					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P36S					Dokumenttitel: **Richtlinie für soziale Medien und externe 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 Standards und Vorschriften

Standard/Regelwerk	Abschnitt/Artikel	Kommentar
ISO/IEC 27001:2022	Abschnitt 8	Definierte Prozesse und rollenbasierte Governance für die Steuerung öffentlicher Kommunikation; Sicherstellung von Genauigkeit, Genehmigungsworkflows und Eskalation von Vorfällen.
ISO/IEC 27002:2022	Maßnahmen 5.10, 5.11, 5.35, 5.36	Regelt die Nutzung, die zulässige Nutzung sowie die externe Kontaktaufnahme und Kommunikation mit Behörden sowie die Berichterstattung zur Einhaltung.
NIST SP 800-53 Rev. 5	AC-8, AU-12, PL-4	Verhaltensregeln für die Nutzung von Systemen und Kommunikationsmitteln, Benutzerhinweise, Aufbewahrung von Audit-Protokollen.
DSGVO	Artikel 5, 25, 32, 33	Grundsätze der Datenverarbeitung, Datenschutz durch Technikgestaltung, Sicherheit der Verarbeitung, Pflichten zur Meldung von Datenschutzverletzungen.
EU NIS2	Artikel 21	Maßnahmen zum Management von Cybersicherheitsrisiken, Pflichten bei Vorfällen und risikobezogener öffentlicher Kommunikation.
EU DORA	Artikel 9, 16	IKT-Risikomanagement und Kommunikationsstrategie für kritische Anbieter.
COBIT 2019	APO09, DSS05	Governance von Servicevereinbarungen und Kommunikation sowie sichere Kommunikationspraktiken und Vorfallmanagement.

1. Zweck

1.1 Diese Richtlinie legt verbindliche Regeln und Verantwortlichkeiten für die Nutzung sozialer Medien und aller Formen externer Kommunikation durch mit der Organisation verbundene Personen fest.

1.2 Sie stellt sicher, dass öffentliche Kommunikation – unabhängig davon, ob geplant oder spontan – korrekt, respektvoll, sicher, rechtskonform und mit dem Markenauftritt der Organisation konsistent ist.

1.3 Diese Richtlinie zielt darauf ab, Risiken im Zusammenhang mit Reputationsschäden, regulatorischen Verstößen, dem Abfluss geistigen Eigentums und unbefugten Offenlegungen über öffentlich zugängliche Kanäle zu minimieren.

1.4 Darüber hinaus fördert sie Rechenschaftspflicht und eine strukturierte Governance für alle Formen digitaler Kommunikation, die die Organisation betreffen oder sich auf sie auswirken.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer, Praktikanten und Vertreter Dritter, die:

2.1.1 im Namen der Organisation kommunizieren, unabhängig davon, ob offiziell oder informell,

2.1.2 in einem öffentlichen Kontext auf eine Zugehörigkeit zur Organisation Bezug nehmen oder diese implizieren,

2.1.3 persönliche oder unternehmensbezogene Konten nutzen, um sich an öffentlichen Diskussionen mit Bezug zur Organisation zu beteiligen.

2.2 Zu den von dieser Richtlinie erfassten Kommunikationskanälen gehören insbesondere:

2.2.1 Social-Media-Plattformen (z. B. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook),

2.2.2 Blogs, Wikis, Foren und öffentliche Diskussionsplattformen,

2.2.3 E-Mail oder Direktnachrichten an externe Parteien (z. B. Kunden, Aufsichtsbehörden, Medien),

2.2.4 Presseinterviews, Vorträge in Podiumsdiskussionen oder aufgezeichnete Medienauftritte,

2.2.5 die Teilnahme an Online-Communitys, in denen auf die Organisation Bezug genommen wird.

2.3 Diese Richtlinie regelt sowohl Echtzeitinhalte als auch vorab geplante Inhalte und gilt für alle Geräte und Konten (persönlich oder unternehmensbezogen), die zur Verbreitung der Kommunikation verwendet werden.

3. Ziele

3.1 Verhinderung der versehentlichen oder vorsätzlichen Offenlegung vertraulicher, sensibler oder regulierter Informationen über externe Kommunikationskanäle.

3.2 Sicherstellung, dass offizielle öffentliche Erklärungen und Inhalte in sozialen Medien korrekt, autorisiert und mit dem Markenauftritt, den ethischen Grundsätzen und der strategischen Kommunikation des Unternehmens abgestimmt sind.

3.3 Verhinderung von Reputationsschäden und Sicherstellung einer konsistenten Kommunikation über interne Abteilungen und externe Plattformen hinweg.

3.4 Einhaltung der anwendbaren rechtlichen Verpflichtungen im Zusammenhang mit öffentlichen Erklärungen, insbesondere nach DSGVO, NIS2, DORA und sektorspezifischen Kommunikationsvorgaben.

3.5 Festlegung klarer Verantwortlichkeiten, zulässiger Anwendungsfälle und Durchsetzungsprotokolle für sämtliches Personal mit öffentlichkeitswirksamen Tätigkeiten.

4. Rollen und Verantwortlichkeiten

4.1 Chief Marketing Officer oder Leitung Kommunikation / PR-Leitung

4.1.1 genehmigt alle offiziellen Unternehmensbotschaften zur externen Veröffentlichung,

4.1.2 pflegt Redaktionspläne für Social-Media-Inhalte und Vorgaben zur Sicherstellung der Markenkonsistenz,

4.1.3 überwacht Online-Erwähnungen und Medienpräsenz im Zusammenhang mit der Organisation.

4.2 Chief Information Security Officer (CISO) / Informationssicherheitsteam

4.2.1 überwacht digitale Plattformen auf Indikatoren für Datenabfluss, Identitätsmissbrauch oder Phishing-Versuche,

4.2.2 koordiniert sich im Fall von Social-Media-basierten Angriffen oder Verstößen mit den Incident-Response-Teams.

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

9. Durchsetzung und Einhaltung

9.1 Diese Richtlinie ist für sämtliches erfasstes Personal und alle Dritten verbindlich. Die Nichteinhaltung kann folgende Maßnahmen nach sich ziehen:

9.1.1 formelle Verwarnungen,

9.1.2 vorübergehenden oder dauerhaften Entzug von Zugriffsrechten auf Plattformen oder Systeme,

9.1.3 disziplinarische Maßnahmen bis hin zur Beendigung des Beschäftigungsverhältnisses,

9.1.4 gerichtliche Schritte, wenn externe Kommunikation zu Reputationsschäden, einer Datenschutzverletzung oder regulatorischer Nichteinhaltung führt.

9.2 Disziplinarmaßnahmen

9.2.1 Interne Verstöße (z. B. Offenlegung vertraulicher Daten, Verleumdung der Organisation) führen zur Einbindung von HR, zu einer formellen Untersuchung und zur Dokumentation in der Personalakte.

9.2.2 Soweit anwendbar, verfolgt die Rechtsabteilung zivilrechtliche Rechtsbehelfe oder informiert Behörden über strafrechtlich relevante Handlungen (z. B. Identitätsanmaßung, Leaks zu Insiderhandel).

9.3 Überwachung der Einhaltung

9.3.1 Die Teams für Informationssicherheit und Kommunikation müssen eine fortlaufende Überwachung durchführen von:

9.3.1.1 Markenerwähnungen auf den wichtigsten Plattformen,

9.3.1.2 inoffizieller Nutzung von Unternehmensbildern oder Marken,

9.3.1.3 bekannten Risiken (z. B. unzufriedene Mitarbeiter, Versuche der Identitätsanmaßung).

9.3.2 Die Überwachung muss im Einklang mit arbeits- und datenschutzrechtlichen Vorgaben erfolgen; alle gekennzeichneten Fälle sind durch eine prüfende Person zu verifizieren.

9.4 Hinweisgebermeldungen und Meldung von Missbrauch

9.4.1 Jeder Mitarbeiter, der einen Verstoß gegen diese Richtlinie vermutet, wird aufgefordert, diesen dem Team für Informationssicherheit, der Rechtsabteilung oder anonym über das Hinweisgeberportal zu melden.

9.4.2 Benachteiligungen gegenüber Hinweisgebern sind strikt untersagt und führen zu unverzüglichen disziplinarischen Maßnahmen.

10. Anforderungen an Überprüfung und Aktualisierung

10.1 Diese Richtlinie muss jährlich oder früher überprüft werden, wenn:

10.1.1 sich regulatorische Anforderungen wesentlich ändern (z. B. neue EU-Vorschriften für digitale Kommunikation),

10.1.2 neue soziale Plattformen oder Kommunikationskanäle eingeführt werden,

10.1.3 ein wesentlicher Vorfall oder wiederholte Verstöße auf Prozesslücken hinweisen,

10.1.4 sich Struktur oder Führung in den Funktionen PR, Recht oder Informationssicherheit wesentlich ändern.

10.2 Die Überprüfung muss gemeinsam durchgeführt werden durch:

10.2.1 die Leitung Marketing / PR,

10.2.2 den CISO oder die Leitung Security Risk,

10.2.3 die Verantwortlichen für Recht und Compliance.

10.3 Aktualisierungen müssen im Register für Richtlinienänderungen dokumentiert und über interne Sensibilisierungskanäle kommuniziert werden. Bei wesentlichen Änderungen müssen alle betroffenen Personen die Richtlinienbestätigung erneut abgeben.

11. Zugehörige Richtlinien und Verknüpfungen

11.1 Diese Richtlinie wird durch folgende Komponenten des Informationssicherheits-Managementsystems (ISMS) der Organisation unterstützt und steht mit ihnen in Zusammenhang:

11.1.1 P1 – Informationssicherheitsrichtlinie: Legt übergeordnete Grundsätze zum Schutz von Informationen fest; hierzu gehört auch sicherzustellen, dass Kommunikation nicht zu unbefugter Offenlegung führt.

11.1.2 P3 – Richtlinie zur zulässigen Nutzung: Definiert zulässige Verhaltensweisen für digitale Plattformen und Technologien und regelt damit unmittelbar die persönliche und berufliche Nutzung sozialer Kanäle.

11.1.3 P6 – Risikomanagement-Richtlinie: Stellt den Risikorahmen für die Bewertung von Bedrohungen im Zusammenhang mit öffentlicher Kommunikation und Reputationsrisiken bereit.

11.1.4 P8 – Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Verlangt Sensibilisierungsprogramme, die Mitarbeitende in sicheren Kommunikationspraktiken und zu Social-Engineering-Bedrohungen schulen.

11.1.5 P13 – Richtlinie zur Datenklassifizierung und Kennzeichnung: Leitet das Personal dabei an, was als streng vertraulich oder vertrauliche Information einzustufen ist und extern nicht offengelegt werden darf.

11.1.6 P30 – Incident-Response-Richtlinie: Definiert den Umgang mit vorfallsbezogenen Sachverhalten im Zusammenhang mit öffentlicher Kommunikation, einschließlich Datenabfluss, Identitätsanmaßung und regulatorischen Verstößen.

11.1.7 P33 – Richtlinie zur Audit- und Compliance-Überwachung: Regelt die Auditprozesse, mit denen Social-Media-Kontrollen, Überwachungssysteme und die Einhaltung der Richtlinie zur externen Kommunikation validiert werden.

12. Referenzstandards und Rahmenwerke

12.1 ISO/IEC 27001:

12.1.1 Abschnitt 8.1 – Operative Planung und Steuerung: Verlangt definierte Prozesse und rollenbasierte Governance für die Steuerung öffentlicher Kommunikation, einschließlich Genauigkeit, Genehmigungsworkflows und Eskalation von Vorfällen mit Daten- oder Reputationsrisiko.

12.2 ISO/IEC 27002:2022:

12.2.1 Maßnahme 5.10 – Nutzung von Informationen: Regelt die autorisierte und ethisch angemessene Verbreitung interner oder externer Kommunikation.

12.2.2 Maßnahme 5.11 – Zulässige Nutzung von Unternehmenswerten: Verstärkt zulässige Praktiken für das Teilen von Inhalten unter Verwendung von Unternehmens-IKT-Assets oder persönlicher Konten.

12.2.3 Maßnahme 5.35 – Kontakt mit Behörden: Verlangt strukturierte und autorisierte externe Kommunikation mit Aufsichtsbehörden und öffentlichen Stellen.

12.2.4 Maßnahme 5.36 – Einhaltung von Richtlinien und Standards: Erzwingt die konsistente Anwendung interner Richtlinien in allen Kommunikationsszenarien.

12.3 NIST SP 800-53 Rev. 5:

12.3.1 PL-4 – Verhaltensregeln: Verlangt formelle Regeln für die Nutzung von Systemen und Kommunikationsmitteln, einschließlich Standards für öffentliche Offenlegungen.

12.3.2 AC-8 – Hinweis zur Systemnutzung: Unterstützt verpflichtende Haftungsausschlüsse und Inhaltswarnungen auf extern ausgerichteten Plattformen.

12.3.3 AU-12 – Aufbewahrung von Audit-Protokollen: Gilt für die Aufbewahrung von Protokollen und Kommunikationshistorien für Vorfallsprüfungen und Audit-Zwecke.

12.4 DSGVO (2016/679):

12.4.1 Artikel 5 – Grundsätze der Datenverarbeitung: Untersagt die unbefugte Weitergabe personenbezogener Daten über öffentliche Kommunikation.

12.4.2 Artikel 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen: Verlangt Datenschutzvorkehrungen in Kommunikationswerkzeugen und Inhalts-Workflows.

12.4.3 Artikel 32 – Sicherheit der Verarbeitung: Umfasst Verschlüsselung, Zugriffskontrolle und Prozesse zur Inhaltsfreigabe.

12.4.4 Artikel 33 – Meldung von Verletzungen des Schutzes personenbezogener Daten: Verlangt die rechtzeitige Offenlegung von Abflüssen personenbezogener Daten über öffentliche Kanäle.

12.5 NIS2-Richtlinie der EU (2022/2555):

12.5.1 Artikel 21 – Maßnahmen zum Management von Cybersicherheitsrisiken: Umfasst Kommunikationsprotokolle und Verpflichtungen bei Vorfällen sowie öffentlicher risikobezogener Kommunikation.

12.6 EU DORA (2022/2554):

12.6.1 Artikel 9 – IKT-Risikomanagement: Gilt für extern ausgelöste Kommunikationsrisiken wie Identitätsanmaßung, Fehlinformationen und reputationsbezogene Störungen.

12.6.2 Artikel 16 – Kommunikationsstrategie: Verlangt, dass kritische Finanzunternehmen oder Dienstleister Kommunikationsrisiken und Reaktionen in Krisenszenarien steuern.

12.7 COBIT 2019:

12.7.1 APO09 – Managed Service Agreements and Communication: Verlangt strukturierte Governance für interne und externe Kommunikation.

12.7.2 DSS05 – Sicherheitsdienste verwalten: Stellt sicher, dass Kommunikationsaktivitäten keine zusätzlichen Risiken einführen oder Verfahren zum Umgang mit Informationssicherheitsvorfällen beeinträchtigen.