					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P03					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	Stanovuje pravidlá správania a požiadavky pre Politiku prijateľného používania
ISO/IEC 27002:2022	Kontroly 6.1, 6.2, 8.1, 8.12	Poskytuje usmernenia pre zodpovednosti v oblasti informačnej bezpečnosti, povedomie a správu zariadení a údajov
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Riadenie prístupu a kontroly povedomia a správania relevantné pre používanie IT aktív
Nariadenie EÚ GDPR	Články 5(1)(f), 32; odôvodnenie 39	Ukladá požiadavky na dôvernosť a integritu, vyžaduje technické a organizačné opatrenia a právny základ na riadne používanie
Smernica EÚ NIS2	Článok 21(2)(a–d)	Vyžaduje prevádzkové politiky a školenia o bezpečnom používaní
Nariadenie EÚ DORA	Článok 5	Podporuje riadenie IKT rizík úpravou správania používateľov
COBIT 2019	APO07, BAI05, DSS05, MEA01	Ľudské zdroje, riadenie zmien, riadené bezpečnostné služby, monitorovanie súladu a výkonnosti

1. Účel

1.1 Táto politika vymedzuje prípustné a neprípustné používanie informačných systémov organizácie, výpočtových zdrojov, komunikačných nástrojov a postupov pri nakladaní s údajmi.

1.2 Zabezpečuje, aby všetci používatelia rozumeli svojim povinnostiam pri používaní podnikových IT aktív a aby ich činnosti podporovali dôvernosť, integritu, dostupnosť a zákonné spracúvanie informácií.

1.3 Táto politika plní požiadavky kontroly 5.10 normy ISO/IEC 27001:2022 tým, že stanovuje pravidlá správania pri používaní systémov a uplatňuje technické a procesné ochranné opatrenia na minimalizáciu rizika nesprávneho používania, nedbanlivosti alebo zneužitia.

1.4 Zároveň podporuje vyšetrovanie a presadzovanie politiky vrátane reakcie na incidenty a disciplinárnych opatrení pri porušení.

2. Rozsah pôsobnosti

2.1 Táto politika sa vzťahuje na všetky osoby a subjekty, ktorým bol udelený prístup k informačným systémom a aktívam organizácie, vrátane, nie však výlučne:

2.1.1 zamestnancov, zmluvných pracovníkov, konzultantov, stážistov a agentúrnych pracovníkov,

2.1.2 dodávateľov tretích strán s prístupom do systémov alebo delegovanými administrátorskými rolami,

2.1.3 hostí alebo partnerov používajúcich IT infraštruktúru vo vlastníctve organizácie alebo autorizovanú organizáciou.

2.2 Rozsah zahŕňa všetky technologické a dátové aktíva organizácie vrátane:

2.2.1 pracovných staníc, notebookov, mobilných zariadení a serverov,

2.2.2 sieťovej infraštruktúry a služieb prevádzkovaných v cloudovom prostredí,

2.2.3 elektronickej pošty, správ, súborových úložísk, kolaboračných platforiem a VPN,

2.2.4 údajov uložených, prenášaných alebo spracúvaných bez ohľadu na formát alebo umiestnenie,

2.2.5 akéhokoľvek osobného zariadenia používaného v rámci režimu používania vlastných zariadení (BYOD), ktoré sa pripája k systémom organizácie.

2.3 Táto politika sa uplatňuje vo všetkých pracovných prostrediach vrátane:

2.3.1 podnikových kancelárií a výrobných lokalít,

2.3.2 miest výkonu práce na diaľku alebo v hybridnom režime,

2.3.3 prevádzok v teréne alebo priestorov spravovaných tretími stranami.

2.4 Všetci používatelia sú povinní potvrdiť oboznámenie sa s touto politikou a dodržiavať ju ako podmienku prístupu do podnikových systémov alebo nakladania s podnikovými údajmi.

3. Ciele

3.1 Stanoviť a presadzovať pravidlá prípustného používania organizačných IT zdrojov.

3.2 Predchádzať neoprávnenému prístupu, úniku údajov alebo škodám vyplývajúcim z nedbanlivého alebo úmyselného škodlivého konania.

3.3 Chrániť podnikové siete, aktíva a údaje pred hrozbami vyplývajúcimi zo správania používateľov.

3.4 Podporiť plnenie zákonných povinností a zmluvných záväzkov preukázaním náležitej starostlivosti pri správe a riadení IT zdrojov.

3.5 Zabezpečiť konzistentnosť a zrozumiteľnosť pri uplatňovaní disciplinárnych opatrení a procesov riadenia výnimiek.

3.6 Podporovať kultúru etického, bezpečného a zodpovedného používania digitálnych a fyzických výpočtových zdrojov.

4. Roly a zodpovednosti

4.1 Vrcholový manažment

4.1.1 Schvaľuje Politiku prijateľného používania (AUP) a zabezpečuje jej súlad s obchodnými cieľmi, regulačnými požiadavkami a hodnotami organizácie.

4.1.2 Prideľuje zdroje na uplatňovanie politiky, školenia, monitorovanie a jej preskúmanie.

4.1.3 V rámci správy systému manažérstva informačnej bezpečnosti (ISMS) preskúmava stav súladu a disciplinárne opatrenia súvisiace s porušeniami politiky.

4.2 Tímy IT a informačnej bezpečnosti

4.2.1 Zavádzajú technické ochranné opatrenia na uplatňovanie tejto politiky, vrátane:

4.2.2 filtrovania obsahu, antimalvérových opatrení, ochrany koncových bodov a nástrojov na monitorovanie siete,

4.2.3 bezpečnostných konfigurácií elektronickej pošty a riešení na prevenciu straty údajov (DLP),

4.2.4 zoznamov blokovaných a povolených položiek pre softvér, hardvér a webové lokality.

4.2.5 Vedú evidenciu aktív schváleného a zakázaného softvéru, zariadení a služieb.

4.2.6 Vyšetrujú podozrenia na porušenie Politiky prijateľného používania (AUP), zhromažďujú forenzné dôkazy a podľa potreby podporujú disciplinárne alebo právne kroky.

4.2.7 Spolupracujú s útvarom ľudských zdrojov a právnym oddelením pri riešení incidentov, eskalácii a plnení oznamovacích povinností.

[... 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 Spúšťače preskúmania a frekvencia

9.1.1 Táto politika sa musí preskúmať:

9.1.1.1 najmenej raz ročne,

9.1.1.2 po každej významnej zmene technológií alebo infraštruktúry,

9.1.1.3 po incidentoch alebo auditných zisteniach, ktoré poukážu na nedostatky v uplatňovaní politiky,

9.1.1.4 v reakcii na zmeny uplatniteľných právnych predpisov alebo zmluvných záväzkov.

9.2 Vlastníctvo a schválenie

9.2.1 Za proces preskúmania zodpovedá CISO alebo určený manažér ISMS.

9.2.2 Aktualizácie musí schváliť vrcholový manažment a musia byť komunikované v celej organizácii.

9.2.3 Potvrdenie aktualizovaných ustanovení sa musí získať opätovne pri novom vydaní politiky.

9.3 Správa dokumentu

9.3.1 Politika musí obsahovať tieto metadáta a údaje o verzii:

9.3.1.1 názov, identifikátor a stupeň klasifikácie,

9.3.1.2 vlastníka politiky a správcu dokumentu,

9.3.1.3 históriu zmien a dôvody aktualizácií,

9.3.1.4 dátum preskúmania a dátum najbližšej plánovanej aktualizácie,

9.3.1.5 odkazy na distribúciu a záznam potvrdení.

9.3.2 Riadená kópia sa musí uchovávať v úložisku dokumentov ISMS so správou verzií.

10. Súvisiace politiky a väzby

10.1 Táto politika sa musí vykladať v spojení s týmito dokumentmi:

10.1.1 P1 – Politika informačnej bezpečnosti: stanovuje základné očakávania správania a záväzok vrcholového manažmentu k prípustnému používaniu.

10.1.2 P4 – Politika riadenia prístupu: vymedzuje oprávnenia a práva spojené s používateľmi, systémami a prístupom k údajom, čím priamo presadzuje hranice prípustného používania.

10.1.3 P6 – Politika riadenia rizík: rieši riziká súvisiace so správaním a podporuje monitorovanie a opatrenia na ošetrenie rizík spojené s hrozbami vyvolanými používateľmi.

10.1.4 P7 – Politika nástupu a ukončenia pracovného pomeru: zabezpečuje potvrdenie podmienok prípustného používania pri nástupe a odobratie prístupov pri odchode.

10.1.5 P9 – Politika práce na diaľku: rozširuje ustanovenia prípustného používania na prostredie práce na diaľku a hybridnej práce.

10.2 Tieto súvisiace politiky spolu vytvárajú model viacvrstvovej obrany pre správu a riadenie správania, technických opatrení a zmluvných vzťahov.

11. Referenčné normy a rámce

11.1 Táto Politika prijateľného používania (AUP) je zosúladená s medzinárodne uznávanými normami a právnymi rámcami s cieľom zabezpečiť vynútiteľné, auditovateľné a na riziku založené kontroly správania pri každom používaní digitálnych a fyzických informačných systémov.

11.2 ISO/IEC 27001:2022

11.2.1 Kontrola 5.10 – Prípustné používanie informácií a ďalších súvisiacich aktív: Táto politika priamo plní požiadavku definovať, komunikovať a uplatňovať pravidlá upravujúce primerané používanie IT zdrojov.

11.2.2 Príloha A, kontrola 6.1 – Zodpovednosti v oblasti informačnej bezpečnosti: Prideľuje jasné zodpovednosti za správanie používateľov a dohľad nad súladom.

11.2.3 Príloha A, kontrola 6.2 – Povedomie, vzdelávanie a školenie v oblasti informačnej bezpečnosti: Procesy školenia a potvrdenia oboznámenia sa s politikou sú súčasťou uplatňovania Politiky prijateľného používania (AUP).

11.2.4 Príloha A, kontroly 8.1 – Zariadenia koncových používateľov a 8.12 – Prevencia straty údajov: Riešia prípustné správanie na používateľských zariadeniach a upravujú činnosti, ktoré by mohli viesť k vystaveniu údajov alebo ich úniku.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (riadenie prístupu pre mobilné zariadenia) a AC-20 (používanie externých informačných systémov): Táto politika vymedzuje povinnosti používateľov a obmedzenia pre používanie vlastných zariadení (BYOD) a prístup do systémov tretích strán.

11.3.2 PL-4 (pravidlá správania): Poskytuje podrobné požiadavky na prípustné používanie v súlade s touto politikou.

11.3.3 AT-2 (školenie bezpečnostného povedomia): Podporené prostredníctvom školení používateľov a zdokumentovaného potvrdenia oboznámenia sa s politikou.

11.3.4 AU-2 (auditné udalosti) a AU-12 (generovanie auditných záznamov): Uplatňovanie politiky je založené na monitorovaní činností používateľov a upozorňovaní na porušenia.

11.4 Nariadenie EÚ GDPR (2016/679):

11.4.1 Článok 5(1)(f): Vyžaduje bezpečnosť a integritu osobných údajov; táto politika zmierňuje riziká vyplývajúce z ľudského správania a neoprávneného používania.

11.4.2 Článok 32: Vyžaduje technické a organizačné opatrenia, ako sú kontroly správania a obmedzenia používania, na ochranu osobných údajov.

11.4.3 Odôvodnenie 39: Zdôrazňuje potrebu zabezpečiť, aby k údajom mali nevyhnutný prístup a aby ich zákonne používali iba oprávnené osoby.

11.5 Smernica EÚ NIS2 (2022/2555):

11.5.1 Článok 21(2)(a–d): Vyžaduje prevádzkové politiky a školenia pre bezpečné používanie systémov, ktoré táto Politika prijateľného používania (AUP) zabezpečuje definovaním pravidiel správania, monitorovania a procesov uplatňovania.

11.6 Nariadenie EÚ DORA (2022/2554):

11.6.1 Článok 5: Táto politika podporuje rámec riadenia IKT rizík tým, že stanovuje pravidlá pre interakciu používateľov so systémami a minimalizuje vystavenie kybernetickým rizikám vyplývajúcim zo správania.

11.7 COBIT 2019:

11.7.1 APO07 – riadené ľudské zdroje: Presadzuje zodpovednosti používateľov a povedomie počas celého životného cyklu zamestnanca.

11.7.2 BAI05 – riadená organizačná zmena: Začleňuje správu prípustného používania do procesov zmien ovplyvňujúcich správanie používateľov.

11.7.3 DSS05 – riadené bezpečnostné služby: Podporuje monitorovanie činností používateľov, upozornenia na správanie a automatizované mechanizmy reakcie.

11.7.4 MEA01 – monitorovanie, hodnotenie a posudzovanie výkonnosti a súladu: Politika vymedzuje metriky a mechanizmy na overovanie súladu používateľov s očakávanými pravidlami správania.