| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vložte název registrované právnické osoby | | | | | | | |
| Číslo dokumentu:<br>P03 | | | | | Název dokumentu:<br>**Zásady přípustného užívání** | | | | | | | |
| Verze:<br>1.0 | | Datum účinnosti:<br>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 | Článek/ustanovení | Komentář |
|---|---|---|
| ISO/IEC 27001:2022 | Kapitola 5 | Stanoví pravidla chování a požadavky pro Zásady přípustného užívání (AUP) |
| ISO/IEC 27002:2022 | Opatření 6.1, 6.2, 8.1, 8.12 | Poskytuje vodítka pro odpovědnosti v oblasti bezpečnosti informací, povědomí a správu zařízení a dat |
| NIST SP 800-53 Rev.5 | AC-19, AC-20, AT-2 | Opatření řízení přístupu a bezpečnostního povědomí relevantní pro užívání IT aktiv |
| GDPR EU | Články 5 odst. 1 písm. f), 32; bod odůvodnění 39 | Vyžaduje důvěrnost a integritu, ukládá technická a organizační opatření a právní základy pro řádné užívání |
| Směrnice NIS2 EU | Článek 21 odst. 2 písm. a)–d) | Ukládá provozní politiky a školení pro bezpečné užívání |
| Nařízení DORA EU | Článek 5 | Podporuje řízení ICT rizik úpravou chování uživatelů |
| COBIT 2019 | APO07, BAI05, DSS05, MEA01 | Lidské zdroje, řízení změn, řízená bezpečnost, monitorování souladu a výkonnosti |

**1. Účel**

1.1 Tyto Zásady přípustného užívání vymezují přípustné a nepřípustné užívání informačních systémů organizace, výpočetních zdrojů, komunikačních nástrojů a postupů nakládání s daty.

1.2 Zajišťují, aby všichni uživatelé rozuměli svým odpovědnostem při používání firemních IT aktiv a aby jejich jednání podporovalo důvěrnost, integritu, dostupnost a zákonné zpracování informací.

1.3 Tato politika naplňuje požadavek ISO/IEC 27001:2022, kapitola 5.10, tím, že stanoví pravidla chování pro užívání systémů a zavádí technická a procesní ochranná opatření ke snížení rizika nesprávného použití, nedbalosti nebo zneužití.

1.4 Dále podporuje vyšetřování a vymáhání požadavků, včetně reakce na incidenty a disciplinárních opatření při porušení.

**2. Rozsah**

**2.1 Tato politika se vztahuje na všechny osoby a subjekty, kterým byl udělen přístup k informačním systémům a aktivům organizace, včetně zejména:**

2.1.1 zaměstnanců, smluvních pracovníků, konzultantů, stážistů a agenturních pracovníků,

2.1.2 dodavatelů třetích stran s přístupem do systémů nebo s delegovanými administrátorskými rolemi,

2.1.3 hostů nebo partnerů využívajících IT infrastrukturu vlastněnou organizací nebo organizací schválenou.

**2.2 Rozsah zahrnuje veškerá technologická a datová aktiva organizace, včetně:**

2.2.1 pracovních stanic, notebooků, mobilních zařízení a serverů,

2.2.2 síťové infrastruktury a služeb hostovaných v cloudu,

2.2.3 e-mailu, zasílání zpráv, ukládání souborů, platforem pro spolupráci a VPN,

2.2.4 dat v klidu, při přenosu nebo při zpracování bez ohledu na jejich formát nebo umístění,

2.2.5 jakéhokoli osobního zařízení používaného v režimu BYOD, které se připojuje k systémům organizace.

**2.3 Tato politika je vymahatelná ve všech pracovních prostředích, včetně:**

2.3.1 firemních kanceláří a výrobních provozů,

2.3.2 míst výkonu práce na dálku nebo v hybridním režimu,

2.3.3 terénních činností nebo prostor spravovaných třetí stranou.

2.4 Všichni uživatelé jsou povinni potvrdit seznámení s touto politikou a dodržovat ji jako podmínku pro přístup k firemním systémům nebo nakládání s firemními daty.

**3. Cíle**

3.1 Stanovit a prosazovat pravidla pro přípustné užívání IT zdrojů organizace.

3.2 Předcházet neoprávněnému přístupu, úniku dat nebo škodám způsobeným nedbalým nebo zlovolným užíváním.

3.3 Chránit firemní sítě, aktiva a data před hrozbami vznikajícími v důsledku chování uživatelů.

3.4 Podporovat plnění právních a smluvních povinností tím, že organizace prokáže náležitou péči při správě a řízení IT zdrojů.

3.5 Zajistit konzistentní a jednoznačné uplatňování disciplinárních opatření a procesů řízení výjimek.

3.6 Podporovat kulturu etického, bezpečného a odpovědného užívání digitálních a fyzických výpočetních zdrojů.

**4. Role a odpovědnosti**

**4.1 Vrcholové vedení**

4.1.1 Schvaluje Zásady přípustného užívání (AUP) a zajišťuje jejich soulad s obchodními cíli, regulatorními požadavky a hodnotami organizace.

4.1.2 Přiděluje zdroje pro prosazování, školení, monitorování a přezkum politiky.

4.1.3 V rámci řízení systému managementu bezpečnosti informací (ISMS) přezkoumává stav souladu a disciplinární opatření související s porušením politiky.

**4.2 IT a týmy informační bezpečnosti**

4.2.1 Zavádějí technická ochranná opatření k prosazování této politiky, včetně:

4.2.2 filtrování obsahu, ochrany před škodlivým kódem, zabezpečení koncových bodů a nástrojů pro monitorování sítě,

4.2.3 konfigurace zabezpečení e-mailu a řešení pro prevenci ztráty dat (DLP),

4.2.4 blokovacích seznamů a seznamů povolených položek pro software, hardware a webové stránky.

4.2.5 Udržují přehled schváleného a zakázaného softwaru, zařízení a služeb.

4.2.6 Vyšetřují podezření na porušení Zásad přípustného užívání (AUP), shromažďují forenzní důkazy a podle potřeby podporují disciplinární nebo právní kroky.

4.2.7 Spolupracují s HR a funkcí Právní a compliance při řešení incidentů, eskalaci a plnění oznamovacích povinností.

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

**9. Požadavky na přezkum a aktualizaci**

**9.1 Důvody přezkumu a četnost**

**9.1.1 Tato politika musí být přezkoumána:**

9.1.1.1 nejméně jednou ročně,

9.1.1.2 po jakýchkoli významných změnách technologií nebo infrastruktury,

9.1.1.3 po incidentech nebo zjištěních auditu, které upozorní na nedostatky v prosazování,

9.1.1.4 v reakci na změny příslušných právních předpisů nebo smluv.

**9.2 Vlastnictví a schvalování**

9.2.1 Za proces přezkumu odpovídá ředitel informační bezpečnosti (CISO) nebo určený manažer ISMS.

9.2.2 Aktualizace musí schválit vrcholové vedení a musí být oznámeny v celé organizaci.

9.2.3 Při opětovném vydání politiky musí být znovu získáno potvrzení seznámení s aktualizovanými podmínkami.

**9.3 Správa dokumentu**

**9.3.1 Politika musí obsahovat následující metadata a údaje o verzování:**

9.3.1.1 název, ID a úroveň klasifikace,

9.3.1.2 vlastníka politiky a správce dokumentu,

9.3.1.3 historii změn a odůvodnění aktualizací,

9.3.1.4 datum přezkumu a datum příští plánované aktualizace,

9.3.1.5 odkazy na distribuční seznamy a evidenci potvrzení seznámení.

9.3.2 Hlavní verze musí být uchovávána v repozitáři dokumentů ISMS v režimu správy verzí.

## 10. Související politiky a vazby

**10.1 Tato politika musí být vykládána ve spojení s následujícími dokumenty:**

10.1.1 P1 – Politika informační bezpečnosti: stanoví základní očekávání ohledně chování a závazek vrcholového vedení k přípustnému užívání.

10.1.2 P4 – Politika řízení přístupu: vymezuje oprávnění a práva spojená s přístupem uživatelů, systémů a dat a přímo prosazuje hranice přípustného užívání.

10.1.3 P6 – Politika řízení rizik: řeší rizika související s chováním a podporuje monitorování a ošetření rizik spojených s hrozbami vyvolanými uživateli.

10.1.4 P7 – Politika nástupu a ukončení: zajišťuje potvrzení seznámení s podmínkami přípustného užívání při nástupu a jejich odvolání při odchodu.

10.1.5 P9 – Politika práce na dálku: rozšiřuje ustanovení o přípustném užívání na prostředí práce na dálku a hybridní práce.

10.2 Tyto související politiky společně tvoří model vícevrstvé obrany pro řízení behaviorálních, technických a smluvních aspektů.

## 11. Referenční normy a rámce

11.1 Tyto Zásady přípustného užívání (AUP) jsou v souladu s mezinárodně uznávanými normami a právními rámci, aby zajistily vymahatelné, auditovatelné a na rizicích založené kontroly chování při veškerém používání digitálních i fyzických informačních systémů.

**11.2 ISO/IEC 27001:2022**

11.2.1 Kapitola 5.10 – Přípustné užívání informací a dalších souvisejících aktiv: tato politika přímo naplňuje požadavek na vymezení, komunikaci a prosazování pravidel upravujících řádné užívání IT zdrojů.

11.2.2 Příloha A, opatření 6.1 – Odpovědnost za bezpečnost informací: přiřazuje jasné odpovědnosti za chování uživatelů a dohled nad souladem.

11.2.3 Příloha A, opatření 6.2 – Povědomí, vzdělávání a školení v oblasti bezpečnosti informací: procesy školení a potvrzení seznámení s politikou jsou začleněny do prosazování Zásad přípustného užívání (AUP).

11.2.4 Příloha A, opatření 8.1 – Zařízení koncových uživatelů a 8.12 – Prevence ztráty dat: řeší přípustné chování na zařízeních uživatelů a upravuje činnosti, které by mohly vést k vystavení dat nebo jejich úniku.

**11.3 NIST SP 800-53 Rev.5:**

11.3.1 AC-19 (řízení přístupu pro mobilní zařízení) a AC-20 (používání externích informačních systémů): tato politika vymezuje povinnosti a omezení uživatelů pro BYOD a přístup do systémů třetích stran.

11.3.2 PL-4 (pravidla chování): poskytuje podrobné požadavky na přípustné užívání v souladu s touto politikou.

11.3.3 AT-2 (školení bezpečnostního povědomí): je podporováno prostřednictvím školení uživatelů a dokumentovaného potvrzení seznámení s politikou.

11.3.4 AU-2 (auditní události) a AU-12 (generování auditních záznamů): prosazování je založeno na monitorování činností uživatelů a upozorňování na porušení.

**11.4 GDPR / obecné nařízení o ochraně osobních údajů (2016/679):**

11.4.1 Článek 5 odst. 1 písm. f): vyžaduje bezpečnost a integritu osobních údajů; tato politika zmírňuje rizika vyplývající z lidského chování a neoprávněného užívání.

11.4.2 Článek 32: ukládá technická a organizační opatření, jako jsou kontroly chování a omezení používání, k ochraně osobních údajů.

11.4.3 Bod odůvodnění 39: zdůrazňuje potřebu zajistit, aby k údajům měly přístup pouze oprávněné osoby v nezbytném rozsahu a aby údaje byly používány zákonným způsobem.

**11.5 Směrnice NIS2 (2022/2555):**

11.5.1 Článek 21 odst. 2 písm. a)–d): vyžaduje provozní politiky a školení pro bezpečné používání systémů, což tyto Zásady přípustného užívání (AUP) zajišťují vymezením chování, monitorování a procesů prosazování.

**11.6 Nařízení DORA (2022/2554):**

11.6.1 Článek 5: tato politika podporuje rámec řízení ICT rizik tím, že stanoví pravidla pro interakci člověka se systémy a minimalizuje expozici kybernetickým rizikům vyplývajícím z chování.

**11.7 COBIT 2019:**

11.7.1 APO07 – APO07: prosazuje odpovědnosti uživatelů a povědomí v průběhu celého životního cyklu zaměstnance.

11.7.2 BAI05 – řízená organizační změna: začleňuje správu přípustného užívání do procesů změn ovlivňujících chování uživatelů.

11.7.3 DSS05 – DSS05: podporuje monitorování činností uživatelů, behaviorální upozornění a automatizované mechanismy reakce.

11.7.4 MEA01 – monitorování, hodnocení a posuzování výkonnosti a souladu: politika stanoví metriky a mechanismy pro ověření souladu uživatelů s očekávaným chováním.