[Logo der Organisation]

[Name der Organisation]

Commented [20A1]: Alle mit eckigen Klammern [] gekennzeichneten Felder in diesem Dokument müssen ausgefüllt werden.

RICHTLINIE DES RISIKOMANAGEMENTS

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

Commented [20A2]: Das Dokumentencodierungssystem sollte mit dem bestehenden System der Organisation für die Dokumentcodierung übereinstimmen. Falls ein solches System nicht vorhanden ist, kann diese Zeile gelöscht werden.

Änderungsprotokoll

Datum	Version	Erstellt von	Beschreibung der Änderung
	0.1	20000Academy	Grundlegende Dokumentvorlage

Inhaltsverzeichnis

1. Zweck, Umfang und Nutzer

Mit dieser Richtlinie soll sichergestellt werden, dass die Risiken und Chancen von [Name der Organisation] durch einen festgelegten Prozess gesteuert werden.

Dieses Dokument wird auf alle Aktivitäten, Prozesse und Dokumente angewendet, die in dem SMS enthalten sind.

Nutzer dieses Dokumentes sind alle Mitarbeiter von [Name der Organisation] sowie alle relevanten externen Parteien, die eine Rolle in dem SMS innehaben.

2. Referenzdokumente

- ISO/IEC 20000-1:2018, Klauseln 8.5.1
- SMS-Plan
- IT Servicekontinuitäts-Management Prozess
- Verfügbarkeitsmanagementprozess
- Informationssicherheit-Managementprozess
- Lieferantenmanagement-Prozess
- Änderungsmanagement-Prozess

3. Richtlinie

3.1. Geltungsbereich und Ziele des Risikomanagements

Der Geltungsbereich des Risikomanagements von [Name der Organisation] umfasst alle Risiken und Chancen, die sich auf das SMS und die von der Organisation bereitgestellten Dienste auswirken können.

Die Ziele des Risikomanagements sind:

- zu gewährleisten, dass das SMS die beabsichtigten Ergebnisse erzielen kann
- unerwünschte Auswirkungen von Risiken zu verhindern oder zu mindern
- [illegible]
- [illegible]

3.2. Prozess-Richtlinie

Risiken und Chancen werden während der Ausführung verschiedener Prozesse des SMS identifiziert und im Risiko- und Chancenverzeichnis erfasst.

Die detaillierte Beschreibung des Prozesses ist nachfolgend dokumentiert:

3.2.1. Identifikation & Aufzeichnung

In den folgenden Phasen kann jeder Mitarbeiter neue Risiken und Chancen erkennen:

Commented [20A3]: Bitte geben Sie den Namen Ihres Unternehmens an.

Commented [20A4]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Toolkit-Ordner „04_SMS_Plan“.

Commented [20A5]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Toolkit-Ordner “ 11_Service_Gewährleistungsprozess /11.2_Service_Kontinuitätsmanagement”.

Commented [20A6]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Toolkit-Ordner “11_Service_Gewährleistungsprozess/ 11.1_Service_Verfügbarkeitsmanagement”.

Commented [20A7]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Toolkit-Ordner “11_Service_Gewährleistungsprozess/ 11.3_Informationssicherheit-Management”.

Commented [20A8]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Toolkit-Ordner “07_Relationship_und_Agreement_Prozesse/ 07.3_Lieferantenmanagement”.

Commented [20A9]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Toolkit-Ordner “09_Service_Design_Erstellen_und_Umstellungsprozess/ 09.1_Änderungsmanagement”.

Commented [20A10]: [illegible]

- [illegible]
- [illegible]
- Überprüfung der Leistung und der Effektivität des SMS und der Services
- Durchführung der Managementbewertungen
- Durchführung interner Audits
- Feedback von Kunden und anderer interessierten Parteien.

Immer wenn ein Mitarbeiter von [Name der Organisation] ein neues Risiko identifiziert, muss er dies [Stellenbezeichnung] mitteilen. [Stellenbezeichnung] erstellt einen neuen Eintrag im Risiko- und Chancenverzeichnis (im Arbeitsblatt „Risiko“).

Immer wenn ein Mitarbeiter von [Name der Organisation] eine neue Chance identifiziert, muss er dies [Stellenbezeichnung] mitteilen. [Stellenbezeichnung] erstellt einen neuen Eintrag im Risiko- und Chancenverzeichnis (im Arbeitsblatt „Chancen“).

Commented [20A11]: [illegible]

Commented [20A12]: Bitte geben Sie die entsprechende Stellenbezeichnung entsprechend Ihrer Organisationspraxis ein, z. B.: IT-Manager, Service-Manager, Risikomanager usw.

Commented [20A13]: Bitte geben Sie die entsprechende Stellenbezeichnung entsprechend Ihrer Organisationspraxis ein, z. B.: IT-Manager, Service-Manager, Risikomanager usw.

3.2.2. Bewertung

[illegible] Auswirkung und Wahrscheinlichkeit addiert werden. Auswirkung und Wahrscheinlichkeit werden anhand der folgenden Richtlinien ausgewählt:

Folgenabschätzung:

Geringe Auswirkung	0	[illegible]
[illegible]	1	Situationen, in denen zusätzliche Kosten entstehen können und die sich nur geringfügig oder mäßig auf rechtliche oder vertragliche Verpflichtungen oder den Ruf der Organisation auswirken.
Hohe Auswirkung	2	[illegible]

Wahrscheinlichkeitseinschätzung:

Geringe Wahrscheinlichkeit	0	Bestehende Kontrollen sind stark und boten bisher ein angemessenes Schutzniveau. In Zukunft werden keine neuen Vorfälle erwartet.
[illegible]	1	[illegible]

Der Risiko-Eigentümer zeichnet die Ergebnisse der Risikobewertung im Risiko- und Chancenverzeichnis (im Arbeitsblatt „Risiko“) auf.

Der zugewiesene Risikoinhaber erstellt eine Schätzung der tatsächlichen Kosten für alle identifizierten Chancenwahrnehmungen. [Stellenbezeichnung] dokumentiert die Kosten im Risiko- und Chancenverzeichnis (im Arbeitsblatt „Chancen“).

3.2.3. Beurteilung

Die folgenden Risikoakzeptanzkriterien sind vom zugewiesenen Risikoeigentümer bei der Bewertung

3.2.4. Behandlung

Jedes inakzeptable Risiko muss behandelt werden. Der zugewiesene Risikoinhaber muss für jedes inakzeptable Risiko eine Risikoreaktionsmaßnahme festlegen. Stellenbezeichnung] muss im Risiko- und Chancenverzeichnis die Risikoreaktionsmaßnahme und deren detaillierte Erläuterung anführen. Zu den Maßnahmen zur Risikoreaktion können gehören:

- Implementierung von Kontrollen zur Reduzierung des Risikos

Wenn die Risikoreaktion die Implementierung einer Kontrolle beinhaltet, dokumentiert [Stellenbezeichnung] die ausgewählte(n) Kontrolle(n) im Risiko- und Chancenverzeichnis (Arbeitsblatt „Kontrollen“).

Grundlage der Bewertungsergebnisse über eine Reaktionsmaßnahme. [Stellenbezeichnung] dokumentiert die Reaktionsmaßnahme im Risiko- und Chancenregister.

3.2.5. Monitoring

Über alle neuen Risiken und Chancen, die im Risiko- und Chancenverzeichnis dokumentiert sind,

Die Risiko-/Chanceninhaber sind für die Überwachung und Berichterstattung [vierteljährlich] über den Status des Risikos/der Chance an [Stellenbezeichnung] verantwortlich.

4. Gültigkeit und Dokumentenmanagement

Commented [20A14]:

Commented [20A15]: Bitte geben Sie die entsprechende Stellenbezeichnung entsprechend Ihrer Organisationspraxis ein, z. B.: IT-Manager, Service-Manager, Risikomanager usw.

Commented [20A16]:

Commented [20A17]: Bitte geben Sie die entsprechende Stellenbezeichnung entsprechend Ihrer Organisationspraxis ein, z. B.: IT-Manager, Service-Manager, Risikomanager usw.

Commented [20A18]: Bitte geben Sie die entsprechende Stellenbezeichnung entsprechend Ihrer Organisationspraxis ein, z. B.: IT-Manager, Service-Manager, Risikomanager usw.

Commented [20A19]: Bitte geben Sie die entsprechende Stellenbezeichnung entsprechend Ihrer Organisationspraxis ein, z. B.: IT-Manager, Service-Manager, Risikomanager usw.

Commented [20A20]: Ändern Sie die Häufigkeit gemäß Ihren Unternehmenspraktiken.

Commented [20A21]: Bitte geben Sie die entsprechende Stellenbezeichnung entsprechend Ihrer Organisationspraxis ein, z. B.: IT-Manager, Service-Manager, Risikomanager usw.

Dieses Dokument ist gültig ab [Datum].

Eigentümer dieses Dokumentes ist [Stellenbezeichnung], welcher zumindest einmal pro Jahr das Dokument überprüfen und, wenn nötig, aktualisieren muss.

Commented [20A22]: Bitte geben Sie die entsprechende Stellenbezeichnung entsprechend Ihrer Organisationspraxis ein, z. B.: IT-Manager, Service-Manager, Risikomanager usw.

Commented [20A23]: Dies ist nur eine Empfehlung. Bitte passen Sie die Häufigkeit entsprechend Ihren Unternehmenspraktiken an.

5. Verwaltung der auf Grundlage dieses Dokumentes aufbewahrten Aufzeichnungen

Name der Aufzeichnung	Aufbewahrungs-Ort	Verantwortlicher für Aufbewahrung	Maßnahme zum Schutz der Aufzeichnung	Aufbewahrungs-Dauer
Verzeichnis der Risiken und Chancen	[Werkzeugname]	[Stellenbezeichnung]	[Stellenbezeichnung]	[...]

Commented [20A24]: Bitte geben Sie die entsprechende Stellenbezeichnung entsprechend Ihrer Organisationspraxis ein, z. B.: IT-Manager, Service-Manager, Risikomanager usw.

Commented [20A25]: Bitte geben Sie die entsprechende Stellenbezeichnung entsprechend Ihrer Organisationspraxis ein, z. B.: IT-Manager, Service-Manager, Risikomanager usw.

Commented [20A26]: Beispiel: für das aktuelle Jahr (seit Jahresbeginn bis heute) - in [Werkzeugname], andernfalls archiviert in [Werkzeugname oder Archivort].

6. Anhänge

- Anhang 1 – Verzeichnis der Risiken und Chancen

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [20A27]: Nur erforderlich, wenn das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen vorschreibt, dass Papierdokumente unterschrieben werden müssen.