					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	Kapitoly 5.1, 5.2, 6.1, 8	Vedení, řízení rizik a operativní řízení externí komunikace
ISO/IEC 27002:2022	Opatření 5.10, 5.11	Přípustné užívání a bezpečnost informací v komunikaci
NIST SP 800-53 Rev.5	PL-4, AU-7, IR-6, AC-22	Pravidla chování, audit, hlášení incidentů a řízení veřejně přístupného obsahu a přístupu
GDPR	Články 5, 32, 33	Zásady ochrany osobních údajů, zabezpečení a oznamování porušení zabezpečení s dopadem na veřejnou komunikaci
směrnice NIS2	Článek 21(2)(e), 21(2)(f)	Politiky pro užívání systémů a řízení rizik v dodavatelském řetězci a ve veřejné komunikaci
nařízení DORA	Článek 14(4)	Komunikační povinnosti po incidentech

1. Účel

1.1. Tato politika stanoví závazná pravidla pro veškerou veřejně dostupnou komunikaci, včetně používání sociálních médií, komunikace s tiskem a externího digitálního obsahu, pokud se vztahuje ke společnosti, jejím pracovníkům, klientům, systémům nebo interním postupům.

1.2. Tato politika pomáhá chránit dobrou pověst společnosti, zajišťovat soulad s právními a regulačními požadavky a snižovat riziko úniku informací, šíření nepravdivých informací nebo bezpečnostních incidentů.

1.3. Umožňuje zaměstnancům, smluvním pracovníkům a partnerům zapojovat se do online diskusí pozitivně a odpovědně a současně předcházet neúmyslnému zpřístupnění informací nebo zkreslené prezentaci skutečností.

1.4. Tato politika podporuje připravenost SME na certifikaci ISO/IEC 27001 tím, že upravuje řízení informací zpřístupňovaných veřejnosti nebo externím zainteresovaným stranám.

2. Rozsah

2.1. Tato politika se vztahuje na všechny osoby spojené s organizací, zejména na:

2.1.1. zaměstnance a smluvní pracovníky,

2.1.2. externí spolupracovníky na volné noze, konzultanty a dodavatele třetích stran,

2.1.3. stážisty nebo pracovníky na částečný úvazek zapojené do poskytování služeb klientům nebo s přístupem k systémům.

2.2. Tato politika se vztahuje na všechny formy externí komunikace odkazující na organizaci, zejména:

2.2.1. příspěvky na sociálních sítích (LinkedIn, Twitter/X, TikTok, Instagram, Facebook apod.),

2.2.2. blogové příspěvky, online fóra, zákaznické recenze a diskusní vlákna,

2.2.3. veřejná vystoupení (např. konference, webináře, podcasty),

2.2.4. e-maily nebo zprávy novinářům, zástupcům veřejné správy nebo influencerům,

2.2.5. veřejně sdílené snímky obrazovky, fotografie nebo videa z pracovního prostředí.

2.3. Tato politika se použije i tehdy, pokud je taková komunikace uskutečněna:

2.3.1. ze soukromých zařízení nebo účtů,

2.3.2. mimo běžnou pracovní dobu,

2.3.3. bez zlého úmyslu — do rozsahu této politiky spadají i neúmyslná nebo mimochodem pronesená vyjádření, pokud odkazují na společnost.

3. Cíle

3.1. Ochrana dobré pověsti: předcházet poškození image společnosti v důsledku neoprávněné nebo nevhodné veřejné komunikace.

3.2. Bezpečnost dat: zabránit neúmyslnému zpřístupnění citlivých dat, interních systémů nebo údajů o klientech prostřednictvím sociálních médií nebo veřejných kanálů.

3.3. Soulad s právními a regulačními požadavky: zajistit, aby veškerý veřejný obsah odkazující na společnost byl v souladu s příslušnými právními předpisy v oblasti ochrany osobních údajů a obchodní komunikace.

3.4. Profesionální jednání: podporovat odpovědnou účast v online diskusích a komunikaci s médii, a to i při používání osobních účtů.

3.5. Připravenost na incidenty: stanovit jasné a proveditelné kroky pro případ neúmyslného zpřístupnění informací nebo porušení této politiky.

4. Role a odpovědnosti

4.1. generální ředitel (GM)

4.1.1. je vlastníkem této politiky a schvaluje ji,

4.1.2. přezkoumává a schvaluje veškerá veřejná vyjádření, komunikaci s tiskem a mediální rozhovory,

4.1.3. zajišťuje, aby tato politika byla srozumitelně komunikována všem zaměstnancům a třetím stranám,

4.1.4. vyšetřuje porušení této politiky a přijímá navazující opatření v koordinaci s postupy reakce na incidenty.

4.2. určený zaměstnanec nebo vedoucí komunikace (je-li určen)

4.2.1. podporuje GM při přezkumu obsahu před externím zveřejněním (např. blogových příspěvků nebo témat vystoupení),

4.2.2. vede záznamy o schválených mediálních aktivitách nebo vysoce rizikových příspěvcích na sociálních sítích,

4.2.3. v rozsahu dostupných kapacit sleduje známé online zmínky o společnosti z hlediska reputačních nebo bezpečnostních rizik.

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

9. Požadavky na přezkoumávání a aktualizaci

9.1. Roční přezkum

9.1.1. Tato politika musí být nejméně jednou ročně přezkoumána generálním ředitelem (GM).

9.1.2. Přezkum musí zajistit soulad s aktualizovanými právními povinnostmi, trendy v komunikaci v odvětví a interními obchodními změnami.

9.2. Přezkumy vyvolané událostí

9.2.1. Tato politika musí být bezodkladně aktualizována po:

9.2.1.1. významném incidentu na sociálních médiích nebo reputačním problému,

9.2.1.2. změně dodavatelů třetích stran zajišťujících komunikaci,

9.2.1.3. přijetí nové legislativy nebo nových regulačních povinností vztahujících se k online komunikaci, médiím nebo značce.

9.3. Dokumentace změn

9.3.1. Všechny aktualizace musí být zaznamenány, včetně data změny, shrnutí změn a schválení GM.

9.3.2. Pro účely auditu a certifikace musí být vedena historie verzí.

9.4. Distribuce aktualizací

9.4.1. Veškerý personál a smluvní pracovníci musí být informováni o všech změnách politiky.

9.4.2. Aktualizované verze musí být sdíleny prostřednictvím e-mailu nebo interních portálů.

9.4.3. Každý dodavatel zajišťující veřejnou komunikaci musí před pokračováním v činnosti potvrdit seznámení s aktualizovanými podmínkami.

10. Související politiky a vazby

10.1. Tato politika je uplatňována v koordinaci s následujícími politikami SME:

10.1.1. P3S – Zásady přípustného užívání: stanoví přípustné chování při používání komunikačních platforem, včetně přístupu k sociálním médiím během pracovní doby.

10.1.2. P8S – Politika povědomí o bezpečnosti informací a školení: zajišťuje, aby byli pracovníci školeni v rozpoznávání rizik nadměrného sdílení, phishingu nebo reputačních hrozeb v online prostředí.

10.1.3. P17S – Politika ochrany dat a soukromí: zajišťuje, aby osobní údaje a údaje zákazníků nebyly sdíleny v externí komunikaci, v souladu s GDPR a dalšími právními požadavky.

10.1.4. P30S – Politika reakce na incidenty: upravuje reakci na neúmyslné veřejné zpřístupnění informací, online hrozby nebo reputační útoky vzniklé v důsledku nesprávného používání sociálních médií.

10.1.5. P37S – Politika souladu s právními a regulačními požadavky: stanoví širší právní a smluvní povinnosti organizace při veřejném sdílení obsahu.

10.2. Tyto politiky musí být uplatňovány společně, aby byla zachována bezpečná, respektující a právně konformní externí prezentace organizace.

11. Referenční normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 5.1 – Vedení a závazek: vyžaduje dohled vedení nad reputačními a informačními riziky.

11.1.2. Kapitola 6.1 – Řízení rizik: zahrnuje rizikovou expozici související s komunikací.

11.1.3. Kapitola 8.1 – Operativní řízení: pokrývá pravidla pro externí komunikaci informací.

11.2. ISO/IEC 27002

11.2.1. Opatření 5.10 – Přípustné užívání informací a aktiv.

11.2.2. Opatření 5.11 – Bezpečnost informací v komunikaci.

11.3. NIST SP 800-53 Rev. 5

11.3.1. PL-4 – Pravidla chování: upravuje přiměřené chování při používání informačních zdrojů.

11.3.2. AU-7 – Redukce auditních záznamů a generování reportů: podporuje monitorování veřejného používání systémů.

11.3.3. IR-6 – Hlášení incidentů: vyžaduje reakci na reputační a komunikační incidenty.

11.3.4. AC-22 – Veřejně přístupný obsah: zajišťuje řízení externích publikací a přístupu k nim.

11.4. GDPR (EU 2016/679)

11.4.1. Článek 5 – Zásady zpracování osobních údajů (přesnost, integrita, odpovědnost).

11.4.2. Článek 32 – Zabezpečení zpracování: vyžaduje ochranná opatření při veřejném sdílení.

11.4.3. Článek 33 – Oznámení porušení zabezpečení: aktivuje se, pokud jsou osobní údaje zpřístupněny prostřednictvím externí komunikace.

11.5. směrnice NIS2 (2022/2555)

11.5.1. Článek 21(2)(e) – Politiky pro užívání informačních systémů, včetně komunikačních platforem.

11.5.2. Článek 21(2)(f) – Politiky pro řízení rizik kybernetické bezpečnosti v dodavatelském řetězci a na veřejných platformách.

11.6. nařízení DORA (2022/2554)

11.6.1. Článek 14(4) – Komunikační povinnosti vůči zákazníkům, třetím stranám a orgánům po provozních incidentech.

11.7. COBIT 2019

11.7.1. APO09 – Řízení dohod o úrovni služeb: pokrývá dohled nad dodavateli a třetími stranami souvisejícími s komunikací.

11.7.2. DSS05 – Řízení bezpečnostních služeb: zahrnuje ochranu veřejně dostupných digitálních aktiv.

11.7.3. EDM03 – Zajištění optimalizace rizik: zdůrazňuje řízení reputačních rizik a rizik souladu souvisejících s komunikací.