 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A26]: Das betreffende Medium kann genauer spezifiziert werden.

Commented [27A27]: Die betreffenden Foren und sozialen Netzwerke können genauer spezifiziert werden.

Commented [27A28]: Löschen, falls keine solche Richtlinie vorhanden ist.

Jede E-Mail Nachricht muss einen Haftungsausschluss enthalten. Dies gilt nicht für Nachrichten, die offizielle Sichtweise der Organisation repräsentiert.

3.15. Urheberrecht

[Stellenbezeichnung] erlaubt ist.

Anwender dürfen keine Software oder anderes Originalmaterial aus anderen Quellen vervielfältigen

Commented [27A29]: Diesen Punkt löschen, falls Maßnahme A.18.1.2 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

3.16. Mobile Computing

3.16.1. Einleitung

Ausstattung für Mobile Computing umfasst alle Arten von tragbaren Rechnern, Mobil-Telefonen,

Commented [27A30]: Diesen Punkt löschen, falls die Richtlinie zu Mobilgeräten und Telearbeit in einem separaten Dokument festgelegt ist.

Commented [27A31]: Diesen Punkt löschen, falls Maßnahme A.6.2.1 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

3.16.2. Grundsätzliche Regeln

Spezielle Sorgfalt muss angewendet werden, sobald Ausstattung für Mobile Computing in Autos oder

folgende Regeln beachten:

- werden.
- Bei der Benutzung von Mobile Computing Geräten an öffentlichen Orten ist durch den
- [hier die technische Umsetzung angeben oder auf ein Dokument mit der Beschreibung des Verfahrens beziehen]
- Umsetzung angeben oder auf ein Dokument mit der Beschreibung des Verfahrens beziehen]

Commented [27A32]: Löschen, falls Maßnahme A.11.2.6 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

- [illegible]
- [illegible] die gesamte Festplatte Pflicht ist oder nur für sensible Dateien, usw.]
- Der Schutz sensibler Daten muss in Übereinstimmung mit der [Richtlinie zur Klassifizierung von Informationen] umgesetzt sein
- [illegible]

[Stellenbezeichnung] ist verantwortlich für die Schulung und Bewusstseinsbildung (Awareness) der [illegible]

3.17. Telearbeit

Telearbeit bedeutet, dass Informations- und Kommunikations-Ausstattung eingesetzt wird, um [illegible] genehmigt werden.

[illegible]

- Schutz von Ausstattung für Mobile Computing wie in vorgenanntem Abschnitt spezifiziert
- [illegible]
- [illegible] wird
- Schutz des geistigen Eigentums der Organisation, entweder für Software oder andere [illegible]
- [illegible]
- [illegible]
- Formulierung erlaubter und verbotener Aktivitäten

3.18. Überwachung der Nutzung von Informations- und Kommunikationssystemen

Alle Daten, die über das Informationssystem oder andere Kommunikationssysteme, sowie über [illegible] gespeichert, versandt oder empfangen werden, gelten als geschäftlicher Art oder nicht, gelten als Eigentum von [illegible]

Der Anwender stimmt zu, dass Berechtigte der Organisation auf diese Daten zugreifen dürfen und [illegible]

[illegible] unerlaubten Kommunikationsmethoden und unerlaubtem Inhalt einsetzen.

Commented [27A33]: Diesen Punkt löschen, falls die Richtlinie zu Mobilgeräten und Telearbeit in einem separaten Dokument festgelegt ist.

Commented [27A34]: Diesen Punkt löschen, falls Maßnahme A.6.2.2 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Commented [27A35]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diesen Artikel:

How to apply information security controls in teleworking according to ISO 27001
https://advisera.com/27001academy/blog/2017/03/22/how-to-apply-information-security-controls-in-teleworking-according-to-iso-27001/

Commented [27A36]: Die Genehmigung kann mündlich oder [illegible]

Commented [27A37]: In kleineren Unternehmen muss dies [illegible]

3.19. Vorfälle

[redacted] möglichen Vorfall hinweist, entsprechend der Vorgaben im Verfahren zum Umgang mit [redacted].

4. Verwaltung von Aufzeichnungen die zu diesem Dokument erstellt wurden

Name der Aufzeichnung	*Aufbewahrungs-Ort*	*Verantwortlicher für Aufbewahrung*	*Maßnahme zum Schutz der Aufzeichnung*	*Aufbewahrungs-Dauer*
[Berechtigungen für die Installation von Software, die Nutzung von Java Applikationen und Active X Controls, für den Einsatz von Kryptographie, zum Download von Programmen von externen Quellen, für die Installation von Zusatzgeräten] – elektronische Form	[Intranet Ordner]	[Stellenbezeichnung]	Aufzeichnungen können nicht bearbeitet werden; nur [Stellenbezeichnung] hat die Berechtigung zum Speichern solcher Aufzeichnungen	Aufzeichnungen werden für die Dauer von 3 Jahren aufbewahrt
[Genehmigung für das Entfernen von Werten aus den Räumlichkeiten der Organisation] – elektronische Form	[Intranet Ordner]	[Stellenbezeichnung]	Aufzeichnungen können nicht bearbeitet werden; nur [Stellenbezeichnung] hat die Berechtigung zum Speichern solcher Aufzeichnungen	Aufzeichnungen werden für die Dauer von 3 Jahren aufbewahrt
[Genehmigung für den Zugriff auf ausgewählte Internetseiten] - elektronische Form	[Intranet Ordner]	[Stellenbezeichnung]	Aufzeichnungen können nicht bearbeitet werden; nur [Stellenbezeichnung] hat die Berechtigung zum Speichern solcher	Aufzeichnungen werden für die Dauer von 3 Jahren aufbewahrt

Commented [27A38]: 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.

Commented [27A39]: Nach Bedarf anpassen.

Commented [27A40]: Nach Bedarf anpassen.

Commented [27A41]: Nach Bedarf anpassen.

			Aufzeichnungen	
[Entscheidung zur zulässigen Art des Austauschs bestimmter Datentypen] - elektronische Form	[Intranet Ordner]	[Stellenbezeichnung]	Aufzeichnungen können nicht bearbeitet werden; nur [Stellenbezeichnung] hat die Berechtigung zum Speichern solcher Aufzeichnungen	Aufzeichnungen werden für die Dauer von 3 Jahren aufbewahrt
[Entscheidung zur Art der Speicherung von Nachrichten mit geschäfts-relevanten Dateninhalten] - elektronische Form	[Intranet Ordner]	[Stellenbezeichnung]	Aufzeichnungen können nicht bearbeitet werden; nur [Stellenbezeichnung] hat die Berechtigung zum Speichern solcher Aufzeichnungen	Aufzeichnungen werden für die Dauer von 3 Jahren aufbewahrt
[Genehmigung für Telearbeit] - elektronische Form	[Intranet Ordner]	[Stellenbezeichnung]	Aufzeichnungen können nicht bearbeitet werden; nur [Stellenbezeichnung] hat die Berechtigung zum Speichern solcher Aufzeichnungen	Aufzeichnungen werden für die Dauer von 3 Jahren aufbewahrt

Commented [27A42]: Nach Bedarf anpassen.

Commented [27A43]: Nach Bedarf anpassen.

Commented [27A44]: Nach Bedarf anpassen.

Nur [Stellenbezeichnung] kann anderen Mitarbeitern Zugang zu jeglichen der oben genannten Dokumente gewähren.

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 [27A45]: 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 [27A46]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.