					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P03S					Názov dokumentu: **Politika prijateľného používania**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 5	Relevantné pre celkový rozsah a implementáciu politiky
ISO/IEC 27002:2022	5.10, 5.11, 5	Usmernenia k požiadavkám a kontrolám prijateľného používania
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Zahŕňa používanie systémov a zariadení, monitorovanie a školenie používateľov
Nariadenie EÚ GDPR	Články 5(1)(f), 32	Integrita a dôvernosť údajov a bezpečnostné opatrenia
Smernica EÚ NIS2	Článok 21(2)(b)	Vyžaduje primerané bezpečnostné politiky vrátane politík prijateľného používania
Nariadenie EÚ DORA	Článok 9	Politika riadenia IKT rizík, kontroly, uplatňovanie
COBIT 2019	DSS05, BAI	Bezpečnostné služby a riadenie znalostí

1. Účel

1.1. Táto politika vymedzuje prijateľné, zodpovedné a bezpečné používanie systémov, zariadení, prístupu na internet, elektronickej pošty, cloudových služieb a akýchkoľvek súkromných zariadení používaných na pracovné účely, ktoré organizácia poskytuje alebo schvaľuje.

1.2. Zabezpečuje, aby osoby rozumeli svojim povinnostiam pri používaní IT zdrojov organizácie a pri ochrane integrity údajov, ochrany osobných údajov a kontinuity prevádzky.

1.3. Táto politika podporuje súlad s normou ISO/IEC 27001:2022 tým, že stanovuje jasné pravidlá správania používateľov v súlade so zákonnými, zmluvnými a regulačnými požiadavkami.

2. Rozsah

2.1. Táto politika sa vzťahuje na všetky osoby, ktoré pristupujú k systémom alebo údajom spoločnosti, spravujú ich alebo s nimi inak pracujú, vrátane:

2.1.1. zamestnancov a zmluvných pracovníkov,

2.1.2. dočasných pracovníkov a stážistov,

2.1.3. externých poskytovateľov IT služieb.

2.2. Politika sa vzťahuje na:

2.2.1. počítače, telefóny a tablety vo vlastníctve spoločnosti,

2.2.2. súkromné zariadenia schválené na pracovné použitie (BYOD),

2.2.3. siete spoločnosti, cloudové platformy a softvérové služby,

2.2.4. prístup na internet, systémy elektronickej pošty, zdieľané úložiská a podnikové aplikácie.

2.3. Táto politika sa uplatňuje vo všetkých pracovných prostrediach — na pracovisku, pri práci na diaľku aj v hybridnom režime — a počas celej pracovnej doby.

3. Ciele

3.1. Stanoviť, čo sa považuje za prijateľné a neprijateľné používanie IT systémov.

3.1.1. Znížiť bezpečnostné riziká spôsobené nesprávnym používaním, neoprávneným prístupom alebo zavlečením malvéru.

3.1.2. Chrániť údaje organizácie, informácie o zákazníkoch a reputáciu spoločnosti.

3.1.3. Stanoviť vymáhateľné pravidlá a zabezpečiť zodpovednosť za konanie všetkých používateľov.

3.1.4. Podporiť monitorovanie a súlad s cieľom včas odhaliť porušenia a prijať nápravné opatrenia.

4. Roly a zodpovednosti

4.1. Generálny manažér (GM)

4.1.1. Schvaľuje túto politiku a zodpovedá za to, aby boli k dispozícii zdroje a právomoci potrebné na jej uplatňovanie.

4.1.2. Preskúmava a schvaľuje všetky výnimky z tejto politiky.

4.2. IT manažér alebo externý poskytovateľ IT služieb

4.2.1. Vedie inventár schváleného softvéru a hardvéru.

4.2.2. Konfiguruje zariadenia tak, aby presadzovali pravidlá prijateľného používania (napr. filtrovanie obsahu, auditné logovanie).

4.2.3. Monitoruje používanie z hľadiska možných porušení a vyšetruje incidenty.

4.2.4. Zabezpečuje, aby súkromné zariadenia (BYOD) používané na pracovné účely boli autorizované a bezpečné.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1. Ročné preskúmanie

9.1.1. Túto politiku musí každoročne preskúmať IT manažér, pričom konečné schválenie udeľuje generálny manažér (GM), aby sa zabezpečilo jej priebežné zosúladenie so spôsobmi používania technológií, vznikajúcimi rizikami a požiadavkami na súlad.

9.2. Spúšťače priebežného preskúmania

9.2.1. Preskúmania sa musia vykonať aj v reakcii na:

9.2.2. nové systémy alebo technológie (napr. novú cloudovú službu alebo platformu koncových zariadení),

9.2.3. závažné porušenia politiky,

9.2.4. aktualizované právne predpisy alebo zmluvné podmienky ovplyvňujúce používanie IT.

9.3. Dokumentácia zmien

9.3.1. Všetky aktualizácie musia byť zaznamenané v evidencii verzií, ktorá obsahuje:

9.3.1.1. číslo verzie,

9.3.1.2. dátum preskúmania,

9.3.1.3. súhrn zmien,

9.3.1.4. schvaľujúci orgán.

9.4. Oboznámenie s politikou

9.4.1. Revidované verzie tejto politiky musia byť sprístupnené všetkým dotknutým používateľom. Zamestnanci musia potvrdiť ich prijatie a porozumenie v rámci svojich povinností v oblasti bezpečnostného povedomia.

10. Súvisiace politiky a väzby

10.1. Táto politika sa uplatňuje spolu s ďalšími politikami SME s cieľom zabezpečiť komplexné pokrytie bezpečnostných zodpovedností:

10.1.1. P4S – Politika riadenia prístupu: Definuje technické a procesné presadzovanie povoleného používania a obmedzení účtov.

10.1.2. P8S – Politika bezpečnostného povedomia a školení: Poskytuje používateľom vzdelávanie o hraniciach prijateľného používania a oznamovacích povinnostiach.

10.1.3. P9S – Politika práce na diaľku: Upravuje používanie systémov spoločnosti mimo pracoviska alebo v domácom prostredí.

10.1.4. P17S – Politika ochrany údajov a súkromia: Presadzuje pravidlá nakladania s osobnými údajmi, ktoré sa prelínajú s monitorovaním prijateľného používania a BYOD.

10.1.5. P30S – Politika reakcie na incidenty: Upravuje postupy vyšetrovania a reakcie na nesprávne používanie alebo porušenie podmienok prijateľného používania.

11. Referenčné normy a rámce

11.1. ISO/IEC 27001

11.1.1. Kapitola 5.10 – Vyžaduje, aby organizácie definovali a presadzovali prijateľné používanie informačných aktív.

11.2. ISO/IEC 27002

11.2.1. Kontrola 5.10 – Poskytuje usmernenia pre prijateľné používanie systémov vrátane povoleného a zakázaného správania.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Rieši riadenie používania systémov vrátane súkromných zariadení.

11.3.2. AC-20 – Vyžaduje autorizáciu a monitorovanie externých systémov.

11.3.3. AT-2 – Zdôrazňuje školenie používateľov o postupoch prijateľného používania.

11.4. Nariadenie EÚ GDPR

11.4.1. Článok 5(1)(f) – Vyžaduje integritu a dôvernosť osobných údajov, ktoré môžu byť ohrozené nesprávnym používaním zo strany používateľov.

11.4.2. Článok 32 – Vyžaduje zavedenie technických a organizačných opatrení na zabezpečenie systémov a údajov.

11.5. Smernica EÚ NIS2

11.5.1. Článok 21(2)(b) – Vyžaduje primerané bezpečnostné politiky vrátane pravidiel prijateľného používania s cieľom zmierňovať kybernetické hrozby.

11.6. Nariadenie EÚ DORA

11.6.1. Článok 9 – Vyžaduje politiky riadenia IKT rizík, ktoré zahŕňajú kontroly používania a mechanizmy uplatňovania.

11.7. COBIT 2019

11.7.1. DSS05 – Riadenie bezpečnostných služieb: Zdôrazňuje kontrolu správania používateľov na základe politík.

11.7.2. BAI08 – Riadenie znalostí: Rieši povedomie o povinnostiach vyplývajúcich z politiky a vzdelávanie v oblasti prijateľného používania.