„Interné“

**PETAN parket, s.r.o., M.R. Štefánika 314, 956 18 Bošany, IČO: 50 341 189**

**Používanie kryptografických prostriedkov a šifrovania**

**(smernica)**

Táto smernica reflektuje pravidlá a postupy v kontexte požiadaviek medzinárodnej normy STN ISO/IEC 27001:2014, ako aj platnej legislatívy v oblasti kybernetickej a informačnej bezpečnosti v rámci riadenia kryptografických a šifrovacích metód v organizácii.

|  |  |
| --- | --- |
| **Číslo dokumentu** | *001/2024* |
| **Vydanie/Dátum** | *Vydanie č. 1/10.04.2024* |
| **Revízia/Dátum** | *Bez revízie/10.04.2024* |
| **Počet strán** | *12* |

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

Obsah

[1. Kľúčové súvisiace predpisy a normy 3](#_Toc103615027)

[2. Účel smernice 3](#_Toc103615028)

[3. Zásady, zodpovednosti a rozsah 3](#_Toc103615029)

[4. Algoritmy schválené na používanie v organizácii 5](#_Toc103615030)

[5. Aplikácie schválené na používanie v organizácii 5](#_Toc103615031)

[6. Softvér a protokoly schválené na používanie v organizácii 6](#_Toc103615032)

[7. Šifrovanie a manažment hesiel 6](#_Toc103615033)

[8. Šifrovanie pre bezpečné uloženie údajov 7](#_Toc103615034)

[9. Šifrovanie pre bezpečný prenos 7](#_Toc103615035)

[10. Kryptografické kľúče – správa 8](#_Toc103615036)

[a) Životný cyklus šifrovacích kľúčov 9](#_Toc103615037)

[b) Používanie šifrovacích kľúčov 9](#_Toc103615038)

[11. Validácia a ochrana údajov, bezpečné kódovanie, vývoj softvéru 10](#_Toc103615039)

[12. Záver 11](#_Toc103615040)

# Kľúčové súvisiace predpisy a normy

1. Súbor medzinárodných noriem radu ISO/IEC 27000
2. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
3. Vyhláška č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
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

# Účel smernice

Dôvernosť, integrita, dostupnosť a hodnovernosť údajov v rámci sietí a informačných systémov, prostredníctvom ktorých je poskytovaná základná služba, sa v organizácii zabezpečuje okrem iných opatrení aj pomocou kryptografických prostriedkov používajúcich dostatočne odolné kryptografické mechanizmy, pričom sú určené pravidlá kryptografickej ochrany údajov pri ich prenose alebo uložení v rámci sietí a informačných systémov organizácie.

Účelom tejto smernice je definovanie vhodných algoritmov, protokolov a softvérov na šifrovanie dát v organizácii ***PETAN parket, s.r.o.*** Smernica sa vzťahuje na všetkých pracovníkov organizácie, ktorí majú prístup k informačným systémom organizácie.

# Zásady, zodpovednosti a rozsah

Oblasťou ochrany informácií metódou ich modifikácie do (pre neoprávnenú osobu) nečitateľnej podoby sa zaoberá vedná disciplína „Kryptológia“. Tá v sebe zahŕňa:

1. **kryptografiu**– v rámci nej sa realizujú návrhy protokolov, algoritmova schém, určených na ochranu dôvernosti, integrity a autenticity údajov. Ide o konkrétne metódy úpravy dát, správ či informácií do podoby, ktorá je nečitateľná bez špeciálnych znalostí;
2. **kryptoanalýzu**– v rámci nej sa skúmajú eventuality útokov na takto zabezpečené údaje, teda na „prelomenie“ definovaných algoritmov/protokolov/schém).

Smernica je určená všetkým pracovníkom manažmentu organizácie zodpovedným za prevádzku a vývoj informačných systémov. Je tiež určená pracovníkom zodpovedným za plánovanie, architektúru, vývoj, testovanie a kontrolu kvality a bezpečnosti takýchto informačných systémov.

Zamestnanci sú povinní akceptovať túto smernicu a dodržiavať pravidlá v nej uvedené. Každé porušenie tejto smernice bude riešené ako ***závažné porušenie pracovnej disciplíny v súlade s pracovným a disciplinárnym poriadkom organizácie***.

Vedenie organizácie musí zabezpečiť, aby pracovníci boli oboznámení s touto smernicou a porozumeli svojim úlohám.

Platí, že každý prenos digitálnej dôvernej informácie cez verejnú sieť (napr. FTP, e-mail, uloženie dát na prenosné zariadenia USB, CD/DVD, prenosný harddisk a notebooky a pod.) musí byť zašifrovaný.

Platí, že uzamykanie súborov heslom bez zašifrovania nie je dostatočná ochrana.

Táto smernica je povinná v nasledujúcich prípadoch:

1. aplikácia je orientovaná na internet,
2. aplikácia spracúva údaje, ktoré sú klasifikované ako interné, chránené alebo prísne chránené,
3. spracovávané údaje zahŕňajú osobné údaje.

V oblasti kryptografických opatrení organizácia riadi nasledovné aktivity:

Pri informačných systémoch s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis.

Pri informačných systémoch s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie elektronických dokumentov, dát na prenosných zariadeniach, ktoré sú vynášané mimo priestorov organizácie správcu, emailovej komunikácie prostredníctvom schváleného softvéru, komunikačných kanálov na výmenu nešifrovaných dát, centrálnych úložísk, záloh.

Princípy šifrovania, úrovne ochrany, zodpovednosti a riadenie šifrovacích kľúčov sa dokumentuje.

Kryptografické prostriedky (napr. zraniteľnosti apod.) sa pravidelne prehodnocujú.

# Algoritmy schválené na používanie v organizácii

Vhodné algoritmy na šifrovanie, schválené na použitie v organizácii, sú:

1. symetrické šifrovanie: (napr. Twofish, Serpent, AES, Blowfish, CAST5, RC4, TDES, IDEA),
2. asymetrické šifrovanie: (napr. RSA, DSA),
3. digitálny podpis: (napr. DSA, RSA, GPG),
4. hashovacie funkcie: (napr. SHA256),
5. komunikácia na webových stránkach: (napr. SSL, TLS),
6. elektronická komunikácia: (napr. TrueCrypt, Bitlocker),
7. komunikácia cez WiFi: (napr. WPA2, WPA3).

# Aplikácie schválené na používanie v organizácii

1. **Email** – pre šifrovanú komunikáciu je *preferovaný systém GPG* (pri jeho nedostupnosti je možné použiť *šifrovanie pomocou 7zip*). Klientsky dôverné emaily je povolené zasielať len so šifrovaním (nezašifrované emaily je povolené odoslať len na výslovnú požiadavku klienta – adresát musí byť povolený). Firemne dôverné emaily je povolené zasielať len so šifrovaním.
2. **FTP**– pre šifrovanú komunikáciu *je preferovaný FTP over SSL/TLS, resp. sFTP (SSH)*.
3. **Prenosné médiá**–USB alebo CD/DVD–pre šifrovanú komunikáciu je *preferovaný systém PGP/GPG alebo TrueCrypt*(pri nedostupnosti je možné použiť *šifrovaniepomocou 7zip*). Je povolený minimálny prenos klientskych informácií, ktoré musia byť uložené len na zašifrovanom médiu alebo na klientom dodanom pamäťovom zariadení.
4. **Notebooky, smartphones a iné prenosné počítače** – pre zabezpečenie uložených dát je *preferovaný softvér TrueCrypt Drive Encryption*.
5. **Aplikácie online**– pre šifrovanú komunikáciu je *preferovaný VPN tunel na báze IPSec/TLS*.Pripojenie z externých systémov alebo na externé systémy na správu systémov sa musí riadiť pravidlom, že vzdialený prístup do vnútorných sietí je zriadenýzásadne iba špecialistom oddelenia IT, resp. systémovým administrátorom, a to výhradne len s cieľom vzdialenej správy. Všetky vzdialené prístupové pripojenia musia byť uskutočnené prostredníctvom zabezpečených kanálov (napr. šifrované sieťové pripojenie pomocou SSH alebo IPSec).

# Softvér a protokoly schválené na používanie v organizácii

Vhodný softvér na protokoly na šifrovanie, schválené na použitie v organizácii sú:

1. *VPN tunel: pre komunikáciu je vytvorená virtuálna privátna sieť pre zabezpečenie šifrovaného prenosu dát medzi dvoma sieťami,*
2. *PGP a GPG: šifrovací softvér,*
3. *BitLocker: šifrovanie pevných diskov,*
4. *TrueCrypt: šifrovací softvér, ktorý umožňuje šifrovanie disku a súborov s podporou algoritmov AES 256 a TwoFish,*
5. *7zip softvér: softvér na archivovanie (zip, raratď...), ktorý podporuje AES 256 šifrovanie,*
6. *bezpečné ukladanie prístupov a hesiel: preferovaný je softvér KeePass.*

# Šifrovanie a manažment hesiel

Organizácia definuje nasledovné aktivity ako povinné:

1. Všetky kryptografické funkcie implementovať výhradne v dôveryhodnom informačnom systéme.
2. Všetky náhodné čísla, názvy a reťazce generovať schváleným generátorom náhodných čísel.
3. Vyžadovať autentifikáciu pre všetky stránky a zdroje, okrem tých, ktoré sú konkrétne určené ako verejné.
4. Všetky prvky autentifikácie je potrebné vynútiť v dôveryhodnom informačnom systéme.
5. Dodržiavať požiadavky na komplexnosť hesiel definované bezpečnostnými pravidlami platnými v organizácii.
6. Vynútiť obmedzenú platnosť hesiel a dodržiavanie pravidiel aktualizácie hesiel, tak aby neumožnili rekonštruovať alebo predvídať ďalšie heslá odvodené od predchádzajúcich.
7. Zmeniť všetky predvolené heslá a ID nastavené/dodané výrobcom (deaktivácia súvisiacich účtov).
8. Zadanie hesla skryť na obrazovke používateľa.
9. Zakázať funkcie automatického dopĺňania hesiel.
10. Upozorniť používateľov, ak dôjde k obnoveniu hesla.

# Šifrovanie pre bezpečné uloženie údajov

Keď sa šifrovanie používa na bezpečné uloženie (nie na prenos informácií), sú pracovníci povinní uchovať heslo a/alebo privátny kľúč (PGP/GPG) v tajnosti.

Pracovníci sú povinní používať schválený šifrovací softvér pre šifrovanie pevných diskov notebookov, pre ukladanie zašifrovaných súborov na prenosné médiá, ako aj pre bezpečné ukladanie prístupov a hesiel: TrueCrypt, PGP/GPG, resp. Bitlocker.

Pre bezpečné ukladanie prístupov a hesiel je preferované využiť kľúčenku KeePass.

# Šifrovanie pre bezpečný prenos

Akýkoľvek spôsob prenosu údajov a samotný spôsob šifrovania zabezpečuje a konfiguruje výhradne oddelenie IT.

Privátny kľúč (PGP/GPG) je potrebné uchovávať v tajnosti (zdieľa sa výhradne iba verejný kľúč).

Pre bezpečný prenos dát je preferovaná nasledovná „cesta“: *FTP cez VPN tunel, resp. práca online (homeoffice) cez VPN tunel.*

*Schválenou alternatívou je:*

* + *použitie sFTPalebo FTPs pre prenos dát a*
  + *SSL/TLS alebo SSH pre online práce.*

Pri odosielaní dát na USB kľúči, ktoré sú zašifrované vhodným softvérom, je potrebné zdieľať heslo prostredníctvom samostatného emailu, SMS alebo faxu (zdieľané tajomstvo, ako sú heslá a šifrovacie kľúče, musí byť komunikované prijímateľovi prostredníctvom špeciálneho kanálu–ten musí byť odlišný od kanálu používaného pre samotný prenos dát).

# Kryptografické kľúče – správa

Organizácia riadi kryptografické kľúče vrátane metód ich ochrany a obnovenia zašifrovaných informácií v prípade straty, kompromitovania alebo poškodenia kryptografických kľúčov.

V organizácii sú vytvorené roly a sú určené zodpovednosti v oblasti zavedenia politiky šifrovania a správy šifrovacích kľúčov.

Organizácia deklaruje, že chráni proti úpravám a strate všetky kryptografické kľúče. Utajené a súkromné kľúče chráni pred neautorizovaným použitím a vyzradením. Zariadenia na vytváranie, uskladňovanie a archiváciu kryptografických kľúčov fyzicky chráni. Eviduje dátumy aktivácie a deaktivácie kryptografických kľúčov tak, aby ich bolo možné použiť len v rámci konkrétneho časového úseku definovaného v súlade s politikou správy kryptografických kľúčov.

Systém správy kryptografických kľúčov a certifikátov je zabezpečený počas celého životného cyklu kryptografických kľúčov a certifikátov.

Správa kryptografických kľúčov a certifikátov v organizácii zahŕňa bezpečné nakladanie s kryptografickými kľúčmi a certifikátmi, generovanie pseudonáhodných čísel a kľúčov, zriadenie, distribúciu, vkladanie, zmenu, obmedzenie platnosti, vyberanie, ukladanie a likvidáciu kľúčov a zneplatnenie certifikátov a umožnenie kontroly a auditu.

Žiadny šifrovací kľúč nesmie byť uložený v nechránenej podobe. Každý master kľúč musí byť uložený v chránenej forme (v čitateľnej podobe nesmie byť dostupný). Prístup k master kľúčom musí byť riadený dvojfaktorovou autentifikáciou.

*Organizácia deklaruje, že pre ochranu svojich interných riadiacich systémov aplikuje nasledovné kryptografické techniky:*

* + *digitálny podpis (pre ochranu informácií prichádzajúcich z prevádzkových kontrolérov, ochrana pred zmenami hardvéru, overenie hardvéru),*
  + *šifrovanie (pre ochranu informácií pred zverejnením alebo neoprávneným monitorovaním).*

*Organizácia deklaruje, že v rámci svojich technológií nasadila bezpečnostné integrované obvody so vstavanými ochrannými prvkami (okrem iného aj pre ochranu pred odhalením šifrovacieho kľúča, pre bezchybnú implementáciu šifrovania, resp. pre zabezpečenie komunikácie z dôveryhodných zdrojov).*

# Životný cyklus šifrovacích kľúčov

Pri zaškolení zamestnanca sa v spolupráci so zamestnancom oddelenia IT generuje privátny a verejný kľúč pomocou schváleného šifrovacieho softvéru. Ďalej je potrebné zadať heslo zo strany zamestnanca (heslo, ktoré bude používané pri šifrovaní/dešifrovaní). Zamestnanec je povinný používať šifrovanie počas vykonávania pracovnej činnosti.

Je potrebné zabezpečiť vymazanie šifrovacích kľúčov pri ukončení pracovného pomeru zamestnanca z repozitára verejných kľúčov az pridelených pracovných zariadení zamestnanca (vymazanie účtu, preinštalovanie zariadenia).

# Používanie šifrovacích kľúčov

Zamestnanec nemôže zdieľať svoj privátny kľúč.

Zamestnanec šifruje všetky citlivé firemné dokumenty a citlivé dokumenty zákazníkov. Ak si zamestnanec nie je istý, či šifrovať alebo nie, tak je povinný informácie šifrovať.

V prípade dočasnej nedostupnosti schváleného šifrovacieho softvéru sa na šifrovanie použije *software 7zip*, ktorý nepodporuje asymetrické šifrovanie (avšak je ním možné šifrovať symetrickou šifrou pomocou AES 256). V takomto prípade je nevyhnutné pre distribúciu hesla príjemcovi použiť iný komunikačný kanál než ten, ktorým je zašifrovaný súbor odoslaný.

# Validácia a ochrana údajov, bezpečné kódovanie, vývoj softvéru

Kryptografické opatrenia organizácia používa na zaistenie dôvernosti (ochrana chránených, prísne chránených a kritických informačných aktív), integrity (elektronický podpis alebo MAC správa o pôvodnosti kódu), neodmietnuteľnosti (evidencia výskytu alebo neexistencie udalosti), ako aj autentizácie (autentizácia používateľa pri požiadavke na prístup alebo výmenu informácií).

Politika organizácie v oblasti riadenia šifrovania (kryptografických opatrení) obsahuje požiadavky na správu kryptografických kľúčov v celom rozsahu ich životného cyklu (vytvorenie, uloženie, archivácia, obnova, rozširovanie, zrušenie a likvidácia).

1. **Organizácia definuje nasledovné aktivity ako povinné:**
   * Vykonať validáciu údajov pre všetky údaje, s ktorými sa v organizácii pracuje.
   * Identifikovať všetky zdroje údajov (dôveryhodné a nedôveryhodné).
   * Implementovať najmenšie privilégiá, obmedziť používateľov iba na ich funkčné úlohy, ktoré musia splniť, a obmedziť prístupné a prezerateľné/upraviteľné údaje a systémové informácie, ktoré sú potrebné na plnenie ich konkrétnych úloh.
   * Odstrániť nepotrebnú dokumentáciu k aplikáciám a informačným systémom, pretože to môže útočníkom odhaliť užitočné informácie.
2. **Organizácia definuje nasledovné aktivity ako odporúčané**
   * Všetky chyby validácie musia mať za následok odmietnutie vstupu.
   * Chrániť všetky uložené alebo dočasné kópie citlivých údajov na serveri pred neoprávneným prístupom (odstrániť dočasné pracovné súbory hneď, keď sú už nepotrebné).
   * Šifrovať uložené vysoko citlivé informácie aj na serveri.
   * Zakázať funkcie automatického dokončovania pri vypĺňaní údajov vo formulároch, od ktorých sa očakáva, že budú obsahovať citlivé informácie vrátane autentifikačných údajov.

# Záver

Táto smernica a z nej vyplývajúca súvisiaca bezpečnostná dokumentácia zavedená v organizácii nadobúda účinnosť schválením predpísanými postupmi.

Za dodržiavanie tejto smernice zodpovedá konateľ organizácie **Kvetoslava Turčeková.**

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.

**Komentár/upozornenie:**

Rôzne metódy prístupu k spracovaniu obsahu tejto smernice môžu viesť k odlišným formám výstupov predmetnej dokumentácie. Každý spracovateľ má svoje vlastné spôsoby štylizácie a v rôznych spoločnostiach sú zavedené rozličné formy vizuálu dokumentov. Priložený návrh obsahu smernice nie je vyčerpávajúci. V praxi sa konkrétne spracovanie tejto dokumentácie môže líšiť z pohľadu rôzneho typu a rozsahu prevádzkovaných/poskytovaných služieb, resp. hĺbky detailu toho-ktorého spracovateľa. Takto uvedený obsah predmetnej smernice je len možným príkladom, ako daný dokument spracovať.

**Poznámky k dokumentu:**

* + Každý riadený dokument by mal obsahovať štandardné znaky riadenej firemnej dokumentácie (minimálne názov a evidenčné číslo dokumentu, číslo vydania, dátum vytvorenia dokumentu a jeho následných revízií, podpis osoby zodpovednej za dokument, ako aj podpis člena vrcholového manažmentu zodpovedného za schvaľovanie riadenej dokumentácie).
  + Pri finálnom spracovaní každého dokumentu odporúčame aplikovať formát vizuálu dokumentov, ktorý je v organizácii už zavedený.