[Logo der Organisation]

[Name der Organisation]

BRING YOUR OWN DEVICE (BYOD) RICHTLINIE

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

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

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

How to write an easy-to-use BYOD policy compliant with ISO 27001 https://advisera.com/27001academy/blog/2015/09/07/how-to-write-an-easy-to-use-byod-policy-compliant-with-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 es, zu definieren, wie [Name der Organisation] die Kontrolle über organisationseigene Informationen behält, während solche Informationen über Geräte abgerufen werden, welche nicht das Eigentum der Organisation sind.

Dieses Dokument bezieht sich daher auf alle persönlichen Geräte, welche die Fähigkeit zur Speicherung, Übertragung oder Bearbeitung jeglicher sensibler Daten aus dem Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS) besitzen. Zu diesen Geräten zählen unter anderem Laptop-Computer, Smartphones, Tablet-Computer, USB-Memorysticks, Digitalkameras, usw., welche im Rahmen dieser Richtlinie kollektiv als BYOD (Bring Your Own Device = Bringe Dein Eigenes Gerät (mit)) bezeichnet werden.

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

2. Referenzdokumente

- ISO/IEC 27001 Norm, Abschnitte A.6.2.1, A.6.2.2, A.13.2.1

3. Sicherheitsregeln zur Nutzung von BYOD

Die in dieser Richtlinie aufgestellten Regeln gelten für alle BYOD, und gleichgültig ob sie für [redacted]

3.1. Unternehmensrichtlinie

[Name der Organisation] unterstützt die umfassende Nutzung von BYOD für Arbeitszwecke, d.h. die [redacted]

[redacted]

BYOD ist, so behält sie sich dennoch das Recht zur Lenkung dieser Daten vor.

Commented [27A4]: Alternativ können Sie diesen Teil durch [redacted]

3.2. Wem ist die Nutzung von BYOD gestattet, und wofür?

[redacted]

haben.

[Stellenbezeichnung] stellt eine Liste von Anwendungen auf, zu denen der Zugang mittels BYOD verboten ist.

3.3. Welche Geräte sind erlaubt?

[illegible] **Commented [27A5]:** z.B. Firewall, Backup, Bildschirmverriegelung, usw.

3.4. Zulässige Nutzung

Für jedes BYOD ist folgendes obligatorisch:

- [illegible]
- [illegible] Mobilgeräte, usw.]
- [Hier die anzuwendende Verschlüsselungsmethode beschreiben und ihren Zweck]
- [illegible] **Commented [27A6]:** z.B. Kennwörter, numerische Kennwörter, biometrische Leser, usw.
- [illegible] **Commented [27A7]:** z.B. Virtuelles Privates Netzwerk (VPN)
- [illegible]
- Wird ein BYOD in der Öffentlichkeit benutzt, so muss der Eigentümer sicherstellen, dass [illegible]
- [illegible]
- [illegible] Informationen] zusätzlich geschützt werden
- [Stellenbezeichnung] ist davon zu unterrichten, bevor ein BYOD entsorgt, verkauft oder einer [illegible]

Das folgende ist mit einem BYOD nicht erlaubt:

- [illegible]
- [illegible]
- [illegible]
- Installierung nicht-lizenzierter (illegaler) Software
- Verbindungen über Bluetooth
- [illegible]
- [illegible]
- Lokale Speicherung der folgenden Daten/Informationen: [Liste sensibler Daten/Informationen]
- [illegible]

3.5. Besondere Rechte

[Name der Organisation] behält sich das Recht vor, sämtliche Firmendaten, die auf einem BYOD [illegible]

[illegible] überwachen.

[Name der Organisation] hat das Recht, sämtliche auf BYOD gespeicherten Daten zu löschen, welche [redacted]

Commented [27A8]: Falls technisch möglich, können Sie hier schreiben: "alle auf BYOD gespeicherten Firmendaten".

3.6. Rückvergütung

[redacted]

Commented [27A9]: Alternativ können Sie hier eine Gebühr definieren, welche an die Mitarbeiter bezahlt wird.

[Name der Organisation] stellt jedoch eine Vergütung für folgendes bereit:

- [redacted]
- [redacted] monatlichen Telekommunikationsrechnung des Geräteigentümers

3.7. Sicherheitsverstöße

Sämtliche Sicherheitsverstöße im Zusammenhang mit BYOD müssen unverzüglich an [redacted]

Commented [27A10]: Dies ist üblicherweise der Sicherheitsbeauftragte oder das Help Desk.

3.8. Training und Awareness

Commented [27A11]: Diese Schulung wird Ihnen dabei helfen, das Sicherheitsbewusstsein zu steigern und das Wissen Ihrer Mitarbeiter zu verfolgen: https://training.advisera.com/awareness-session/security-awareness-training/

[redacted] bezüglich der am häufigsten vorkommenden Bedrohungen oder Gefährdungen.

4. Verwaltung der auf der Basis dieses Dokuments aufbewahrten Aufzeichnungen

Name der Aufzeichnung	Aufbewahrungsort	Für die Aufbewahrung verantwortliche Person	Maßnahmen für Aufzeichnungsschutz	Aufbewahrungszeit
[Liste der berechtigten Anwender von BYOD und wozu sie Zugang haben]	[Intranet der Firma]	[Stellen-bezeichnung]	Nur [Stellenbezeichnung] darf die Liste bearbeiten und eine neue Version derselben herausgeben	Eine ungültig gewordene Liste wird 3 Jahre lang archiviert
[Liste der erlaubten BYOD, sowie deren	[Intranet der Firma]	[Stellen-bezeichnung]	Nur [Stellenbezeichnung] darf die Liste	Eine ungültig gewordene Liste wird 3 Jahre lang

Commented [27A12]: 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 [27A13]: Nach Bedarf anpassen.

Commented [27A14]: Nach Bedarf anpassen.

jeweiligen Einstellungen]			bearbeiten und eine neue Version derselben herausgeben	archiviert
[Liste der verbotenen BYOD Anwendungen]	[Intranet der Firma]	[Stellen-bezeichnung]	Nur [Stellenbezeichnung] darf die Liste bearbeiten und eine neue Version derselben herausgeben	Eine ungültig gewordene Liste wird 3 Jahre lang archiviert

Commented [27A15]: Nach Bedarf anpassen.

5. Gültigkeit und Dokumenten-Handhabung

Dieses Dokument ist gültig ab [date].

Der Eigentümer dieses Dokuments ist [Stellenbezeichnung], und dieser muss das Dokument mindestens einmal jährlich und gegebenenfalls aktualisieren. [Stellenbezeichnung] überprüft alle 3 Monate die Liste der berechtigten Anwender, die Liste der erlaubten Geräte, sowie die Liste der verbotenen Anwendungen.

Commented [27A16]: Dies ist lediglich eine Empfehlung. Häufigkeit nach Bedarf anpassen.

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

- [illegible]
- [illegible]

[Stellenbezeichnung]
[Name]

_____
[Unterschrift]

Commented [27A17]: Nur notwendig, falls das Verfahren zur Lenkung von Dokumenten und Aufzeichnungen das Unterschreiben von Papierdokumenten vorschreibt.