					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P03S					Název dokumentu: **Zásady přípustného používání**							
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 5	Relevantní pro celkový rozsah a zavedení této politiky
ISO/IEC 27002:2022	5.10, 5.11, 5	Poskytuje pokyny k požadavkům a opatřením pro přípustné používání
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Pokrývá používání systémů a zařízení, monitorování a školení uživatelů
GDPR	Články 5(1)(f), 32	Integrita a důvěrnost údajů a bezpečnostní opatření
směrnice NIS2	Článek 21(2)(b)	Ukládá zavedení odpovídajících bezpečnostních politik a pravidel přípustného používání
nařízení DORA	Článek 9	Politika řízení ICT rizik, kontroly a jejich uplatňování
COBIT 2019	DSS05, BAI08	Bezpečnostní služby a řízení znalostí

1. Účel

1.1. Tyto Zásady přípustného používání stanovují pravidla pro přípustné, odpovědné a bezpečné používání systémů, zařízení, přístupu k internetu, elektronické pošty, cloudových služeb a všech soukromých zařízení používaných pro pracovní účely.

1.2. Zajišťují, aby všechny dotčené osoby rozuměly svým povinnostem při používání IT zdrojů organizace a při ochraně integrity dat, soukromí a kontinuity provozu.

1.3. Tato politika podporuje soulad s ISO/IEC 27001:2022 tím, že stanoví jasná pravidla chování uživatelů v souladu s právními, smluvními a regulatorními požadavky.

2. Rozsah

2.1. Tato politika se vztahuje na všechny osoby, které přistupují k firemním systémům nebo datům, spravují je nebo s nimi jinak pracují, včetně:

2.1.1. zaměstnanců a smluvních pracovníků,

2.1.2. dočasných pracovníků a stážistů,

2.1.3. externích poskytovatelů IT služeb.

2.2. Tato politika se vztahuje na:

2.2.1. firemní počítače, telefony a tablety,

2.2.2. soukromá zařízení schválená pro pracovní použití v režimu BYOD,

2.2.3. firemní sítě, cloudové platformy a softwarové služby,

2.2.4. přístup k internetu, e-mailové systémy, sdílená úložiště a podnikové aplikace.

2.3. Tato politika platí ve všech pracovních režimech – na pracovišti, na dálku i v hybridním režimu – po celou dobu výkonu práce.

3. Cíle

3.1. Vymezit, co se považuje za přípustné a nepřípustné používání IT systémů.

3.1.1. Snížit bezpečnostní rizika vyplývající ze zneužití, neoprávněného přístupu nebo zavlečení malwaru.

3.1.2. Chránit obchodní data, informace o zákaznících a dobrou pověst společnosti.

3.1.3. Zavést vymahatelná pravidla a zajistit odpovědnost všech uživatelů.

3.1.4. Podpořit monitorování a soulad za účelem včasného odhalení porušení a přijetí nápravných opatření.

4. Role a odpovědnosti

4.1. Generální ředitel

4.1.1. Schvaluje tuto politiku a odpovídá za zajištění zdrojů a pravomocí nezbytných pro její uplatňování.

4.1.2. Přezkoumává a schvaluje veškeré výjimky z této politiky.

4.2. IT manažer nebo externí poskytovatel IT služeb

4.2.1. Vede seznam schváleného softwaru a hardwaru.

4.2.2. Konfiguruje zařízení tak, aby vynucovala pravidla přípustného používání (např. filtrování obsahu, auditní záznamy přístupů).

4.2.3. Monitoruje používání z hlediska možného porušení a vyšetřuje incidenty.

4.2.4. Zajišťuje, aby soukromá zařízení používaná pro pracovní účely v režimu BYOD byla schválena a bezpečně nakonfigurována.

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

9. Požadavky na přezkoumání a aktualizaci

9.1. Každoroční přezkum

9.1.1. Tato politika musí být každoročně přezkoumána IT manažerem a následně schválena generálním ředitelem, aby bylo zajištěno, že zůstává v souladu se způsoby používání technologií, nově vznikajícími riziky a požadavky na soulad.

9.2. Spouštěče průběžného přezkumu

9.2.1. Přezkum musí být proveden také v reakci na:

9.2.2. nové systémy nebo technologie (např. nová cloudová služba nebo platforma koncových zařízení),

9.2.3. závažná porušení politiky,

9.2.4. aktualizované právní předpisy nebo smluvní podmínky ovlivňující používání IT.

9.3. Dokumentace změn

9.3.1. Všechny aktualizace musí být zaznamenány v evidenci verzí, která obsahuje:

9.3.1.1. číslo verze,

9.3.1.2. datum přezkumu,

9.3.1.3. shrnutí změn,

9.3.1.4. schvalující autoritu.

9.4. Komunikace politiky

9.4.1. Revidované verze této politiky musí být sdíleny se všemi dotčenými uživateli. Zaměstnanci musí potvrdit převzetí a porozumění v rámci svých povinností v oblasti bezpečnostního povědomí.

10. Související politiky a návaznosti

10.1. Tato politika je provázána s několika dalšími SME politikami, aby bylo zajištěno komplexní pokrytí bezpečnostních odpovědností:

10.1.1. P4S – Politika řízení přístupu: stanoví technické a procesní mechanismy vynucování povoleného používání a omezení účtů.

10.1.2. P8S – Politika bezpečnostního povědomí a školení: zajišťuje vzdělávání uživatelů v oblasti hranic přípustného používání a oznamovacích povinností.

10.1.3. P9S – Politika práce na dálku: upravuje používání firemních systémů mimo pracoviště nebo v domácím prostředí.

10.1.4. P17S – Politika ochrany osobních údajů a soukromí: stanoví pravidla pro nakládání s osobními údaji, která souvisejí s monitorováním přípustného používání a s používáním soukromých zařízení v režimu BYOD.

10.1.5. P30S – Politika reakce na incidenty: upravuje postupy pro vyšetřování a řešení zneužití nebo porušení pravidel přípustného používání.

11. Referenční normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 5.10 – Vyžaduje, aby organizace definovaly a uplatňovaly pravidla přípustného používání firemního majetku.

11.2. ISO/IEC 27002

11.2.1. Opatření 5.10 – Poskytuje pokyny pro přípustné používání systémů, včetně povoleného a zakázaného chování.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Upravuje řízení používání systémů, včetně režimu BYOD.

11.3.2. AC-20 – Vyžaduje autorizaci a monitorování externích systémů.

11.3.3. AT-2 – Zdůrazňuje školení uživatelů v oblasti postupů přípustného používání.

11.4. GDPR

11.4.1. Článek 5(1)(f) – Vyžaduje integritu a důvěrnost osobních údajů, které mohou být ohroženy zneužitím ze strany uživatelů.

11.4.2. Článek 32 – Ukládá zavedení technických a organizačních opatření k zabezpečení systémů a údajů.

11.5. směrnice NIS2

11.5.1. Článek 21(2)(b) – Vyžaduje odpovídající bezpečnostní politiky, včetně pravidel přípustného používání, ke zmírnění kybernetických hrozeb.

11.6. nařízení DORA

11.6.1. Článek 9 – Vyžaduje politiky řízení ICT rizik, které zahrnují kontroly používání a mechanismy jejich uplatňování.

11.7. COBIT 2019

11.7.1. DSS05 – Řízení bezpečnostních služeb: zdůrazňuje řízení chování uživatelů na základě politik.

11.7.2. BAI08 – Řízení znalostí: řeší povědomí o odpovědnostech vyplývajících z politik a vzdělávání v oblasti přípustného používání.