[Logo der Organisation]

[Name der Organisation]

ERKLÄRUNG ZUR ANWENDBARKEIT

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

Commented [27A1]: Um zu erlernen, wie Sie dieses Dokument ausfüllen und echte Beispiele darüber zu sehen, was Sie schreiben müssen, schauen Sie sich dieses Video-Tutorial an:
"How to Write ISO 27001 Statement of Applicability".

Um auf das Tutorial zuzugreifen: Suchen Sie in Ihrem Posteingang die E-Mail, die Sie zum Zeitpunkt des Kaufes erhalten haben. Dort finden Sie einen Link und ein Passwort, mit denen Sie auf das Video-Tutorial zugreifen können.

Commented [27A2]: Alle mit eckigen Klammern [ ] markierte Felder in diesem Dokument müssen ausgefüllt werden.

Commented [27A3]: Für eine Anleitung wie die Erklärung zur Anwendbarkeit zu schreiben ist, lesen Sie diesen Artikel:

Die Bedeutung der Erklärung zur Anwendbarkeit für ISO 27001
https://advisera.com/27001academy/de/knowledgebase/die-bedeutung-der-erklarung-zur-anwendbarkeit-fur-iso-27001/

Commented [27A4]: 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 Definition, welche Maßnahmen zur Umsetzung in [Name der Organisation] geeignet sind, welches die Maßnahmenziele sind, wie diese umgesetzt werden, sowie die Genehmigung von Restrisiken und die formale Genehmigung der Umsetzung genannter Maßnahmen.

Dieses Dokument beinhaltet alle Maßnahmen, die in Anhang A der ISO 27001 Norm aufgeführt sind. Die Maßnahmen sind auf den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems anzuwenden.

Anwender dieses Dokuments sind alle Mitarbeiter von [Name der Organisation] mit einer Funktion im ISMS.

2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitt 6.1.3 d)
- Informationssicherheitspolitik
- Methodik zur Risikoeinschätzung und Risikobehandlung
- Bericht zur Risikoeinschätzung und Risikobehandlung

3. Anwendbarkeit von Maßnahmen

Die folgenden Maßnahmen aus ISO 27001 Anhang A sind anwendbar:

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
A.5	Sicherheitspolitik					
A.5.1	Management-Leitlinien zur Informationssicherheit					
A.5.1.1	[illegible]				[illegible]	
A.5.1.2	[illegible]				Jede Richtlinie mit einem [illegible]	
A.6	[illegible]					
A.6.1	Interne Organisation					

Commented [27A5]: Um mehr über die ISO 27001-Maßnahmen aus Anhang A zu erfahren, werfen Sie einen Blick auf dieses Buch:

ISO 27001 Annex A Controls in Plain English
https://advisera.com/books/iso-27001-annex-controls-plain-english/

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „," zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important?
https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
A.6.1.1	[illegible]				Die Verantwortlichkeiten für Informations-sicherheit sind in verschiedenen [illegible]	
A.6.1.2	Pflichtentrennung				Jede Tätigkeit, welche der Handhabung sensibler [illegible] anderen Person ausgeführt.	
A.6.1.3	[illegible]				[Stellenbezeichnung] ist [illegible]	
A.6.1.4	[illegible]				[Stellenbezeichnung] ist verantwortlich für die [illegible]	
A.6.1.5	Informationssicherheit im Projektmanagement				Der Projektmanager muss in jedem Projekt die [illegible]	
A.6.2	Mobilgeräte und Telearbeit					
A.6.2.1	[illegible]				[illegible]	
A.6.2.2	[illegible]				[IT-Sicherheitspolitik]/ [illegible]	
A.7	Personelle Sicherheit					

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „,“ zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [27A11]: Unterschiedlichen Interessengruppen können vershciedene Arbeitsfunktionen aufgetragen werden, was jeweils von deren Arbeitsspezialisierung abhängig ist.

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „," zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]	[illegible]					
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „," zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]					
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]					
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]					

> **Commented [27A9]:** Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.
>
> In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.
>
> Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „," zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.
>
> In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

> **Commented [27A10]:** Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".
>
> Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

> **Commented [27A6]:** Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

> **Commented [27A7]:** Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.
>
> Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

> **Commented [27A8]:** Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:
>
> ISO 27001 control objectives – Why are they important?
> https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „," zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „,“ zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important?
https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „," zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important?
https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „," zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [27A12]: Falls notwendig, kann eine technische Beschreibung, wie diese BereicheUmfelder voneinander abgegrenzt sind, hinzugefügt werden. Die Kriterien für den Transfer vom Entwicklungsbereich zum Testumfeld und vom Testumfeld zum betrieblichen Umfeld können ebenfalls beschrieben werden.

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]						

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „,“ zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

Commented [27A13]: Falls notwendig, kryptografischen Schutz, Zugangsbeschränkung, usw. im Einklang mit der Zugangssteuerungsrichtlinie hinzufügen.

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]						

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „," zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important?
https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]					
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „,“ zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „," zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important?
https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					
[illegible]	[illegible]					

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „," zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „," zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

ID	Maßnahmen gemäß ISO/IEC 27001	Anwend-barkeit (JA/ NEIN)	Grund für Auswahl/ Ausschluss	Maßnah-menziele	Umsetzungs-methode	Status
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	
[illegible]	[illegible]				[illegible]	

Commented [27A9]: Umsetzungs-Methode – hier das Dokument, die technische Maßnahme dazu angeben oder den Prozess beschreiben. Frei lassen, falls die Maßnahme als nicht anwendbar markiert ist.

In der Tabelle werden Dokumente aus diesem Dokumentationspaket aufgelistet, die für die jeweilige Maßnahme ausschlaggebend sind; falls keine der Dokumente für die Maßnahme relevant sind, wird der Prozess beschrieben.

Wenn zwei Dokumente durch einen Schrägstrich "/" voneinander abgesetzt sind, müssen Sie entweder das erste oder das zweite Dokument wählen. Befindet sich ein Komma „," zwischen zwei Dokumenten, so sollten für die entsprechende Maßnahme beide Dokumente implementiert werden.

In dem Dokument "Liste der Dokumente" sind alle in dem Paket enthaltenen Dokumente aufgelistet, zusammen mit einer Anmerkung, ob das jeweilige Dokument gemäß Norm obligatorisch ist oder nicht.

Commented [27A10]: Hier den Umsetzungsstatus einfüllen, z.B. "geplant", "teilweise umgesetzt", "vollständig umgesetzt".

Leer lassen, wenn die entsprechende Maßnahme als nicht anwendbar markiert ist.

Commented [27A6]: Basierend auf den Ergebnissen der Risikoeinschätzung, der vertraglichen und rechtlichen Verpflichtungen.

Commented [27A7]: Sie sollten für jede Maßnahme definiert werden und nach Möglichkeit auch messbar sein. Es ist allerdings auch möglich, die Maßnahmenziele zu kopieren, die in den Kapiteln der Abschnitte des Anhang A gelistet sind.

Leer lassen, wenn die Maßnahme als nicht anwendbar markiert ist.

Commented [27A8]: Um mehr über Maßnahmenziele zu erfahren, lesen Sie diesen Artikel:

ISO 27001 control objectives – Why are they important? https://advisera.com/27001academy/blog/2012/04/10/iso-27001-control-objectives-why-are-they-important/

4. Akzeptanz von Restrisiken

Da nicht alle Risiken über den Risikomanagement-Prozess reduziert werden konnten, werden alle Restrisiken hiermit akzeptiert:

1. [illegible]
2. [illegible]

Commented [27A14]: Die Akzeptanz von Restrisiken muss der Methodik für Risikoeinschätzung und Risikobehandlung entsprechen.

Commented [27A15]: Diesen Text und die nachstehende Tabelle löschen, falls keine Restrisiken mit den Werten 3 und 4 bestehen.

[illegible] Verzeichnis der Risikobehandlung als Quelle nutzen]

Nr.	Name des Wertes	[illegible]	[illegible]	[illegible]	Neue Auswir-kung	[illegible]	Restrisiko

5. Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab [Datum]

Der Eigentümer des Dokuments ist [Stellenbezeichnung], der das Dokument mindestens einmal jährlich und immer unmittelbar im Anschluss an eine Überprüfung der Risikoeinschätzung und Aktualisierungen der Verzeichnisse zu Risikoeinschätzung und Risikobehandlung prüfen und gegebenenfalls aktualisieren muss.

Commented [27A16]: Dies ist lediglich eine Empfehlung; Häufigkeit gegebenenfalls anpassen.

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

- [illegible]
- [illegible]
- [illegible]

[Stellenbezeichnung]
[Name]

Commented [27A17]: Die Erklärung zur Anwendbarkeit muss von den Risiko-Eigentümern, bzw. vom Top-Managment im Namen derselben, genehmigt werden.

_____
[Unterschrift]

Commented [27A18]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.