**Inštalácia softvéru a zariadení v sieťach a informačných systémoch (smernica)**

Táto interná smernica je spracovaná na základe dobrej praxe a reflektuje pravidlá a postupy v kontexte požiadaviek medzinárodnej normy ISO/IEC 27001 v oblasti bezpečnosti prevádzky (Príloha A.12 Bezpečnosť prevádzky, A.12.5 Riadenie operačného softvéru, A.12.5.1 Inštalácia softvéru na operačné systémy, Príloha A.12 Bezpečnosť prevádzky, A.12.5 Riadenie operačného softvéru, A.12.6.2 Obmedzenia pri inštalácii softvéru). Smernica vychádza tiež z požiadaviek legislatívy v oblasti informačnej a kybernetickej bezpečnosti.

|  |  |
| --- | --- |
| **Číslo dokumentu** | *004/2024* |
| **Vydanie/Dátum** | *Vydanie č. 1/10.04.2024* |
| **Revízia/Dátum** | *Bez revízie/10.04.2024* |
| **Počet strán** | *11* |

|  |  |  |
| --- | --- | --- |
| **Autor dokumentu** | *Štandart BPPO s. r. o.* |  |
| **Vlastník dokumentu** | *PETAN parket, s.r.o.* |  |
| **Schválil** | *Kvetoslava Turčeková, konateľ* | *Podpis* |

**Kľúčové súvisiace predpisy a normy**

1. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
2. Vyhláška č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení [najmä však § 11 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. g) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti)]
3. Súbor medzinárodných noriem radu ISO/IEC 27000
4. Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe
5. Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy (najmä však Príloha č. 2, bod F. Bezpečnosť pri prevádzke informačných systémov a sietí, bod H. Ochrana proti škodlivému kódu)
6. Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 546/2021 Z. z., ktorou sa mení a dopĺňa vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy (najmä však § 21 Audio a video súbory, § 22 Súbory audio a video streamingu, § 36 Používanie zásuvných modulov a doplnkov webových prehliadačov a klientskych aplikácií)

**Čl. 1**

**Úvod**

1. Cieľom tejto smernice je rámcovo stanoviť základné pravidlá pre užívateľov, ktorí využívajú informačné i komunikačné technológie v organizácii pri svojej práci.
2. Účelom tejto smernice je rozšíriť pravidlá v oblasti informačnej bezpečnosti v kontexte inštalácie hardvéru a softvéru do aktív organizácie (sietí a informačných systémov), v oblasti určovania vlastníkov aktív a definovania základných zodpovedností a procesov.
3. Táto smernica sa týka najmä základných pravidiel inštalácie hardvéru a softvéru v súvislosti s fyzickými alebo virtuálnymi pracovnými stanicami, mobilnými zariadeniami a perifériami, ktoré sú v organizácii prevádzkované.
4. Táto smernica upravuje povinné postupy a stanovuje pravidlá riadenia inštalácií a zmien aplikácií, hardvéru, softvéru v rámci sietí a informačných systémov organizácie.

**Čl. 2**

**Kompetencie a povinnosti súvisiace s inštaláciou hardvéru a softvéru**

1. Vedenie organizácie
2. Vedenie organizácie zabezpečuje zdroje pre procesy zabezpečenia kybernetickej a informačnej bezpečnosti v kontexte inštalácie softvéru a hardvéru a pre riadenie informačnej a kybernetickej bezpečnosti v organizácii.
3. Komisia pre riadenie zmien
4. Organizácia pre účely riadenia zmien vytvorila Komisiu pre riadenie zmien.
5. Členom Komisie pre riadenie zmien je povinne manažér kybernetickej bezpečnosti organizácie. Ostatní členovia sú menovaní vedením organizácie podľa jej vnútorných priorít.
6. Vedenie organizácie schvaľuje rozsiahle zmeny a dozerá na ich výkon prostredníctvom Komisie pre riadenie zmien v súlade s čl. 4 tejto smernice.
7. Komisia pre riadenie zmien je povinná bezodkladne reagovať na žiadosť o rozsiahlu zmenu v súlade s čl. 4 tejto smernice, posúdiť druh zmeny, oprávnenosť požiadavky a rozhodnúť o ďalšom postupe.
8. Vedúci organizačného útvaru informačných technológií (IT)
9. Je vlastníkom procesu riadenia zmien v rámci inštalácie softvéru a hardvéru v organizácii. V tomto kontexte koncepčne a metodicky vedie ostatné útvary organizácie.
10. Je zodpovedný za plánovanie rozsiahlych zmien infraštruktúry informačných a komunikačných technológií organizácie.
11. Zabezpečuje informovanie vedenia organizácie a manažéra informačnej bezpečnosti o plánovaných a súrnych (podľa čl. 4) závažných zmenách alebo udelení núdzových výnimiek.
12. V prípade podozrenia na kybernetický bezpečnostný incident alebo porušenie pravidiel definovaných touto smernicou alebo inou záväznou normou alebo právnym predpisom má právo rozhodnúť o vykonaní súrnych závažných zmien (podľa čl. 4) alebo o udelení núdzovej výnimky.
13. Správcovia sietí, informačných systémov a aplikácií
14. Sú povinní dodržiavať stanovené pravidlá riadenia inštalácií hardvéru a softvéru v organizácii určené touto smernicou, ďalej zabezpečiť a udržiavať konfigurácie sietí, informačných systémov a aplikácií v aktuálnom stave v zmysle platných politík, v súlade s platnou architektúrou a v zmysle rozhodnutí o zmenách.
15. Na vyžiadanie vedúceho oddelenia IT sú správcovia sietí, informačných systémov a aplikácií povinní poskytnúť súčinnosť pri požiadavke na zmeny a zabezpečiť plnú súčinnosť.
16. Sú povinní bezodkladne implementovať opatrenia, ktoré boli navrhnuté a manažmentom schválené v kontexte požiadavky na zmeny súvisiace s inštaláciou hardvéru alebo softvéru v organizácii.
17. V prípade kybernetického bezpečnostného incidentu, pri ktorom existuje riziko poškodenia kritických aktív organizácie alebo poškodenia dobrého mena organizácie, má správca sietí, informačných systémov a aplikácií právo požadovať od ktoréhokoľvek zamestnanca alebo pracovníka organizácie súčinnosť pre vykonanie súrnych závažných zmien (podľa čl. 4). Všetci zamestnanci a pracovníci organizácie sú povinní takúto súčinnosť bezodkladne poskytnúť.
18. Zamestnanci a pracovníci tretích strán
19. Sú povinní dodržiavať minimálne nasledovné opatrenia:
20. nezasahovať do hardvérovej konfigurácie zverených a používaných aktív organizácie a dodržiavať obmedzenia na inštaláciu a používanie softvéru,
21. nesťahovať a neinštalovať nelegálny softvér alebo voľne šíriteľný softvér bez konzultácie s organizačným útvarom IT,
22. nepoužívať a neinštalovať softvér pre siete so vzájomným sprístupňovaním koncových staníc (peer to peer siete),
23. nedeaktivovať ani nemeniť nastavenia žiadnej ochrany nainštalovanej na akomkoľvek IT zariadení, ktorá nie je v súlade s bezpečnostnými pravidlami organizácie,
24. nešíriť úmyselne škodlivý kód v rámci akejkoľvek siete alebo informačného systému organizácie, zákazníka, tretích strán a verejnej siete,
25. nevykonávať žiadnu inštaláciu alebo používanie neštandardných komunikačných nástrojov,
26. nevykonávať žiadnu inštaláciu softvéru, ktorá je v rozpore s právami duševného vlastníctva alebo licenčnými právami,
27. neinštalovať neschválené aplikácie tretích strán,
28. nevykonávať žiadne hackovanie informácií alebo programov.
29. Sú povinní umožniť automatickú aktualizáciu antivírusového softvéru a aktualizáciu operačného systému na zverených zariadeniach.
30. Je im zakázané akýmkoľvek spôsobom svojvoľne zmeniť konfiguráciu pracovnej stanice alebo informačného systému, najmä však:
31. nastavenia personálneho firewallu,
32. bezpečnostné nastavenia operačného systému,
33. sieťové nastavenia,
34. nastavenia bezpečnostných politík,
35. údaje v registroch a log súboroch operačného systému.

Toto sa nevzťahuje na zamestnanca, ktorý je zodpovedný za správu sietí alebo informačných systémov organizácie, ak ide o plnenie jeho pracovných úloh.

1. Inštaláciu operačných systémov a aplikačného vybavenia na pracovné stanice zabezpečuje výhradne organizačný útvar IT.
2. Sú povinní absolvovať školenie podľa pridelenej role v organizácii a zodpovednosti definovanej v tejto smernici, a to spôsobom školenia o bezpečnostnej dokumentácii zavedenej v organizácii.
3. Sú v plnom rozsahu zodpovední za škody spôsobené zneužitím jeho identity. Pokiaľ dôjde k vyzradeniu hesla alebo zneužitiu identity, sú povinní neodkladne informovať organizačný útvar IT.
4. Ak zistia akýkoľvek nesúlad s ustanoveniami tejto smernice, majú povinnosť na toto upozorniť prostredníctvom svojho nadriadeného.
5. Využívanie IT zariadení pre osobnú potrebu a na prístup k internetu je akceptované, pokiaľ užívateľ dodržiava rozumnú mieru využívania internetu, dodržiava zákony Slovenskej republiky, zásady informačnej bezpečnosti a používa schválený a pravidelne aktualizovaný antivírusový program (v súlade s požiadavkami v čl. 5 tejto smernice).
6. Sú povinní poskytnúť súčinnosť pri riadení zmien súvisiacich s inštaláciou hardvéru alebo softvéru.
7. V prípade úmyselného poškodenia prideleného aktíva alebo jeho poškodenia z nedbanlivosti zo strany zamestnanca bude táto skutočnosť riešená ako bezpečnostný incident s možnými pracovnoprávnymi následkami.

**Čl. 3**

**Riadenie inštalácií operačného softvéru**

1. Organizácia vytvorila, implementovala a udržiava operačný softvér prevádzkovaných sietí a informačných systémov v organizácii v aktualizovanom stave.
2. Aktualizácie operačného softvéru vykonávajú výhradne na to vyškolení administrátori autorizovaní vedením organizácie.
3. Operačný softvér sa musí implementovať až po precíznom otestovaní v testovacom prostredí.
4. Pre riadenie operačného softvéru musí byť spracovaná kontinuita činností.
5. Predchádzajúce verzie operačného softvéru sa musia uchovať pre prípad havárie siete alebo informačného systému organizácie.
6. Softvér dodaný treťou stranou (dodávateľom), ktorý sa používa v prevádzkových systémoch, sa musí udržiavať na úrovni podporovanej dodávateľom.

**Čl. 4**

**Riadenie zmien v kontexte inštalácie hardvéru a softvéru**

1. Organizácia vytvorila, implementovala a udržiava formálnu politiku zakazujúcu inštalovanie a používanie neautorizovaného softvéru a hardvéru.
2. Organizácia vytvorila, implementovala a udržiava formálnu politiku ochrany proti rizikám v kontexte získavania súborov a softvéru z externých sietí alebo cez externé siete, alebo prostredníctvom iných médií. V tejto súvislosti riadi technické zraniteľnosti.
3. Organizácia v pravidelných intervaloch vykonáva revíziu hardvéru a softvéru na podporu funkčnosti kritických procesov organizácie.
4. Ak sa použije dodatočný neschválený softvér alebo nástroje, musia byť tieto formálne autorizovateľné auditovateľným spôsobom zo strany manažmentu organizácie a/alebo zákazníka.
5. Pre potreby riadenia zmien v rámci inštalácií hardvéru alebo softvéru sú v organizácii definované tri základné úrovne z hľadiska závažnosti dopadu na procesy, architektúru a funkcionalitu technickej a technologickej infraštruktúry:
6. Malá (jednoduchá) zmena (označuje sa „ZMENA1 – Malá“)
7. Za malé zmeny sú považované také, ktoré nemajú kritický dopad na aplikačnú architektúru a kontinuitu činností. Tieto činnosti patria k bežným povinnostiam správcov sietí a informačných systémov, ktoré sú popísané v opisoch práce jednotlivých pracovných pozícií.
8. O malú zmenu je oprávnený požiadať projektový manažér v rámci projektových úloh, manažér kvality alebo bezpečnostný pracovník v rámci testovania bezpečnostných opatrení a bezpečnostnej architektúry.
9. Malé zmeny nepodliehajú schvaľovaciemu procesu v procedúrach konfiguračného manažmentu.
10. Závažná zmena (označuje sa „ZMENA2 – Závažná“)
11. Za závažné zmeny sú považované také, ktoré môžu spôsobiť bezprostredný kritický dopad na procesy, na architektúru alebo funkcionalitu technickej a bezpečnostnej infraštruktúry organizácie.
12. Za schvaľovanie požiadaviek na závažnú zmenu je zodpovedný vedúci organizačného útvaru IT. Ten je povinný bezodkladne reagovať na požiadavky na zmenu, posúdiť druh zmeny, oprávnenosť požiadavky a rozhodnúť o ďalšom postupe.
13. Každý oprávnený žiadateľ, ktorý požaduje závažnú zmenu, je povinný zapísať požiadavku na tento typ zmeny v príslušnom systéme pre evidenciu zmien.
14. Rozsiahla zmena (označuje sa „ZMENA3 – Rozsiahla“)
15. Za rozsiahle zmeny sú považované také, ktoré sú vykonávané s cieľom plánovanej dôležitej úpravy obchodných procesov s dopadom na celú organizáciu, resp. úpravy podnikovej, systémovej, aplikačnej alebo bezpečnostnej architektúry, s predpokladom dočasného prerušenia činností na dobu dlhšiu ako 3 pracovné dni.
16. Žiadať o rozsiahle zmeny je oprávnený výhradne vedúci organizačného útvaru IT.
17. Schvaľovať žiadosť o zmenu pre rozsiahle zmeny je oprávnená výhradne Komisia pre riadenie zmien.
18. Každý oprávnený žiadateľ, ktorý požaduje rozsiahlu zmenu, je povinný zapísať požiadavku na tento typ zmeny v príslušnom systéme pre evidenciu zmien.
19. Pre potreby riadenia zmien v rámci inštalácií hardvéru alebo softvéru sú v organizácii definované dve základné priority vykonania zmien pre účely rozhodovacích procesov:
	1. štandardná zmena (čas vykonania zmeny nemá vplyv na procesy a realizované projekty organizácie),
	2. súrna zmena (vykonanie zmeny je nutné pre zaručenie kontinuity činností, pre zníženie vysokého bezpečnostného rizika alebo pre riešenie identifikovaného bezpečnostného incidentu). Tento bod súvisí s procesom definovanom v čl. 2 bod III písm. d).

**Čl. 5**

**Neoprávnená inštalácia softvéru**

1. Softvér získaný stiahnutím z internetu alebo distribúciou na prenosných médiách môže obsahovať škodlivý kód, ktorý sa inštaláciou softvéru môže rozšíriť do celej siete alebo informačného systému organizácie.
2. Neoprávnený softvér nie je s veľkou pravdepodobnosťou kompatibilný so schválenými nainštalovanými programami v organizácii a inštaláciou neoprávneného softvéru môžu prestať fungovať už nainštalované programy.
3. V organizácii sú zavedené pravidlá určujúce zoznam schváleného softvéru a hardvéru.
4. V organizácii je v rámci možnej neoprávnenej inštalácie softvéru zakázané:
5. pripojenie súkromného počítača používateľa do počítačovej siete organizácie,
6. pripojenie súkromného modemu k pracovnému počítaču,
7. pripojenie neschválenej tlačiarne k pracovnému počítaču,
8. pripojenie neschválených prenositeľných pamäťových zariadení k pracovnému počítaču,
9. pripojenie neschváleného bezdrôtového prístupového bodu do počítačovej siete.

**Čl. 6**

**Údržba sietí a informačných systémov v kontexte ochrany pred škodlivým softvérom**

1. Údržba sietí a informačných systémov a zariadení sa vykonáva:
2. **preventívne** – najmä kontrola komponentov siete alebo informačného systému, aplikácia záplat alebo inštalácia nových verzií podporovaných výrobcom,
3. **pri poruchách** – najmä výmena alebo oprava chybnej súčasti siete alebo informačného systému.
4. Organizácia pre inštaláciu hardvéru a softvéru zaviedla princíp najnižšieho privilégia.
5. V organizácii platí pravidlo, že bezpečnostné záplaty sa musia inštalovať pravidelne.
6. Pravidelne na ročnej báze sa musí vykonávať podrobné preskúmanie bezpečnostných vlastností softvéru používaného v organizácii.
7. Všetky pracovné stanice organizácie musia mať spustenú antivírusovú ochranu.
8. Všetky nové softvérové a dátové súbory, najmä ak pochádzajú z neznámeho alebo nedôveryhodného zdroja alebo z nechránených zariadení, sa musia pred použitím skontrolovať na prítomnosť vírusov.
9. Všetky softvérové aj hardvérové zmeny sa musia pred nasadením do prevádzky preskúšať.

**Čl. 7**

**Záverečné ustanovenia**

1. Táto smernica je záväzná pre všetkých zamestnancov organizácie vrátane pracovníkov tretích strán.
2. Táto smernica definuje rámcové procesy pre zamestnancov a pracovníkov tretích strán, ktorí v organizácii zabezpečujú procesy súvisiace so zmenami infraštruktúry informačných a komunikačných technológií v kontexte inštalácie softvéru a hardvéru v rámci ich celého životného cyklu.
3. Za dodržiavanie tejto smernice zodpovedá konateľ organizácie Kvetoslava Turčeková.
4. Odborný výklad tejto smernice je oprávnený podávať a kontrolou jej dodržiavania formou auditov je poverený konateľ organizácie Kvetoslava Turčeková.
5. Táto smernica a z nej vyplývajúca súvisiaca bezpečnostná dokumentácia zavedená v organizácii nadobúda účinnosť schválením predpísanými postupmi.
6. Ak v priebehu účinnosti tejto smernice dôjde k zmenám platných ustanovení, noriem, predpisov a internej dokumentácie, s ktorými bude táto smernica v nesúlade, vedenie organizácie ju zmení vydaním ďalšej nasledujúcej verzie.
7. Porušenie povinností vyplývajúcich z tejto smernice môže byť považované za závažné porušenie pracovnej disciplíny alebo menej závažné až závažné porušenie zmluvy s treťou stranou a môže byť dôvodom pre okamžité skončenie pracovného pomeru zo strany zamestnávateľa v zmysle platných predpisov, resp. zmluvného vzťahu s treťou stranou. Zároveň takéto konanie môže byť dôvodom pre uplatňovanie nároku na náhradu škody zo strany zamestnávateľa.

Bošany, dňa...... Schválil: .............................................

 konateľ organizácie

 Kvetoslava Turčeková