					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P36S					Název dokumentu: **Politika sociálních médií a externí komunikace**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma / právní předpis	Kapitola / článek	Komentář
ISO/IEC 27001:2022	Kapitola 8	Definované procesy a řízení založené na rolích pro správu veřejné komunikace, zajištění přesnosti, schvalovací workflow a eskalaci incidentů.
ISO/IEC 27002:2022	Opatření 5.10, 5.11, 5.35, 5.36	Upravuje používání informací, přípustné užívání a externí komunikaci s orgány veřejné moci a prokazování souladu.
NIST SP 800-53 Rev.5	AC-8, AU-12, PL-4	Pravidla pro používání systémů a komunikačních prostředků, upozornění pro uživatele a uchovávání auditních záznamů.
GDPR EU	Články 5, 25, 32, 33	Zásady zpracování osobních údajů, ochrana osobních údajů již od návrhu, zabezpečení zpracování a požadavky na oznamování porušení zabezpečení osobních údajů.
směrnice NIS2	Článek 21	Opatření pro řízení rizik v oblasti ICT a povinnosti při incidentech a veřejné komunikaci související s riziky.
nařízení DORA	Články 9, 16	Řízení rizik v oblasti ICT a komunikační strategie pro kritické poskytovatele.
COBIT 2019	APO09, DSS05	Řízení dohod o úrovni služeb (SLA), komunikace a bezpečné komunikační postupy / zvládání incidentů.

1. Účel

1.1 Tato politika stanoví závazná pravidla a odpovědnosti pro používání sociálních médií a všech forem externí komunikace personálem spojeným s organizací.

1.2 Zajišťuje, aby veřejná sdělení, plánovaná i spontánní, byla přesná, respektující, bezpečná, v souladu s právními předpisy a konzistentní se značkou organizace.

1.3 Cílem této politiky je minimalizovat rizika spojená s poškozením dobré pověsti, porušením regulačních požadavků, únikem duševního vlastnictví a neoprávněným zveřejněním prostřednictvím veřejně dostupných kanálů.

1.4 Tato politika dále podporuje odpovědnost a strukturované řízení všech forem digitální komunikace, které se organizace týkají nebo ji ovlivňují.

2. Rozsah

2.1 Tato politika se vztahuje na všechny zaměstnance, smluvní pracovníky, stážisty a zástupce třetích stran, kteří:

2.1.1 komunikují jménem organizace, ať již oficiálně, nebo neformálně,

2.1.2 veřejně odkazují na své spojení s organizací nebo je naznačují,

2.1.3 používají osobní nebo firemní účty k účasti na veřejných diskusích týkajících se organizace.

2.2 Mezi komunikační kanály spadající do působnosti této politiky patří mimo jiné:

2.2.1 platformy sociálních médií (např. LinkedIn, X/Twitter, Instagram, TikTok, YouTube, Facebook),

2.2.2 blogy, wiki, fóra a veřejné diskusní platformy,

2.2.3 e-mail nebo přímé zprávy externím stranám (např. klientům, regulačním orgánům, médiím),

2.2.4 rozhovory pro tisk, účast v panelových diskusích nebo vystoupení v nahrávaných médiích,

2.2.5 účast v online komunitách, v nichž je organizace zmiňována.

2.3 Tato politika upravuje obsah zveřejňovaný v reálném čase i obsah plánovaný předem a vztahuje se na všechna zařízení a účty (osobní i firemní), které jsou použity k šíření takové komunikace.

3. Cíle

3.1 Předcházet náhodnému nebo úmyslnému zveřejnění důvěrných, citlivých nebo regulovaných informací prostřednictvím externích komunikačních kanálů.

3.2 Zajistit, aby oficiální veřejná prohlášení a obsah na sociálních médiích byly přesné, autorizované a v souladu se značkou organizace, etickými zásadami a strategickou komunikací.

3.3 Předcházet poškození dobré pověsti a zajistit konzistentnost sdělení napříč interními útvary a externími platformami.

3.4 Plnit příslušné právní povinnosti vztahující se k veřejným prohlášením, včetně, nikoli však výlučně, GDPR, směrnice NIS2, nařízení DORA a pravidel komunikace specifických pro dané odvětví.

3.5 Vymezit jasné odpovědnosti, přípustné způsoby použití a postupy prosazování požadavků této politiky pro veškerý personál zapojený do činností orientovaných navenek.

4. Role a odpovědnosti

4.1 Ředitel marketingu nebo komunikace / vedoucí PR

4.1.1 schvaluje veškerá oficiální sdělení organizace určená k externímu zveřejnění,

4.1.2 spravuje obsahové kalendáře pro sociální média a pravidla pro konzistentní prezentaci značky,

4.1.3 monitoruje online zmínky a mediální výstupy týkající se organizace.

4.2 Ředitel informační bezpečnosti (CISO) / bezpečnostní tým

4.2.1 monitoruje digitální platformy z hlediska indikátorů úniku dat, vydávání se za jinou osobu nebo pokusů o phishing,

4.2.2 koordinuje postup s týmy reakce na incidenty v případě útoků nebo narušení souvisejících se sociálními médii.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Vymáhání a dodržování

9.1 Tato politika je závazná pro veškerý dotčený personál a třetí strany. Nedodržení může vést k:

9.1.1 formálním upozorněním,

9.1.2 dočasnému nebo trvalému odebrání přístupu k platformám nebo systémům,

9.1.3 disciplinárním opatřením, včetně ukončení pracovního poměru,

9.1.4 právním krokům, pokud externí komunikace vede k poškození dobré pověsti, porušení zabezpečení dat nebo regulačnímu nesouladu.

9.2 Disciplinární opatření

9.2.1 Interní porušení (např. únik důvěrných dat, pomluva organizace) vyvolají zapojení HR, formální šetření a dokumentaci v osobním spisu zaměstnance.

9.2.2 Pokud je to relevantní, právní oddělení a compliance uplatní občanskoprávní nároky nebo informuje příslušné orgány o podezření na trestnou činnost (např. vydávání se za jinou osobu, úniky související s insider trading).

9.3 Monitorování souladu

9.3.1 Bezpečnostní a komunikační týmy musí průběžně monitorovat:

9.3.1.1 zmínky o značce na hlavních platformách,

9.3.1.2 neoficiální používání obrazových prvků organizace nebo ochranných známek,

9.3.1.3 známá rizika (např. nespokojení zaměstnanci, pokusy o vydávání se za jinou osobu).

9.3.2 Monitorování musí být v souladu s právními předpisy a požadavky na ochranu soukromí zaměstnanců a všechny označené případy musí být ověřeny lidským posouzením.

9.4 Oznamovací mechanismus a hlášení zneužití

9.4.1 Každý zaměstnanec, který má podezření na porušení této politiky, je povinen je nahlásit týmu informační bezpečnosti, právnímu oddělení a compliance nebo anonymně prostřednictvím oznamovacího portálu.

9.4.2 Jakákoli odveta vůči oznamovatelům je přísně zakázána a bude předmětem okamžitého disciplinárního opatření.

10. Požadavky na přezkoumávání a aktualizaci

10.1 Tato politika musí být přezkoumána každoročně nebo dříve, pokud:

10.1.1 dojde k významným změnám regulačních požadavků (např. nové právní předpisy EU v oblasti digitální komunikace),

10.1.2 jsou zavedeny nové sociální platformy nebo komunikační kanály,

10.1.3 dojde k významnému incidentu nebo opakovaným porušením, která naznačují nedostatky v procesech,

10.1.4 dojde ke strukturální změně nebo změně vedení ve funkcích PR, právního oddělení a compliance nebo bezpečnosti.

10.2 Přezkum musí společně provést:

10.2.1 vedoucí marketingu / PR,

10.2.2 CISO nebo vedoucí řízení bezpečnostních rizik,

10.2.3 zástupci právního oddělení a compliance.

10.3 Aktualizace musí být zdokumentovány v registru změn politik a komunikovány prostřednictvím interních kanálů na podporu povědomí. Pokud dojde k podstatným změnám, musí veškerý dotčený personál znovu potvrdit seznámení s politikou.

11. Související politiky a vazby

11.1 Tato politika je podporována a souvisí s následujícími součástmi systému řízení bezpečnosti informací (ISMS) organizace:

11.1.1 P1 – Politika informační bezpečnosti: stanoví zastřešující zásady pro ochranu informací, včetně zajištění, aby komunikace nevedla k neoprávněnému zveřejnění.

11.1.2 P3 – Zásady přípustného užívání: vymezují přípustné chování při používání digitálních platforem a technologií, což přímo upravuje osobní i profesní využívání sociálních kanálů.

11.1.3 P6 – Politika řízení rizik: poskytuje rámec pro hodnocení rizik souvisejících s veřejnou komunikací a reputační expozicí.

11.1.4 P8 – Politika bezpečnostního povědomí a školení: stanoví programy povědomí, které vzdělávají pracovníky v oblasti bezpečných komunikačních postupů a hrozeb sociálního inženýrství.

11.1.5 P13 – Politika klasifikace dat a označování: poskytuje personálu vodítka, co představuje omezené nebo důvěrné informace, které nesmí být zveřejněny externě.

11.1.6 P30 – Politika reakce na incidenty: stanoví, jak zvládat incidenty související s veřejnou komunikací, včetně úniků dat, vydávání se za jinou osobu a porušení regulačních požadavků.

11.1.7 P33 – Politika monitorování auditu a souladu: upravuje auditní procesy, které ověřují kontroly sociálních médií, monitorovací systémy a soulad s politikami externí komunikace.

12. Referenční normy a rámce

12.1 ISO/IEC 27001:

12.1.1 Kapitola 8.1 – Operativní plánování a řízení: vyžaduje definované procesy a řízení založené na rolích pro správu veřejné komunikace, zajištění přesnosti, schvalovací workflow a eskalaci incidentů souvisejících s daty nebo reputačním rizikem.

12.2 ISO/IEC 27002:2022:

12.2.1 Opatření 5.10 – Používání informací: upravuje autorizované a etické šíření interní nebo externí komunikace.

12.2.2 Opatření 5.11 – Přípustné užívání informací a aktiv: posiluje přípustné postupy pro sdílení obsahu s využitím firemního majetku nebo osobních účtů.

12.2.3 Opatření 5.35 – Kontakt s orgány veřejné moci: vyžaduje strukturovanou a autorizovanou externí komunikaci s regulačními orgány a veřejnými institucemi.

12.2.4 Opatření 5.36 – Soulad s politikami a normami: vyžaduje konzistentní uplatňování interních politik ve všech komunikačních situacích.

12.3 NIST SP 800-53 Rev.5:

12.3.1 PL-4 – Pravidla chování: vyžaduje formální pravidla pro používání systémů a komunikačních prostředků, včetně standardů pro veřejné zveřejňování.

12.3.2 AC-8 – Oznámení o používání systému: podporuje povinná prohlášení a obsahová upozornění na platformách orientovaných navenek.

12.3.3 AU-12 – Uchovávání auditních záznamů: vztahuje se na uchovávání logů a historie komunikace pro účely přezkoumání incidentů a auditu.

12.4 GDPR (2016/679):

12.4.1 Článek 5 – Zásady zpracování osobních údajů: zakazuje neoprávněné sdílení osobních údajů prostřednictvím veřejné komunikace.

12.4.2 Článek 25 – Ochrana osobních údajů již od návrhu a ve výchozím nastavení: vyžaduje opatření na ochranu soukromí v komunikačních nástrojích a postupech práce s obsahem.

12.4.3 Článek 32 – Zabezpečení zpracování: vyžaduje šifrování, řízení přístupu a procesy schvalování obsahu.

12.4.4 Článek 33 – Oznámení porušení zabezpečení: ukládá včasné oznámení úniků osobních údajů prostřednictvím veřejných kanálů.

12.5 směrnice NIS2 (2022/2555):

12.5.1 Článek 21 – Opatření pro řízení kybernetických rizik: zahrnuje komunikační protokoly a povinnosti během incidentů a veřejné komunikace o rizicích.

12.6 nařízení DORA (2022/2554):

12.6.1 Článek 9 – Řízení rizik v oblasti ICT: vztahuje se na komunikační rizika vyvolaná externě, jako je vydávání se za jinou osobu, dezinformace a narušení dobré pověsti.

12.6.2 Článek 16 – Komunikační strategie: vyžaduje, aby kritičtí poskytovatelé finančních nebo servisních služeb řídili komunikační rizika a reakce v krizových scénářích.

12.7 COBIT 2019:

12.7.1 APO09 – Řízení dohod o poskytování služeb a komunikace: vyžaduje strukturované řízení interní i externí komunikace.

12.7.2 DSS05 – Řízení bezpečnostních služeb: zajišťuje, aby komunikační činnosti nezaváděly dodatečné riziko ani nenarušovaly procesy zvládání incidentů.