[Logo der Organisation]

[Name der Organisation]

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

INFORMATIONSICHERHEITSMANAGEMENT-PROZESS

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

Commented [20A2]: Das Codierungssystem eines Dokuments sollte im Einklang mit dem bestehenden System zur Dokumenten-Codierung des Unternehmens sein. Im Falle, dass ein solches System nicht vorhanden ist, kann diese Zeile gelöscht werden.

Change-Historie

Datum	Version	Erstellt von	Beschreibung des Change
	0.1	20000Academy	Grundlegende Dokumentenvorlage

Inhaltsverzeichnis

1. Zweck, Umfang und Anwender

Das Ziel dieses Dokuments ist, den Zweck, den Umfang, die Prinzipien und die Aktivitäten des Informationssicherheitsmanagement-Prozesses zu definieren.

Dieses Dokument wird auf alle Prozesse und Aktivitäten des SMS angewandt.

Anwender dieses Dokuments sind alle Mitarbeiter von [Name der Organisation] sowie alle externen Parteien, die eine Rolle im SMS haben.

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

2. Referenzdokumente

- ISO 20000-1:2018, Klauseln 7.5.4.e), 8.7.3.
- Vorfallmanagement-Prozess
- Service Request Management-Prozess
- Informationssicherheit-Richtlinien
- ISO 20000-1:2011, Klauseln 6.6.; 8.1.; 9.2.

Commented [20A4]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Dokumentations- Toolkit-Ordner "10_Resolution_Fulfillment_Prozesse/ 10.1_Vorfallmanagement".

Commented [20A5]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Dokumentations- Toolkit-Ordner "10_Resolution_Fulfillment_Prozesse/ 10.2_Service_Request_Management".

3. Prozessübersicht

Die Aktivitäten des Informationssicherheit-Managements sind in den Informationssicherheits-Richtlinien beschrieben.

[redacted]

Commented [20A6]: [redacted]

4. Rollen und Verantwortlichkeiten

[Stellenbezeichnung] weist die Rolle des Sicherheitsmanagers zu.

Commented [20A7]: Bitte geben Sie die entsprechende Stellenbezeichnung entsprechend Ihrer Organisationspraxis ein, z. B.: IT-Manager, Chief Sicherheitsbeauftragter, Chief Informationssicherheitsbeauftragter usw.

Verantwortlichkeiten des Informationssicherheits-Managers:

- Gesamtverantwortung für die Durchführung von Aktivitäten im Rahmen des Informationssicherheits-Management-Prozesses.
- Koordinierung mit anderen Service Management-Rollen.
- Verantwortlich für Berichterstellung und Informationsmanagement.
- Entwickelt und wartet die Informationssicherheits-Richtlinien.
- [redacted]

- Überwacht und handhabt alle Sicherheitsverstöße.
- [illegible]
- [illegible]

Commented [20A8]: [illegible]

5. Messung und Berichterstattung

Der Informationssicherheitsmanager ist verantwortlich für:

- Definition und Bewertung [jährlich] der kritischen Erfolgsfaktoren (CSFs), die die im SMS-Plan definierten aktuellen SMS-Ziele und die entsprechenden Leistungskennzahlen (KPIs) unterstützen, mit denen der Fortschritt bei der Erreichung der CSFs überwacht werden kann.
- Dokumentierung der ausgewählten CSFs und KPIs in der Matrix der Prozess Messungen.
- Sicherstellung, dass die Messungen gemäß der definierten Häufigkeit durchgeführt werden und Dokumentierung des Ergebnisses in der Matrix der Prozessmessungen.
- [illegible]
- [illegible]
- [illegible]

Commented [20A9]: Sie können die Häufigkeit entsprechend Ihren Unternehmenspraktiken ändern.

Commented [20A10]: Eine Vorlage für dieses Dokument finden Sie im ISO 20000 Toolkit-Ordner „13_Managementbewertung“.

Commented [20A11]: [illegible]

Commented [20A12]: [illegible]

Commented [20A13]: [illegible]

Immer wenn die SMS-Ziele im SMS-Plan aktualisiert werden, bewertet und aktualisiert der Informationssicherheitsmanager die CSFs und KPIs in der Matrix der Prozessmessungen, um die neuen Ziele widerzuspiegeln.

6. Verwaltung der Datensätze, die aufgrund dieses Dokuments aufbewahrt werden

Name des Records	Speicherort	Verantwortliche Person für die Speicherung	Zugriffskontrollen für die Sicherheit der Records	Aufbewahrungszeit
Informations-sicherheit-Richtlinien	[Ort eintragen]	Informations-sicherheit-Manager	Informations-sicherheit- Manager	Richtlinien werden aktualisiert; alte Version wird archiviert und 2 Jahre aufbewahrt.
Berichte	[Tool-Name]	Informations-sicherheit-Manager	Informations-sicherheit-Manager	Berichte werden für [3 Jahre] aufbewahrt.

Commented [20A14]: Ändern, wenn nötig.

Commented [20A15]: Ändern, wenn nötig.

Commented [20A16]: Sie können die Aufbewahrungsdauer an Ihre Unternehmenspraktiken anpassen.

7. Gültigkeit und Dokumenten-Management

Dieses Dokument ist gültig ab [Datum].

Eigentümer dieses Dokuments ist [Stellenbeschreibung], der das Dokument überprüfen und, wenn nötig, zumindest einmal pro Jahr aktualisieren muss.

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

Commented [20A18]: Dies ist nur eine Empfehlung; Passen Sie die Häufigkeit entsprechend Ihren Unternehmenspraktiken an.

8. Anhänge

- Anhang 1 – Informationssicherheits-Richtlinien

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [20A19]: Nur nötig, wenn das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen vorgibt, dass Papierdokumente unterzeichnet werden müssen