[Logo der Organisation]

[Name der Organisation]

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

INFORMATIONSICHERHEITSMANAGEMENT-RICHTLINIEN

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, die Ausrichtung, die Prinzipien und die grundsätzlichen Regeln von Informationssicherheit zu definieren.

Dieses Dokument wird auf alle Verfahren 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 8.7.3, 7.5.4.e)
- Informationssicherheitsmanagement-Prozess
- IT-Service Kontinuitätsmanagement Prozess
- Service Verfügbarkeitsmanagement-Prozess
- Vorfallmanagement-Prozess
- Änderungsmanagement-Prozess

Commented [20A4]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Dokumentations- Toolkit-Ordner „11_Service_Gewährleistungsprozesse / 11.2_IT_Service_Kontinuitätsmanagement“.

Commented [20A5]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Dokumentations- Toolkit-Ordner „11_Service_Gewährleistungsprozesse / 11.1_Verfügbarkeitsmanagement”.

Commented [20A6]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Dokumentations- Toolkit-Ordner “10_Resolution_Fulfillment_Prozesse/ 10.1_Vorfallmanagement”.

Commented [20A7]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Dokumentations- Toolkit-Ordner “09_Service_Design_Erstellen_Umstellung_Prozesse/ 09.1_Änderungsmanagement”.

3. Begriffsbestimmungen

Vertraulichkeit – Merkmal der Informationen, wodurch sie nur für autorisierte Personen oder Systeme zugänglich sind.

Integrität – Merkmal der Informationen, wodurch sie nur von autorisierten Personen oder Systemen auf erlaubte Weise geändert werden dürfen.

Zugänglichkeit – Merkmal der Informationen, wodurch darauf nur durch autorisierte Personen zugegriffen werden kann, wenn sie benötigt werden.

[illegible]

[illegible]

4. Ziel

Das Ziel vom Informationssicherheit- Management ist, die Vertraulichkeit, Integrität und Zugänglichkeit von Informationswerten, Unternehmenswerten und Services zu gewährleisten.

[illegible]

Commented [20A8]: [illegible]

4.1 Informationssicherheit-Richtlinien

Die Informationssicherheit-Richtlinien sind eine Leitlinie, die Regeln für die Verwendung und missbräuchliche Verwendung der Informationssicherheit von [Name der Organisation) vorgibt.

[Stellenbezeichnung] genehmigt die Informationssicherheit-Richtlinien.

Commented [20A9]: Bitte geben Sie die entsprechende Stellenbezeichnung vom Top-Management gemäß Ihren Organisationspraktiken ein, z. B.: CEO, CIO, IT-Direktor, IT-Manager usw.

[illegible]

[illegible]

Commented [20A10]: [illegible]

4.2 Informationssicherheit-Anforderungen

Gesetzliche und behördliche Anforderungen, sowie vertragliche Verpflichtungen, welche für die Organisation im Bereich der Informationssicherheit relevant sind und die von Informationssicherheit-Aktivitäten eingehalten werden, sind im SMS-Plan aufgelistet.

Commented [20A11]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Dokumentations- Toolkit-Ordner “04_SMS_Plan”.

Service-Anforderungen, die von Informationssicherheit-Aktivitäten erfüllt werden, sind den Service Level-Anforderungen aufgelistet.

Commented [20A12]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Dokumentations- Toolkit-Ordner “07_Relationship_Agreement_Prozesse/ 07.2_Service_Level_Management”.

4.3 Risikomanagement

Commented [20A13]: [illegible]

Der Informationssicherheitsmanager ist dafür verantwortlich, Informationssicherheitsrisiken festzustellen und das Risiko und Chancen-Verzeichnis auszufüllen. Der Risikolevel wird entsprechend [illegible]

Commented [20A14]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Dokumentations- Toolkit-Ordner “05_Lenkung_der_Risikent”.

Commented [20A15]: [illegible]

4.4 Informationssicherheits-Kontrollen

[Name der Organisation] hat implementiert und betreibt physische, administrative und technische Informationssicherheit-Kontrollen. Der Informationssicherheitsmanager ist dafür verantwortlich, sicherzustellen, dass:

- Sicherheits-Kontrollen identifiziert und im Verzeichnis der Risiken und Chancen dokumentiert werden,
- Sicherheits-Kontrollen eine Risikobeschreibung enthalten, auf welche sich die Kontrollen beziehen,
- Sicherheits-Kontrollen eine Beschreibung des Betriebs und der Wartung enthalten.

Die Effektivität der Kontrollen wird während der internen Sicherheits-Audits überprüft. Der interne Audit-Bericht enthält die notwendigen Aktionen.

Commented [20A16]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Dokumentations- Toolkit-Ordner “12_Interner_Audit”.

[Stellenbezeichnung] ist für Folgendes verantwortlich:

Commented [20A17]: Bitte geben Sie die entsprechende Stellenbezeichnung gemäß Ihren Organisationspraktiken ein, z. B.: Informationssicherheit- Manager, Supplier Manager und Service Level Manager.

- [illegible]
- [illegible]

Commented [20A18]: [illegible]

4.5 Interne Audits

Ein interner Informationssicherheit-Audit wird [einmal pro Jahr] durchgeführt. [Stellenbezeichnung] ernennt einen Auditor.

Commented [20A19]: Sie können die Häufigkeit an Ihre Unternehmenspraktiken anpassen.

Commented [20A20]: Bitte geben Sie die entsprechende Stellenbezeichnung des Top-Managements gemäß Ihren Organisationspraktiken ein, z. B.: CEO, CIO, IT-Direktor, IT-Manager usw.

[illegible]

Der Informationssicherheitsmanager ist dafür verantwortlich, die Lösung der Ergebnisse des internen Audits, für die ein Formular für Korrektur- und Vorbeugungsmaßnahmen aufgezeichnet wurde, zu verfolgen und zu managen.

Commented [20A21]: Sie finden eine Vorlage für dieses Dokument im ISO 20000 Dokumentations- Toolkit-Ordner “12_Interner_Audit”.

4.6 Kommunikation der Richtlinien

Der Informationssicherheitsmanager hat sicherzustellen, dass alle Mitarbeiter von [Name der [illegible] Wichtigkeit der Einhaltung dieser Richtlinien vertraut sind.

Commented [20A22]: [illegible]

Nach jeder größeren Änderung der Richtlinie und mindestens [einmal im Jahr] sendet der [illegible] Erinnerung an die Wichtigkeit der Einhaltung der Richtlinie darstellt.

Commented [20A23]: Sie können die Häufigkeit an Ihre Unternehmensrichtlinien anpassen.

Commented [20A24]: [illegible]

4.7 Sicherheitsvorfall- Management

Sicherheitsvorfälle werden durch den Vorfallmanagement-Prozess verwaltet. [illegible] Vorfallmanager.

Commented [20A25]: Geben Sie die Kategorie der Informationssicherheitsvorfälle ein.

[illegible]

Der Informationssicherheitsmanager analysiert die Arten, den Umfang und die Auswirkungen von Informationssicherheitsvorfällen.

Informationssicherheitsvorfälle werden überprüft und Verbesserungen werden durch den Informationssicherheitsmanager identifiziert.

5. Gültigkeit und Dokumenten-Management

Dieses Dokument ist gültig ab [Datum].

[illegible]

Commented [20A26]: Bitte geben Sie die entsprechende Stellenbezeichnung entsprechend Ihrer Organisationspraxis ein, z. B.: IT-Manager, Service-Manager, Informationssicherheits-Manager usw.

Commented [20A27]: [illegible]

[Stellenbezeichnung] genehmigt diese Richtlinien.

Commented [20A28]: Bitte geben Sie die entsprechende Stellenbezeichnung vom Top-Management gemäß Ihrer Organisationspraxis ein, z. B.: CEO, CIO, IT-Direktor, IT-Manager usw.

[Name der Organisation]

[Stellenbezeichnung]
[Name]

____
[Unterschrift]

Commented [20A29]: Nur nötig, wenn das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen vorgibt, dass Papierdokumente unterzeichnet werden müssen