					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P03S					Dokumenttitel: **Richtlinie zur zulässigen Nutzung**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

An relevanten Standards und Vorschriften ausgerichtet

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Abschnitt 5	Relevant für den allgemeinen Geltungsbereich und die Umsetzung der Richtlinie
ISO/IEC 27002:2022	5.10, 5.11, 5	Leitlinien zu Anforderungen und Maßnahmen für die zulässige Nutzung
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Deckt die Nutzung von Systemen/Geräten, Überwachung und Benutzerschulung ab
EU GDPR	Artikel 5(1)(f), 32	Integrität und Vertraulichkeit von Daten sowie Sicherheitsmaßnahmen
EU NIS2	Artikel 21(2)(b)	Verlangt angemessene Sicherheitsrichtlinien einschließlich Regeln zur zulässigen Nutzung
EU DORA	Artikel 9	Richtlinie für das IKT-Risikomanagement, Kontrollen und Durchsetzung
COBIT 2019	DSS05, BAI	Sicherheitsdienste und Wissensmanagement

1. Zweck

1.1. Diese Richtlinie definiert die zulässige, verantwortungsvolle und sichere Nutzung der vom Unternehmen bereitgestellten Systeme, Geräte, Internetzugänge, E-Mail-Dienste und Cloud-Services sowie von privat genutzten Geräten, die für geschäftliche Zwecke verwendet werden.

1.2. Sie stellt sicher, dass alle Personen ihre Verpflichtungen bei der Nutzung der IT-Ressourcen der Organisation verstehen und dabei Datenintegrität, Datenschutz und Betriebskontinuität schützen.

1.3. Diese Richtlinie unterstützt die Einhaltung der ISO/IEC 27001:2022, indem sie klare Standards für das Benutzerverhalten festlegt, die an gesetzliche, vertragliche und regulatorische Anforderungen angepasst sind.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für alle Personen, die auf Unternehmenssysteme oder Daten zugreifen, diese verwalten oder mit ihnen interagieren, einschließlich:

2.1.1. Mitarbeiter und Auftragnehmer

2.1.2. Zeitarbeitskräfte und Praktikanten

2.1.3. Externe IT-Dienstleister

2.2. Sie umfasst:

2.2.1. Unternehmenseigene Computer, Telefone und Tablets

2.2.2. Für die geschäftliche Nutzung genehmigte private Geräte (Bring Your Own Device, BYOD)

2.2.3. Unternehmensnetzwerke, Cloud-Plattformen und Softwaredienste

2.2.4. Internetzugang, E-Mail-Systeme, gemeinsam genutzte Speicherbereiche und Geschäftsanwendungen

2.3. Diese Richtlinie gilt in allen Arbeitsumgebungen – vor Ort, im Remote-Betrieb und in hybriden Umgebungen – sowie während der gesamten Geschäftszeiten.

3. Ziele

3.1. Festlegung, was als zulässige und unzulässige Nutzung von IT-Systemen gilt.

3.1.1. Verringerung von Sicherheitsrisiken durch missbräuchliche Nutzung, unbefugten Zugriff oder das Einschleusen von Schadsoftware.

3.1.2. Schutz von Geschäftsdaten, Kundeninformationen und dem Ansehen des Unternehmens.

3.1.3. Festlegung durchsetzbarer Regeln und Sicherstellung der Rechenschaftspflicht aller Benutzer.

3.1.4. Unterstützung von Überwachung und Compliance, um Verstöße frühzeitig zu erkennen und Korrekturmaßnahmen einzuleiten.

4. Rollen und Verantwortlichkeiten

4.1. Geschäftsführer (GM)

4.1.1. Genehmigt diese Richtlinie und stellt sicher, dass die für ihre Durchsetzung erforderlichen Ressourcen und Befugnisse vorhanden sind.

4.1.2. Prüft und genehmigt alle Ausnahmen von dieser Richtlinie.

4.2. IT-Manager oder IT-Support-Dienstleister

4.2.1. Führt Verzeichnisse der genehmigten Software und Hardware.

4.2.2. Konfiguriert Geräte zur Durchsetzung der Regeln zur zulässigen Nutzung (z. B. Inhaltsfilterung, Zugriffsprotokollierung).

4.2.3. Überwacht die Nutzung auf potenzielle Verstöße und untersucht Sicherheitsvorfälle.

4.2.4. Stellt sicher, dass private Geräte (Bring Your Own Device, BYOD) bei geschäftlicher Nutzung autorisiert und sicher konfiguriert sind.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Anforderungen an Überprüfung und Aktualisierung

9.1. Jährliche Überprüfung

9.1.1. Diese Richtlinie muss jährlich durch den IT-Manager und mit abschließender Genehmigung durch den Geschäftsführer (GM) überprüft werden, um sicherzustellen, dass sie weiterhin auf Nutzungsmuster von Technologien, neu auftretende Risiken und Compliance-Verpflichtungen abgestimmt ist.

9.2. Anlässe für außerplanmäßige Überprüfungen

9.2.1. Überprüfungen müssen außerdem durchgeführt werden bei:

9.2.2. neuen Systemen oder Technologien (z. B. neuer Cloud-Service oder neue Endpoint-Plattform)

9.2.3. erheblichen Richtlinienverstößen

9.2.4. aktualisierten Gesetzen oder Vertragsbedingungen, die die IT-Nutzung betreffen

9.3. Änderungsdokumentation

9.3.1. Alle Aktualisierungen müssen in einem Versionsprotokoll dokumentiert werden, das Folgendes enthält:

9.3.1.1. Versionsnummer

9.3.1.2. Prüfdatum

9.3.1.3. Zusammenfassung der Änderungen

9.3.1.4. Genehmigende Stelle

9.4. Kommunikation der Richtlinie

9.4.1. Überarbeitete Fassungen dieser Richtlinie müssen allen betroffenen Benutzern bereitgestellt werden. Mitarbeiter müssen den Erhalt und das Verständnis im Rahmen ihrer Verpflichtungen zur Security-Awareness-Schulung bestätigen.

10. Zugehörige Richtlinien und Verknüpfungen

10.1. Diese Richtlinie wirkt mit mehreren anderen SME-Richtlinien zusammen, um eine umfassende Abdeckung der Sicherheitsverantwortlichkeiten sicherzustellen:

10.1.1. P4S – Richtlinie zur Zugriffskontrolle: Definiert die technische und verfahrensbezogene Durchsetzung der zulässigen Nutzung und von Kontobeschränkungen.

10.1.2. P8S – Richtlinie zur Sensibilisierung für Informationssicherheit und Schulung: Regelt die Benutzerschulung zu den Grenzen der zulässigen Nutzung und zu Meldepflichten.

10.1.3. P9S – Richtlinie für Remote-Arbeit: Regelt die Nutzung von Unternehmenssystemen in externen oder häuslichen Arbeitsumgebungen.

10.1.4. P17S – Datenschutz- und Privatsphäre-Richtlinie: Legt Regeln für den Umgang mit personenbezogenen Daten fest, die sich mit der Überwachung der zulässigen Nutzung und Bring Your Own Device (BYOD) überschneiden.

10.1.5. P30S – Incident-Response-Richtlinie (P30): Regelt Verfahren zur Untersuchung und Reaktion auf Missbrauch oder Verstöße gegen die Bedingungen der zulässigen Nutzung.

11. Referenzstandards und Rahmenwerke

11.1. ISO/IEC 27001

11.1.1. Maßnahme 5.10 – Verlangt, dass Organisationen die zulässige Nutzung von Unternehmenswerten definieren und durchsetzen.

11.2. ISO/IEC 27002

11.2.1. Maßnahme 5.10 – Enthält Leitlinien zur zulässigen Nutzung von Systemen, einschließlich erlaubter und verbotener Verhaltensweisen.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Behandelt die Kontrolle der Systemnutzung, einschließlich privat genutzter Geräte.

11.3.2. AC-20 – Verlangt die Autorisierung und Überwachung externer Systeme.

11.3.3. AT-2 – Betont die Schulung von Benutzern zu Praktiken der zulässigen Nutzung.

11.4. EU GDPR

11.4.1. Artikel 5(1)(f) – Verlangt die Integrität und Vertraulichkeit personenbezogener Daten, die durch missbräuchliche Nutzung durch Benutzer beeinträchtigt werden können.

11.4.2. Artikel 32 – Verlangt die Umsetzung technischer und organisatorischer Maßnahmen zum Schutz von Systemen und Daten.

11.5. EU NIS2

11.5.1. Artikel 21(2)(b) – Verlangt angemessene Sicherheitsrichtlinien, einschließlich Regeln zur zulässigen Nutzung, um Cyberbedrohungen zu mindern.

11.6. EU DORA

11.6.1. Artikel 9 – Verlangt IKT-Risikomanagement-Richtlinien, die Nutzungskontrollen und Durchsetzungsmechanismen einschließen.

11.7. COBIT 2019

11.7.1. DSS05 – Sicherheitsdienste verwalten: Betont die richtlinienbasierte Kontrolle des Benutzerverhaltens.

11.7.2. BAI08 – Wissensmanagement verwalten: Behandelt das Bewusstsein für Richtlinienverantwortlichkeiten und die Schulung zur zulässigen Nutzung.