					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P36S					Dokumenttitel: **Richtlinie zu Social Media und externer Kommunikation**							
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**

Ausgerichtet an Normen und Vorschriften

Standard/Regulierung	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 5.1, 5.2, 6.1, 8	Führung, Risiken und operative Steuerung der externen Kommunikation
ISO/IEC 27002:2022	Maßnahmen 5.10, 5.11	Zulässige Nutzung und Informationssicherheit in der Kommunikation
NIST SP 800-53 Rev. 5	PL-4, AU-7, IR-6, AC-22	Verhaltensregeln, Audit, Vorfallmeldung sowie Steuerung öffentlich zugänglicher Inhalte und Zugriffe
DSGVO	Artikel 5, 32, 33	Datenschutzgrundsätze, Sicherheit und Meldung von Verletzungen des Schutzes personenbezogener Daten mit Auswirkungen auf die öffentliche Kommunikation
EU NIS2	Artikel 21(2)(e), 21(2)(f)	Richtlinien zur Systemnutzung und zum Risikomanagement in der Lieferkette sowie bei öffentlicher Kommunikation
EU DORA	Artikel 14(4)	Kommunikationspflichten nach Vorfällen

1. Zweck

1.1. Diese Richtlinie legt verbindliche Vorgaben für jede öffentlich sichtbare Kommunikation fest, einschließlich der Nutzung von Social Media, Presseanfragen und externen digitalen Inhalten, sofern dabei auf das Unternehmen, dessen Personal, Kunden, Systeme oder interne Abläufe Bezug genommen wird.

1.2. Die Richtlinie dient dem Schutz der Reputation des Unternehmens, der Einhaltung rechtlicher und regulatorischer Anforderungen sowie der Verringerung des Risikos von Datenabfluss, Falschinformationen oder Sicherheitsvorfällen.

1.3. Sie ermöglicht es Mitarbeitenden und Partnern, sich positiv und verantwortungsvoll an Online-Diskussionen zu beteiligen, ohne versehentliche Offenlegungen oder irreführende Darstellungen zu verursachen.

1.4. Die Richtlinie stärkt die Zertifizierungsfähigkeit des SME nach ISO/IEC 27001, indem sie die Steuerung von Informationen regelt, die der Öffentlichkeit oder externen Interessengruppen zugänglich gemacht werden.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für alle mit der Organisation verbundenen Personen, einschließlich:

2.1.1. Mitarbeitende und Auftragnehmer

2.1.2. Freiberufler, Berater und externe Lieferanten

2.1.3. Praktikanten oder Teilzeitkräfte, die an der Leistungserbringung für Kunden beteiligt sind oder Zugriff auf Systeme haben

2.2. Die Richtlinie gilt für alle Formen externer Kommunikation mit Bezug zur Organisation, einschließlich:

2.2.1. Social-Media-Beiträge (LinkedIn, Twitter/X, TikTok, Instagram, Facebook usw.)

2.2.2. Blogbeiträge, Online-Foren, Kundenbewertungen und Diskussionsverläufe

2.2.3. Vorträge und Auftritte (z. B. auf Konferenzen, in Webinaren oder Podcasts)

2.2.4. E-Mails oder Nachrichten an Journalisten, Regierungsvertreter oder Influencer

2.2.5. Öffentlich freigegebene Screenshots, Fotos oder Videos aus Arbeitsumgebungen

2.3. Die Richtlinie gilt auch dann, wenn diese Kommunikation erfolgt:

2.3.1. über persönliche Geräte oder Konten

2.3.2. außerhalb der regulären Arbeitszeiten

2.3.3. ohne böswillige Absicht; auch versehentliche oder beiläufige Äußerungen fallen in den Geltungsbereich, wenn sie sich auf das Unternehmen beziehen

3. Ziele

3.1. Schutz der Reputation: Vermeidung von Schäden am Unternehmensimage durch nicht autorisierte oder unangemessene öffentliche Kommunikation

3.2. Informationssicherheit: Vermeidung der unbeabsichtigten Offenlegung sensibler Daten, interner Systeme oder Kundendetails über Social Media oder öffentliche Kanäle

3.3. Rechtliche und regulatorische Compliance: Sicherstellung, dass alle öffentlichen Inhalte mit Bezug zum Unternehmen die einschlägigen Datenschutzanforderungen und Vorgaben zur geschäftlichen Kommunikation einhalten

3.4. Professionelles Verhalten: Förderung einer verantwortungsvollen Beteiligung an Online-Diskussionen und Medienkontakten, auch über persönliche Konten

3.5. Reaktionsfähigkeit bei Vorfällen: Bereitstellung klarer, umsetzbarer Schritte für den Fall versehentlicher Offenlegungen oder Richtlinienverstöße

4. Rollen und Verantwortlichkeiten

4.1. General Manager (GM)

4.1.1. ist Eigentümer dieser Richtlinie und genehmigt sie

4.1.2. prüft und autorisiert alle öffentlich sichtbaren Stellungnahmen, Pressekontakte oder Medieninterviews

4.1.3. stellt sicher, dass diese Richtlinie allen Mitarbeitenden und Dritten eindeutig kommuniziert wird

4.1.4. untersucht Verstöße gegen diese Richtlinie und reagiert darauf in Übereinstimmung mit den Verfahren des Incident-Response-Frameworks

4.2. Benannter Mitarbeiter oder Kommunikationsverantwortlicher (falls benannt)

4.2.1. unterstützt den GM bei der Prüfung von Inhalten vor der externen Veröffentlichung (z. B. Blogbeiträge, Vortragsthemen)

4.2.2. führt Nachweise über genehmigte Medienaktivitäten oder risikobehaftete Social-Media-Beiträge

4.2.3. überwacht, soweit es die verfügbaren Kapazitäten zulassen, bekannte Online-Erwähnungen des Unternehmens auf Reputations- oder Sicherheitsrisiken

[... 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 ist mindestens einmal jährlich durch den General Manager (GM) zu überprüfen

9.1.2. Die Überprüfung muss die Ausrichtung an aktualisierten rechtlichen Verpflichtungen, Trends in der Branchenkommunikation und internen geschäftlichen Veränderungen sicherstellen

9.2. Anlassbezogene Überprüfungen

9.2.1. Diese Richtlinie ist unverzüglich zu aktualisieren nach:

9.2.1.1. einem erheblichen Social-Media-Vorfall oder Reputationsproblem

9.2.1.2. einer Änderung bei Drittparteien, die Kommunikationsaufgaben wahrnehmen

9.2.1.3. neuer Gesetzgebung oder neuen regulatorischen Verpflichtungen in Bezug auf Online-Kommunikation, Medien oder Markenauftritt

9.3. Dokumentation von Änderungen

9.3.1. Alle Aktualisierungen müssen dokumentiert werden, einschließlich Datum der Überarbeitung, Zusammenfassung der Änderungen und Genehmigung durch den GM

9.3.2. Für Audit- und Zertifizierungszwecke ist eine Versionshistorie zu führen

9.4. Verteilung von Aktualisierungen

9.4.1. Das gesamte Personal und alle Auftragnehmer müssen über Änderungen dieser Richtlinie informiert werden

9.4.2. Aktualisierte Fassungen müssen per E-Mail oder über interne Portale bereitgestellt werden

9.4.3. Jeder Lieferant für öffentliche Kommunikation muss aktualisierte Bedingungen bestätigen, bevor die Arbeit fortgesetzt wird

10. Zugehörige Richtlinien und Verknüpfungen

10.1. Diese Richtlinie wird in Abstimmung mit den folgenden SME-Richtlinien angewendet:

10.1.1. P3S – Richtlinie zur zulässigen Nutzung: Definiert zulässiges Verhalten bei der Nutzung von Kommunikationsplattformen, einschließlich des Zugriffs auf Social Media während der Arbeitszeit

10.1.2. P8S – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Stellt sicher, dass Mitarbeitende darin geschult sind, Risiken durch übermäßiges Teilen von Informationen, Phishing oder Reputationsbedrohungen im Internet zu erkennen

10.1.3. P17S – Richtlinie zu Datenschutz und Privatsphäre: Stellt sicher, dass personenbezogene Daten und Kundendaten nicht in externer Kommunikation geteilt werden, im Einklang mit der DSGVO und anderen rechtlichen Anforderungen

10.1.4. P30S – Incident-Response-Richtlinie: Regelt die Reaktion auf versehentliche öffentliche Offenlegung, Online-Bedrohungen oder Reputationsangriffe infolge missbräuchlicher Nutzung von Social Media

10.1.5. P37S – Richtlinie zur rechtlichen und regulatorischen Compliance: Legt die übergeordneten rechtlichen und vertraglichen Verpflichtungen der Organisation bei der öffentlichen Weitergabe von Inhalten fest

10.2. Diese Richtlinien müssen gemeinsam angewendet werden, um eine sichere, respektvolle und rechtskonforme externe Präsenz sicherzustellen.

11. Referenzstandards und Rahmenwerke

11.1. ISO/IEC 27001

11.1.1. Klausel 5.1 – Führung und Verpflichtung: verlangt die Aufsicht der Leitung über Reputations- und Informationsrisiken

11.1.2. Klausel 6.1 – Risikomanagement: umfasst kommunikationsbezogene Risikoexponierungen

11.1.3. Klausel 8.1 – Operative Steuerung: umfasst Vorgaben dazu, wie Informationen extern kommuniziert werden

11.2. ISO/IEC 27002

11.2.1. Maßnahme 5.10 – Zulässige Nutzung von Informationen und Werten

11.2.2. Maßnahme 5.11 – Informationssicherheit in der Kommunikation

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Verhaltensregeln: regelt angemessenes Verhalten bei der Nutzung von Informationsressourcen

11.3.2. AU-7 – Audit-Reduzierung und Berichtserstellung: unterstützt die Überwachung der öffentlichen Nutzung von Systemen

11.3.3. IR-6 – Vorfallmeldung: verlangt die Reaktion auf Reputations- und Kommunikationsverstöße

11.3.4. AC-22 – Öffentlich zugängliche Inhalte: stellt die Steuerung externer Veröffentlichungen und Zugriffe sicher

11.4. DSGVO (2016/679)

11.4.1. Artikel 5 – Grundsätze für die Verarbeitung personenbezogener Daten (Richtigkeit, Integrität, Rechenschaftspflicht)

11.4.2. Artikel 32 – Sicherheit der Verarbeitung: verlangt Schutzmaßnahmen für die öffentliche Weitergabe

11.4.3. Artikel 33 – Meldung von Verletzungen des Schutzes personenbezogener Daten: wird ausgelöst, wenn personenbezogene Daten über externe Kommunikation offengelegt werden

11.5. EU NIS2-Richtlinie (2022/2555)

11.5.1. Artikel 21(2)(e) – Richtlinien zur Nutzung von Informationssystemen, einschließlich Kommunikationsplattformen

11.5.2. Artikel 21(2)(f) – Richtlinien zum Umgang mit Cybersicherheitsrisiken in der Lieferkette und auf öffentlichen Plattformen

11.6. EU DORA (2022/2554)

11.6.1. Artikel 14(4) – Kommunikationspflichten gegenüber Kunden, Drittparteien und Behörden nach operativen Vorfällen

11.7. COBIT 2019

11.7.1. APO09 – Servicevereinbarungen verwalten: umfasst die Aufsicht über Lieferanten und kommunikationsbezogene Drittparteien

11.7.2. DSS05 – Sicherheitsdienste verwalten: umfasst den Schutz öffentlich sichtbarer digitaler Werte

11.7.3. EDM03 – Risikooptimierung sicherstellen: betont den Umgang mit Reputations- und Compliance-Risiken im Zusammenhang mit Kommunikation