[Logo der Organisation]

[Name der Organisation]

ZUGANGSSTEUERUNGSRICHTLINIE

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

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

Commented [27A2]: Um mehr über dieses Thema zu erfahren, lesen Sie bitte diesen Artikel:

How to handle access control according to ISO 27001
https://advisera.com/27001academy/blog/2015/07/27/how-to-handle-access-control-according-to-iso-27001/

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 von Regelungen für den Zugang zu verschiedenen Systemen, Gerätschaften, Einrichtungen und Informationen auf Basis der geschäftlichen und Sicherheitsanforderungen an den Zugang.

Dieses Dokument gilt für den gesamten Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS), d.h. für alle Systeme, Gerätschaften, Einrichtungen und Informationen, die innerhalb des ISMS Anwendungsbereiches genutzt werden.

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

2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitte A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.3
- Informationssicherheitspolitik
- Erklärung zur Anwendbarkeit
- [Richtlinie zur Klassifizierung von Informationen]
- [Erklärung zur Akzeptanz von ISMS-Dokumenten]
- [Liste gesetzlicher, amtlicher, vertraglicher und anderer Anforderungen]

Commented [27A4]: Falls Ihnen eine solche Liste nicht vorliegt, können Sie hier zusätzliche Aufzählungspunkte mit allen gesetzlichen Auflagen und vertraglichen Verpflichtungen einfügen, die Anforderungen für die Zugangssteuerung enthalten.

3. Zugangssteuerung

3.1. Einleitung

[illegible] System und jeden Dienst geben.

Commented [27A5]: Löschen, falls Maßnahme A.9.2.1 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Der Zugang zu allen physischen Bereichen der Organisation ist erlaubt, ausgenommen zu Bereichen, [illegible]

Vorliegende Richtlinie spezifiziert Regelungen für den Zugang zu Systemen, Diensten und [illegible]

Commented [27A6]: Löschen, falls die Richtlinie zur Klassifizierung von Informationen nicht dokumentiert ist.

3.2. Benutzer-Profil A

Commented [27A7]: An das in der Organisation übliche Benennungs-Schema anpassen.

Benutzer-Profil A besitzt die folgenden Zugangsberechtigungen:

[illegible]	***Benutzerberechtigungen***

Commented [27A8]: Dies kann auf Ebene des kompletten Systems oder für einzelne Module angegeben werden.

Commented [27A9]: Konkreter angeben, ob diese [illegible]

Folgende Stellenbezeichnungen besitzen Benutzerberechtigungen entsprechend Benutzer-Profil A:

- [illegible]
- [illegible]

Commented [27A10]: Alle Stellenbezeichnungen auflisten. Es [illegible]

3.3. Benutzer-Profil B

Commented [27A11]: Weitere Benutzer-Profile können, wie in diesem Punkt beschrieb en, aufgelistet werden.

Benutzer-Profil B besitzt die folgenden Zugangsberechtigungen:

[illegible]	[illegible]

Commented [27A12]: Dies kann auf Ebene des kompletten Systems oder für einzelne Module angegeben werden.

Commented [27A13]: Konkreter angeben, ob diese [illegible]

Folgende Stellenbezeichnungen besitzen Benutzerberechtigungen entsprechend Benutzer-Profil B:

- [illegible]
- [illegible]

3.4. Verwaltung von Sonderrechten

Commented [27A14]: Löschen, falls Maßnahme A.9.2.3 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

[illegible]

Commented [27A15]: Diese Tabelle kann durch eine Erklärung [illegible]

[illegible]	[illegible]	***Art des Genehmigungs-Verfahrens***

Commented [27A16]: Per E-Mail, durch schriftlichen Beschluss, mündlich, durch das System, usw. – nach Möglichkeit sollte es hierzu eine Aufzeichnung geben.

Bei der Zuteilung von Sonderrechten muss der Verantwortliche sowohl die Geschäfts- und [illegible] der Richtlinie zur Klassifizierung von Informationen zugegriffen werden kann.

3.5. Regelmäßige Überprüfung von Zugangsrechten

Commented [27A17]: Löschen, falls Maßnahme A.9.2.5 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

[illegible] übereinstimmen:

Commented [27A18]: Nach Bedarf anpassen.

[illegible]	***Intervalle für regelmäßige Überprüfung***

Commented [27A19]: Die Häufigkeit sollte entsprechend des, [illegible]

[illegible]

Commented [27A20]: Ein Formblatt, ein formaler Bericht, handschriftliche Notizen, usw. können verwendet werden.

3.6. Statusänderung oder Vertragsbeendigung

Commented [27A21]: Löschen, falls Maßnahme A.9.2.6 in der Erklärung zur Anwendbarkeit als Ausschluss behandelt wird.

Bei Änderung oder Beendigung der Anstellung muss [Stellenbezeichnung] umgehend die [redacted]

[redacted] Verantwortlichen informieren, welche den entsprechenden externen Parteien Berechtigungen erteilt haben.

[redacted] Verantwortlichen entzogen oder geändert werden.

3.7. Technische Umsetzung

Die technische Umsetzung der Erteilung oder Entziehung von Benutzerberechtigungen wird von [redacted]

[redacted]	***Verantwortlicher für die Durchführung***

[redacted] Benutzerberechtigungen autorisiert sind.

3.8. Verwaltung von Benutzer-Passworten

Commented [27A22]: Diesen Punkt löschen, falls die Passwort-Richtlinie in einem separaten Dokument festgelegt ist.

Bei der Vergabe und Benutzung von Anwender-Passworten müssen folgende Regelungen befolgt werden:

Commented [27A23]: Diese Regeln an die festgestellten Risiken und an System-Funktionalitäten anpassen.

Commented [27A24]: Unterschiedliche Regeln können für Administrator- und Benutzer-Passworte festgelegt werden.

- [redacted] vorgeschrieben
- [redacted]

- Jeder Nutzer muss gegebenenfalls die Möglichkeit haben, sein/ihr eigenes Passwort [redacted]
- [redacted]
- Temporäre Passworte müssen dem Nutzer auf eine sichere Weise kommuniziert werden und die Identität des Nutzers muss vorher überprüft werden
- [redacted]
- [redacted] wählen
- Das Passwortmanagement-System muss Nutzer dazu zwingen, ihre Passworte vierteljährlich zu ändern
- [redacted]
- [redacted]
- Das Passwort darf während der Anmeldung nicht offen einsehbar sein
- [redacted]
- [redacted] erstmaligen Einrichtung geändert werden
- [redacted]

Commented [27A25]: Hierzu können weitere Details angegeben werden.

Commented [27A26]: z.B. durch E-Mail Versand einer Anweisung an den Benutzer.

Commented [27A27]: z.B. durch Anmeldung am System innerhalb einer bestimmten Zeitspanne, usw.

4. Verwaltung von Aufzeichnungen die zu diesem Dokument erstellt wurden

Name der Aufzeichnung	***Aufbewahrungs-Ort***	***Verantwortlicher für Aufbewahrung***	***Maßnahme zum Schutz der Aufzeichnung***	***Aufbewahr Dauer***
[Nachweis für die Zuteilung von Sonderrechten (in elektronischer Form - E-Mail Nachricht)]	[Intranet Ordner]	[Stellenbezeichnung des für die technische Umsetzung Verantwortlichen]	Die Aufzeichnung kann nicht bearbeitet werden; ausschließlich [Stellenbezeichnung] ist berechtigt, solche Aufzeichnungen aufzubewahren	Aufzeichnu werden für die Dauer von 3 Jahren aufbewahrt
[Protokolle der regelmäßigen Überprüfung von Zugangsberechtigungen]	[Rechner von [Stellenbezeichnung] / Schrank von [Stellen-bezeichnung]]	[Stellenbezeichnung]	Nur [Stellenbezeichnung] hat Zugangsberechtigung zu solchen	Aufzeichnungen werden für die Dauer von 3 Jahren aufbewahrt

Commented [27A28]: 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 [27A29]: Nach Bedarf anpassen.

Commented [27A30]: Nach Bedarf anpassen.

			Aufzeichnungen	

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 halbjährlich prüfen und gegebenenfalls aktualisieren muss.

Commented [27A31]: 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]
- [illegible]

[Stellenbezeichnung]
[Name]

____
[Unterschrift]

Commented [27A32]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.