„Bezpečnostné opatrenia pre riadenie spracúvania osobných údajov“

Spracované ITAK s.r.o.. Baštová 38 945 01 Komárno
pre :

Obec Okoličná na Ostrove, Hlavná 68, 94613 Okoličná na Ostrove

IČO: 00306622, DIČ: 2021014798

1 Úvod

Dokument „Bezpečnostné opatrenia pre riadenie spracúvania osobných údajov“ je jedným z dokumentov, ktorý Obec Okoličná na Ostrove, Hlavná 68, 94613 Okoličná na Ostrove
IČO: 00306622, DIČ: 2021014798
štatutár **……**
(ďalej len „ Obec Okoličná na Ostrove “) prijíma pre zabezpečenie ochrany osobných údajov pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania. Obec Okoličná na Ostrove vydáva „Bezpečnostné opatrenia pre riadenie spracúvania osobných údajov“ v zmysle zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon o ochrane osobných údajov“).

1.1 Rozsah zdokumentovaných opatrení Obec Okoličná na Ostrove

Celá dokumentácia ochrany osobných údajov je tvorená týmito dokumentmi a ich časťami:

- V dokumente s názvom „Bezpečnostné opatrenia pre riadenie spracúvania osobných údajov“, ktorý obsahuje časti:
  - základné pravidlá ochrany osobných údajov
  - riadenie procesu personálnej bezpečnosti
  - riadenie aktív prevádzkovateľa
  - kontrolná činnosť a preskúmavanie
  - riadenie bezpečnostných incidentov
  - riadenie dostupnosti
  - riadenie prevádzky
  - riadenie bezpečnostných rizík
  - a bezpečnosť systémov.
- A v dokumente s názvom „Bezpečnostné opatrenia pre manipuláciu s osobnými údajmi“, ktorý obsahuje časti:
  - vymedzenie základných pojmov
  - dohľad nad ochranou osobných údajov
  - informačný systém
  - práva dotknutej osoby pri spracúvaní osobných údajov
  - oprávnená osoba
  - zásady spracúvania osobných údajov.

Oboznámenie sa s príslušnými bezpečnostnými opatreniami oprávnená osoba potvrdí svojím podpisom v záverečnej časti dokumentu.

1.2 Štruktúra a formát dokumentácie

Je potrebné zabezpečiť, aby všetky oprávnené osoby mali k dispozícii len aktualizovanú dokumentáciu. Štruktúra dokumentácie je tvorená textom a tabuľkami.

Označenia

Označenia bezpečnostných opatrení pozostávajú z:

- názvu organizácie a sídla,
- názvu bezpečnostných opatrení,
- číselného označenia verzie dokumentu, ktoré je potrebné voliť súvisle a vzostupne.

Všeobecný popis procesu
Pre dosiahnutie prehľadnosti prijatých bezpečnostných opatrení je dokumentácia koncipovaná procesne.
(*Podľa charakteru bezpečnostných opatrení je dokumentácia rozčlenená do* ***samostatných procesov****. Kedy procesom rozumieme súbor vzájomne súvisiacich činností alebo vzájomne pôsobiacich činností, ktoré transformujú vstupy na výstupy. A subprocesov, ktorými budeme rozumieť časť procesu. Samostatné subprocesy tak tvoria jeden proces.)*

Pre všeobecný popis príslušného procesu je použitý úvodný zápis, v ktorom je identifikovaný:

- cieľ procesu,
- vstupy do procesu,
- výstupy z procesu,
- príčiny neriadenosti procesu,
- monitorovacie kritériá,
- metódy riadenia procesu
- profit z procesu,
- a súvisiace formuláre procesu.

Formuláre
Formulár je dokument využívaný pre záznam údajov o priebehu procesu.

1.3 Distribúcia, dostupnosť, aktualizácia

Obec Okoličná na Ostrove je povinná bez zbytočného odkladu zabezpečovať aktualizáciu zdokumentovaných bezpečnostných opatrení, aby zodpovedala prijatým zmenám pri spracúvaní osobných údajov a to až do ukončenia spracúvania osobných údajov v informačnom systéme. Taktiež je povinná zabezpečovať potrebnú aktualizáciu údajov vo vzťahu k Úradu na ochranu osobných údajov Slovenskej republiky.

Aktualizácia
Návrhy na aktualizáciu alebo pripomienky k platným bezpečnostným opatreniam sú oprávnení podávať všetci pracovníci organizácie a to listovou formou alebo elektronicky (formulár s názvom „návrhy na vypracovanie – aktualizáciu – zrušenie opatrení“).
Určený pracovník sleduje a eviduje všetky predložené podnety, pripomienky a návrhy na aktualizáciu opatrení, prejednáva podnety, návrhy a pripomienky so štatutárnym orgánom, ktorý rozhodne o vykonaní aktualizácie opatrení.

Distribúcia
Obec Okoličná na Ostrove zvolí vhodný spôsob distribúcie dokumentácie tak, aby bola prístupná všetkým pracovníkom, ktorí ju potrebujú pri svojej pracovnej činnosti a určí bezpečné miesto pre ukladanie originálov dokumentácie, najnovších (aktuálnych verzií), ale aj všetkých predchádzajúcich.

Riadenie zmien dokumentácie
Všetky zmeny v dokumentácii musia byť riadené tak, aby pracovníci mali vždy k dispozícií aktuálne verzie dokumentácie. Z dokumentácie musí byť vždy jasné, že bola vedením
Obec Okoličná na Ostrove schválená a o ktoré číslo verzie ide.
Určený pracovník vedie o dokumentácii zoznam v členení:

- označenie a názov dokumentácie,
- číslo verzie, ktorú majú pracovníci momentálne k dispozícii (aktuálna),
- dátum schválenia príslušnej verzie (formulár s názvom „prehľad používaných bezpečnostných opatrení“).

2 Základné pravidlá ochrany osobných údajov

2.1 Všeobecný popis procesu pre zabezpečenie dodržiavania základných pravidiel ochrany osobných údajov prevádzkovateľa

Cieľ procesu: Zabezpečiť základnú identifikáciu povinností organizácie vyplývajúcich z legislatívy, zjednotiť štruktúru dokumentácie a poskytnúť základný prehľad povinností zákona o ochrane osobných údajov.

Vstupy do procesu: Požiadavka niektorého z procesov spracúvania osobných údajov, požiadavky legislatívy, žiadosť dotknutej osoby.

Výstupy z procesu: Aktuálna dokumentácia ochrany osobných údajov organizácie, vybavovanie žiadostí dotknutých osôb v zmysle zákona o ochrane osobných údajov.

Príčiny neriadenosti: Nedostatočná motivácia pracovníkov, nedostatočné finančné zdroje organizácie, nedostatočné vzdelávanie pracovníkov.

Monitorovacie kritériá: Dodržiavanie zásad spracúvania osobných údajov v zmysle zákona o ochrane osobných údajov.

Metódy riadenia: Vzdelávanie oprávnených osôb, sledovanie súvisiacej legislatívy.

Profit z riadeného procesu: Zlepšovanie stavu spracúvania osobných údajov, eliminácia bezpečnostných incidentov spôsobených oprávnenou osobou.

Súvisiace formuláre:

- preukázanie príslušnosti oprávnenej osoby,
- návrhy na vypracovanie – aktualizáciu – zrušenie opatrení,
- prehľad používaných bezpečnostných opatrení,
- poverenie zodpovednej osoby.

2.2 Základné pojmy

Na účely dokumentácie ochrany osobných údajov v zmysle zákona 18/2018 Z.z.§5 sa rozumie:
a)súhlasom dotknutej osoby akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov,
b)genetickými údajmi osobné údaje týkajúce sa zdedených genetických charakteristických znakov fyzickej osoby alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby,
c)biometrickými údajmi osobné údaje, ktoré sú výsledkom osobitného technického spracúvania osobných údajov týkajúcich sa fyzických charakteristických znakov fyzickej osoby, fyziologických charakteristických znakov fyzickej osoby alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú jedinečnú identifikáciu alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako najmä vyobrazenie tváre alebo daktyloskopické údaje,
d)údajmi týkajúcimi sa zdravia osobné údaje týkajúce sa fyzického zdravia alebo duševného zdravia fyzickej osoby vrátane údajov o poskytovaní zdravotnej starostlivosti alebo služieb

súvisiacich s poskytovaním zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave,
e)spracúvaním osobných údajov spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami,
f)obmedzením spracúvania osobných údajov označenie uchovávaných osobných údajov s cieľom obmedziť ich spracúvanie v budúcnosti,
g)profilovaním akákoľvek forma automatizovaného spracúvania osobných údajov spočívajúceho v použití osobných údajov na vyhodnotenie určitých osobných znakov alebo charakteristík týkajúcich sa fyzickej osoby, najmä na analýzu alebo predvídanie znakov alebo charakteristík dotknutej osoby súvisiacich s jej výkonnosťou v práci, majetkovými pomermi, zdravím, osobnými preferenciami, záujmami, spoľahlivosťou, správaním, polohou alebo pohybom,
h)pseudonymizáciou spracúvanie osobných údajov spôsobom, že ich nie je možné priradiť ku konkrétnej dotknutej osobe bez použitia dodatočných informácií, ak sa takéto dodatočné informácie uchovávajú oddelene a vzťahujú sa na ne technické a organizačné opatrenia na zabezpečenie toho, aby osobné údaje nebolo možné priradiť identifikovanej fyzickej osobe alebo identifikovateľnej fyzickej osobe,
i)logom záznam o priebehu činnosti používateľa v automatizovanom informačnom systéme,
j)šifrovaním transformácia osobných údajov spôsobom, ktorým opätovné spracúvanie je možné len po zadaní zvoleného parametra, ako je kľúč alebo heslo,
k)online identifikátorom identifikátor poskytnutý aplikáciou, nástrojom alebo protokolom, najmä IP adresa, cookies, prihlasovacie údaje do online služieb, rádiofrekvenčná identifikácia, ktoré môžu zanechávať stopy, ktoré sa najmä v kombinácii s jedinečnými identifikátormi alebo inými informáciami môžu použiť na vytvorenie profilu dotknutej osoby a na jej identifikáciu,
l)informačným systémom akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom základe alebo geografickom základe,
m)porušením ochrany osobných údajov porušenie bezpečnosti, ktoré vedie k náhodnému alebo nezákonnému zničeniu, strate, zmene alebo k neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov alebo inak spracúvaných osobných údajov, alebo k neoprávnenému prístupu k nim,
n)dotknutou osobou každá fyzická osoba, ktorej osobné údaje sa spracúvajú,
o)prevádzkovateľom každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov,
p)sprostredkovateľom každý, kto spracúva osobné údaje v mene prevádzkovateľa,
q)príjemcom každý, komu sa osobné údaje poskytnú bez ohľadu na to, či je treťou stranou; za príjemcu sa nepovažuje orgán verejnej moci, ktorý spracúva osobné údaje na základe osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, v súlade s pravidlami ochrany osobných údajov vzťahujúcimi sa na daný účel spracúvania osobných údajov,
r)treťou stranou každý, kto nie je dotknutou osobou, prevádzkovateľ, sprostredkovateľ alebo inou fyzickou osobou, ktorá na základe poverenia prevádzkovateľa alebo sprostredkovateľa spracúva osobné údaje,
s)zodpovednou osobou osoba určená prevádzkovateľom alebo sprostredkovateľom, ktorá plní úlohy podľa tohto zákona,
t)zástupcom fyzická osoba alebo právnická osoba so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v členskom štáte, ktorú prevádzkovateľ alebo

sprostredkovateľ písomne poveril podľa § 35,
u)podnikom fyzická osoba – podnikateľ alebo právnická osoba vykonávajúca hospodársku činnosť bez ohľadu na jej právnu formu vrátane združení fyzických osôb alebo združení právnických osôb, ktoré pravidelne vykonávajú hospodársku činnosť,
v)skupinou podnikov ovládajúci podnik a ním ovládané podniky,
w)hlavnou prevádzkarňou
1.miesto centrálnej správy prevádzkovateľa v Európskej únii, ak ide o prevádzkovateľa s prevádzkarňami vo viac než jednom členskom štáte, okrem prípadu, keď sa rozhodnutia o účeloch a prostriedkoch spracúvania osobných údajov prijímajú v inej prevádzkarni prevádzkovateľa v Európskej únii a táto iná prevádzkareň má právomoc presadiť vykonanie takýchto rozhodnutí, pričom v takom prípade sa za hlavnú prevádzkareň považuje prevádzkareň, ktorá takéto rozhodnutia prijala,
2.miesto centrálnej správy sprostredkovateľa v Európskej únii, ak ide o sprostredkovateľa s prevádzkarňami vo viac než jednom členskom štáte alebo ak sprostredkovateľ nemá centrálnu správu v Európskej únii, prevádzkareň sprostredkovateľa v Európskej únii, v ktorej sa v kontexte činností prevádzkarne sprostredkovateľa uskutočňujú hlavné spracovateľské činnosti, a to v rozsahu, v akom sa na sprostredkovateľa vzťahujú osobitné povinnosti podľa tohto zákona,
x)vnútropodnikovými pravidlami postupy ochrany osobných údajov, ktoré dodržiava prevádzkovateľ alebo sprostredkovateľ so sídlom, miestom podnikania, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom na území Slovenskej republiky na účely prenosu osobných údajov prevádzkovateľovi alebo sprostredkovateľovi v tretej krajine,
y)kódexom správania súbor pravidiel ochrany osobných údajov dotknutej osoby, ktorý sa prevádzkovateľ alebo sprostredkovateľ zaviazal dodržiavať,
z)medzinárodnou organizáciou organizácia a jej podriadené subjekty, ktoré sa riadia medzinárodným právom verejným, alebo akýkoľvek iný subjekt, ktorý bol zriadený dohodou medzi dvoma alebo viacerými krajinami alebo na základe takejto dohody,
aa)členským štátom štát, ktorý je členským štátom Európskej únie alebo zmluvnou stranou Dohody o Európskom hospodárskom priestore,
ab)treťou krajinou krajina, ktorá nie je členským štátom,
ac)zamestnancom úradu zamestnanec v pracovnom pomere alebo v obdobnom pracovnom vzťahu podľa osobitného predpisu6) alebo štátny zamestnanec, ktorý vykonáva štátnu službu v štátnozamestnaneckom pomere podľa osobitného predpisu7)

2.3 Zásady spracúvania osobných údajov

Osobné údaje možno spracúvať len spôsobom ustanoveným zákonom o ochrane osobných údajov a v jeho medziach tak, aby nedošlo k porušeniu základných práv a slobôd dotknutých osôb, najmä k porušeniu ich práva na zachovanie ľudskej dôstojnosti alebo k iným neoprávneným zásahom do ich práva na ochranu súkromia.

Musia byť preto dodržané zásady v mysle zásad zákona č.18/2018 Z.z. a to :

- **Zásada zákonnosti**
- **Zásada obmedzenia účelu**
- **Zásada minimalizácie osobných údajov**
- **Zásada správnosti**
- **Zásada minimalizácie uchovávania**
- **Zásada integrity a dôvernosti**
- **Zásada zodpovednosti**

- **Zákonnosť spracúvania**
- **Zásada dodržania podmienky poskytnutia súhlasu so spracúvaním osobných údajov**
- **Zásada spracúvania osobitných kategórií osobných údajov**
- **Zásada spracúvania osobných údajov bez potreby identifikácie**

2.3.1 Základné povinnosti Obec Okoličná na Ostrove pri spracúvaní osobných údajov

Obec Okoličná na Ostrove ako prevádzkovateľ informačných systémov je povinný:

- Pred začatím spracúvania osobných údajov vymedziť účel spracúvania osobných údajov. Účel spracúvania osobných údajov musí byť jasný, vymedzený jednoznačne a konkrétne a musí byť v súlade s Ústavou Slovenskej republiky, ústavnými zákonmi, zákonmi a medzinárodnými zmluvami, ktorými je Slovenská republika viazaná.
- Určiť podmienky spracúvania osobných údajov tak, aby neobmedzil právo dotknutej osoby ustanovené zákonom.
- Získavať osobné údaje výlučne na vymedzený alebo ustanovený účel. Je neprípustné získavať osobné údaje pod zámienkou iného účelu spracúvania alebo inej činnosti. Pri získavaní osobných údajov je potrebné zabezpečiť plnenie požiadaviek a zásad zákona

č.18/2018 Z.z. o ochrane osobných údajov. V tejto súvislosti zabezpečiť poučenie oprávnených osôb, že v prípade ak budú vyzvané k preukázaniu svojej totožnosti alebo príslušnosti je oprávnená osoba povinná tejto žiadosti vyhovieť (formulár s názvom „preukázanie príslušnosti oprávnenej osoby“).

- Zabezpečiť, aby sa spracúvali len také osobné údaje, ktoré svojím rozsahom a obsahom zodpovedajú účelu ich spracúvania a sú nevyhnutné na jeho dosiahnutie.
- Zabezpečiť, aby sa osobné údaje spracúvali a využívali výlučne spôsobom, ktorý zodpovedá účelu, na ktorý boli zhromaždené. Je neprípustné združovať osobné údaje, ktoré boli získané osobitne na rozdielne účely.
- Spracúvať len správne, úplné a podľa potreby aktualizované osobné údaje vo vzťahu k účelu spracúvania. Nesprávne a neúplné osobné údaje je potrebné blokovať a bez zbytočného odkladu opraviť alebo doplniť. Nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, prevádzkovateľ zreteľne označí a bez zbytočného odkladu zlikviduje.
- Zabezpečiť, aby zhromaždené osobné údaje boli spracúvané vo forme umožňujúcej identifikáciu dotknutých osôb počas doby nie dlhšej, ako je nevyhnutné na dosiahnutie účelu spracúvania.
- Zlikvidovať tie osobné údaje, ktorých účel spracúvania sa skončil. Po skončení účelu spracúvania možno osobné údaje ďalej spracúvať len za zákonom stanovených podmienok o ochrane osobných údajov.
- Spracúvať osobné údaje v súlade s dobrými mravmi a konať spôsobom, ktorý neodporuje zákonu.
- Zhromaždené osobné údaje na pôvodne určený účel, prevádzkovateľ nemôže spracúvať na iný účel, ktorý je nezlučiteľný s pôvodným účelom spracúvania.
- Počas trvania pôvodne určeného účelu spracúvania osobných údajov ako aj po jeho skončení je prípustné zhromaždené osobné údaje spracúvať v nevyhnutnom rozsahu na historický výskum, vedecký výskum a vývoj alebo na účely štatistiky, čo sa nepovažuje za nezlučiteľné s pôvodným účelom spracúvania. Takto spracúvané osobné údaje

Obec Okoličná na Ostrove nemôže použiť na podporu opatrení alebo rozhodnutí prijatých proti dotknutej osobe a nemôže ich využiť proti záujmom dotknutej osoby na obmedzenie jej základných práv a slobôd. Počas spracúvania osobných údajov na účely podľa prvej vety je prevádzkovateľ povinný ich označiť, anonymizovať ich, ak tým možno dosiahnuť účel spracúvania a zlikvidovať

ich ihneď ako sa stanú nepotrebnými.Pri spracúvaní osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel je prevádzkovateľ a sprostredkovateľ povinný prijať primerané záruky pre práva dotknutej osoby. Tieto záruky obsahujú zavedenie primeraných a účinných technických a organizačných opatrení najmä na zabezpečenie dodržiavania zásady minimalizácie údajov a pseudonymizácie.

2.3.2 Pravdivosť osobných údajov

Do informačných systémov Obec Okoličná na Ostrove možno poskytnúť iba pravdivé osobné údaje. Za nepravdivosť osobných údajov zodpovedá ten, kto ich do informačného systému poskytol (napr. dotknutá osoba, zákonný zástupca a pod.).

2.3.3 Správnosť a aktuálnosť osobných údajov

Osobný údaj sa považuje za správny, kým sa nepreukáže opak. Správnosť a aktuálnosť osobných údajov zabezpečuje Obec Okoličná na Ostrove najmä informovaním zákonných zástupcov o povinnosti ohlasovať zmeny osobných údajov.

2.3.4 Likvidácia osobných údajov

Obec Okoličná na Ostrove po splnení účelu spracúvania osobných údajov, v prípade ak osobné údaje nie sú súčasťou registratúrneho záznamu podľa osobitného zákona, zabezpečí ich likvidáciu v zmysle príslušného bezpečnostného opatrenia.

2.3.5 Spracúvanie osobných údajov oprávnenými osobami

Spracúvanie osobných údajov môže vykonávať iba osoba, ktorá bola riadne poučená o svojich právach, povinnostiach a zodpovednostiach za ich porušenie ešte pred uskutočnením prvej operácie s osobnými údajmi.

2.4 Spracúvanie osobitných kategórií osobných údajov

Osobitnú kategóriu osobných údajov tvoria osobné údaje, ktoré by mohli viesť k diskriminácii dotknutej osoby. V zmysle zákona č.18/2018 Z.z. § 16 ods 1 Spracúvanie osobitných kategórií osobných údajov :Zakazuje sa spracúvanie osobitných kategórií osobných údajov. Osobitnými kategóriami osobných údajov sú údaje, ktoré odhaľujú rasový pôvod alebo etnický pôvod, politické názory, náboženskú vieru, filozofické presvedčenie, členstvo v odborových organizáciách, genetické údaje, biometrické údaje, údaje týkajúce sa zdravia alebo údaje týkajúce sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

Zákaz spracúvania osobitných kategórií osobných údajov neplatí, ak
V zmysle zákona č.18/2018 Z.z. § 16 ods 2 pism.

a) dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov aspoň na jeden konkrétny účel; súhlas je neplatný, ak jeho poskytnutie vylučuje osobitný predpis,
b)spracúvanie je nevyhnutné na účel plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva, práva sociálneho zabezpečenia, sociálnej ochrany alebo verejného zdravotného poistenia podľa osobitného predpisu, medzinárodnej zmluvy, ktorou je Slovenská republika viazaná, alebo podľa kolektívnej zmluvy, ak poskytujú primerané

záruky ochrany základných práv a záujmov dotknutej osoby,
e)spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila,
f)spracúvanie je nevyhnutné na uplatnenie právneho nároku,alebo pri výkone súdnej právomoci,

2.4.1 Osobné údaje o psychickej identite

Spracúvať osobné údaje o psychickej identite fyzickej osoby alebo o jej psychickej pracovnej spôsobilosti môže spracúvať iba psychológ alebo iná osoba, ktorej to umožňuje zákon (napr. lekár vykonávajúci psychoterapeutickú činnosť).

2.4.2 Všeobecne použiteľný identifikátor

Pri spracúvaní osobných údajov možno využiť na účely určenia fyzickej osoby všeobecne použiteľný identifikátor ustanovený osobitným zákonom – rodné číslo len vtedy, ak jeho použitie je nevyhnutné na dosiahnutie daného účelu spracúvania. Spracúvať iný identifikátor, ktorý v sebe skrýva charakteristiky dotknutej osoby, alebo zverejňovať všeobecne použiteľný identifikátor sa zakazuje.

2.4.3 Údaje o porušení zákonov

Spracúvanie osobných údajov o porušení ustanovení zakladajúcich trestnú zodpovednosť alebo administratívnoprávnu zodpovednosť môže vykonávať len ten, komu to umožňuje osobitný zákon.

2.4.4 Biometrické údaje

Prevádzkovateľ je oprávnený spracúvať biometrické údaje len vtedy, ak je to primerané účelu spracúvania a nevyhnutné na jeho dosiahnutie a ak:

- to prevádzkovateľovi vyplýva výslovne zo zákona,
- dotknutá osoba dala na spracúvanie písomný alebo inak hodnoverne preukázateľný súhlas

2.5 Zodpovedná osoba

Obec Okoličná na Ostrove ktorá spracúva osobné údaje prostredníctvom oprávnených osôb výkonom dohľadu písomne poveruje zodpovednú osobu, ktorá dozerá na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov .Jej úlohy sú plnené v zmysle zákona č. 18/2018 Z.z, § 45 a § 46 a sú uvedené v zmluve. Musí byť takisto splnená oznamovacia povinnosť smerom k UOOU a prevádzkovateľ je povinný zverejniť, napríklad na webovom sídle, kontaktné údaje zodpovednej osoby

2.6 Evidencia informačných systémov

O informačných systémoch, ktoré nepodliehajú oznamovacej povinnosti alebo osobitnej registrácii, je povinná viesť evidenciu, a to najneskôr odo dňa začatia spracúvania osobných údajov.
Povinnú evidenciu je potrebné aktualizovať až do dňa ukončenia spracúvania osobných údajov v informačnom systéme. Povinnosť aktualizácie sa nevzťahuje na počet oprávnených osôb.
V prípade, ak by došlo k zmene resp. k spracúvaniu osobných údajov v ďalšom informačnom systéme, Obec Okoličná na Ostrove ešte pred začatím spracúvania osobných údajov posúdi povinnosť evidencie

3 Riadenie procesu personálnej bezpečnosti

3.1 Všeobecný popis procesu riadenia personálnej bezpečnosti

Cieľ procesu: Zabezpečiť, aby pracovníci – oprávnené osoby, iné fyzické osoby ako aj zmluvní partneri z pozícií tretích strán si boli vedomí svojich práv, povinností, zodpovedností a boli vhodní na výkon procesov a subprocesov, ktoré súvisia so spracúvaním osobných údajov.

Vstupy do procesu: Požiadavka niektorého z procesov na personálne obsadenie, požiadavky legislatívy, správanie zmluvnej strany.

Výstupy z procesu: Pracovník kompetentný na výkon pridelenej činnosti spracúvania osobných údajov, preukázateľne poučená oprávnená osoba podľa zákona o ochrane osobných údajov, jasne zadefinované pravidlá v zmluvách so sprostredkovateľmi a pod.

Príčiny neriadenosti: Nedostatočná motivácia pracovníkov, nedostatočné finančné zdroje organizácie, nedostatočné vzdelávanie a poučenia pracovníkov, nevhodne obsadené pracovné miesto nekompetentným pracovníkom vplyvom neúplne definovanej požiadavky na pracovné miesto.

Monitorovacie kritériá: Poučené oprávnené osoby v zmysle zákona o ochrane osobných údajov, zmluvné vzťahy s externými subjektami spĺňajúce náležitosti zákona o ochrane osobných údajov.

Metódy riadenia: vzdelávanie oprávnených osôb, popis pracovných miest, interná kontrolná činnosť.

Profit z riadeného procesu: neustále zlepšovanie stavu spracúvania osobných údajov, eliminácia bezpečnostných incidentov spôsobených pracovníkom spracúvajúcim osobné údaje.

Súvisiace formuláre:

- záznam o poučení oprávnenej osoby,
- záznam o vykonanom školení pracovníkov,
- preverenie spôsobilosti sprostredkovateľa,
- vzor zmluvy medzi prevádzkovateľom a sprostredkovateľom.

3.2 Pred vznikom pracovnoprávneho, zmluvného či obdobného vzťahu Obec Okoličná na Ostrove s jednotlivcom alebo externým subjektom

Cieľom vo fáze výberu pracovníka alebo zmluvného partnera je, aby títo rozumeli zodpovednostiam, aby boli kompetentní na výkon práce s ohľadom na svoje vzdelanie, zručnosti a skúsenosti.

3.2.1 Definovanie pracovného miesta a očakávaní

Podľa organizačnej štruktúry prevádzkovateľa na obsadzovanú pracovnú pozíciu, ktorej pracovník bude tzv. oprávnenou osobou alebo inou fyzickou osobou, je potrebné jasne definovať popis pracovného miesta minimálne v rozsahu:

- názov pracovnej pozície,
- pracovné činnosti, ktoré sú jeho náplňou ,

- osobnostné predpoklady,
- obvyklé pracovné podmienky,
- kvalifikačné požiadavky,
- kompetencie (odborné zručnosti, odborné vedomosti, všeobecné spôsobilosti,
- ktoré bezpečnostné opatrenia pre ochranu osobných údajov sa pracovníka týkajú.

3.2.2 Overenie správnosti predložených dokladov a výber pracovníka

V závislosti od obsadzovanej pracovnej pozície, uchádzač o zamestnanie oprávnenej osobe predkladá minimálne:
a) životopis, ktorého kontrolu úplnosti a presnosti vykoná oprávnená osoba (nahliadnutím do osobného dokladu uchádzača a pod.),
b) potvrdenie dosiahnutého vzdelania.
Posúdenie nevyhnutnosti požadovaných dokladov vykonáva prevádzkovateľom určený pracovník.
Predložené doklady oprávnené osoby ďalej spracúvajú len v nevyhnutnom rozsahu a po nevyhnutnú dobu v zmysle zákona o ochrane osobných údajov.
Následne uchádzačovi o zamestnanie (dotknutej osobe) predložené doklady, ktoré nebudú predmetom ďalšieho spracúvania, vrátia (osobne alebo minimálne v doporučenej zásielke alebo v zásielke určenej do vlastných rúk), prípadne bezpečne zlikvidujú.

3.3 Počas pracovnoprávneho, zmluvného či obdobného vzťahu s prevádzkovateľom a jednotlivcom alebo externým subjektom

3.3.1 Poučenie pracovníkov a zverenie aktív

Ešte pred prvým pokynom k vykonaniu akejkoľvek spracovateľskej operácie s osobnými údajmi, či manipuláciou s aktívami, určený pracovník prevádzkovateľa vykoná poučenie.
Prevádzkovateľ je povinný opätovne poučiť oprávnenú osobu, ak došlo k podstatnej zmene jej pracovného, služobného alebo funkčného zaradenia, a tým sa významne zmenil obsah náplne jej pracovných činností, alebo sa podstatne zmenili podmienky spracúvania osobných údajov alebo rozsah spracúvaných osobných údajov v rámci jej pracovného, služobného alebo funkčného zaradenia.

3.3.2 Udržiavanie bezpečnostného povedomia

Bezpečnostné povedomie oprávnených musí byť udržiavané pravidelnými školeniami, ktoré okrem iného obsiahnu aktualizované bezpečnostné politiky organizácie, ale aj zácvik korektného používania aktív prevádzkovateľa, až po disciplinárny proces.
Súčasťou bezpečnostného povedomia všetkých oprávnených osôb by mali byť informácie nielen z oblasti legislatívy, ale aj o možných hrozbách. Aby v prípade, že by tieto využili zraniteľnosť niektorého z aktív, procesu alebo subprocesu, oprávnené osoby vedeli reagovať.
To znamená, aby zo strany oprávnenej osoby došlo k:
a) rozpoznaniu,
b) oznámeniu,
c) a zaznamenaniu možnej slabiny, resp. zraniteľného miesta systému.
Spôsob oznámenia by mal byť čo najjednoduchší a dostupný. Oprávnené osoby je potrebné dôrazne upozorniť, aby sa nesnažili preukazovať výskyt zraniteľného miesta, nakoľko toto by mohlo byť chápané ako neoprávnené testovanie a jedna z možností potenciálneho zneužitia aktív. Súčasťou poučenia je aj časť týkajúca sa porušenia pracovnej disciplíny, v členení podľa intenzity porušenia, ako aj spôsoboch riešenia (disciplinárneho konania).

Školenia pracovníkov

Za týmto účelom je potrebné vykonávať školenia pracovníkov. V tejto súvislosti sú pracovníci

oboznámení aj:
a) o najpravdepodobnejších hrozbách (napríklad. ako aj výsledok procesu riadenie bezpečnostných rizík),
b) o možných zraniteľnostiach organizácie, ktoré by hrozba mohla využiť,
c) ako sa hrozba prejavuje,
d) aké činnosti vykonať po spozorovaní,
e) koho kontaktovať a akým spôsobom,
f) aké dopady na integritu a dostupnosť spracúvania osobných údajov by prejav hrozby znamenal,
g) ako a aké záznamy vytvoriť.

Záznam o školení

O školení je potrebné viesť písomný záznam, ktorý obsahuje:
- dátum školenia
- meno, priezvisko, pracovná pozícia a vlastnoručný podpis pracovníka, ktorý sa školenia zúčastnil
- predmet a osnovu školenia
- a kto školenie vykonal.

3.3.3 Disciplinárny proces

Oprávnené osoby, ktoré boli preukázateľne poučené preberajú zodpovednosť za prácu s osobnými údajmi a aktívami. Aj napriek tomu, je však nevyhnutné, aby organizácia mala zavedený disciplinárny proces pre pracovníkov, ktorí porušili pridelené zodpovednosti s cieľom chrániť aktíva a predchádzať porušovaniu bezpečnostnej politiky.

3.4 Po skončení pracovnoprávneho, zmluvného či obdobného vzťahu s prevádzkovateľom a jednotlivcom alebo externým subjektom

Po rozviazaní pracovného, zmluvného či obdobného vzťahu s Obec Okoličná na Ostrove či už ide o jednotlivca alebo externý subjekt, je dôležité zabezpečiť, aby došlo najmä:
a) k dodržiavaniu záväzkov mlčanlivosti,
b) k vráteniu všetkých aktív, ktoré pracovník používal,
c) k odňatiu prístupových práv do informačných systémov.

3.4.1 Dodržiavanie záväzkov mlčanlivosti

Prevádzkovateľ

Prevádzkovateľ je povinný zachovávať mlčanlivosť o osobných údajoch, ktoré spracúva. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania osobných údajov.

Oprávnená osoba a iná fyzická osoba

Oprávnená osoba je povinná zachovávať mlčanlivosť o osobných údajoch, s ktorými príde do styku; tie nesmie využiť ani pre osobnú potrebu a bez súhlasu prevádzkovateľa ich nesmie zverejniť a nikomu poskytnúť ani sprístupniť. Toto platí aj pre iné fyzické osoby, ktoré prídu do styku s osobnými údajmi u prevádzkovateľa alebo sprostredkovateľa. Povinnosť mlčanlivosti podľa tohto odseku trvá aj po zániku funkcie oprávnenej osoby alebo po skončení jej pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru alebo obdobného pracovného vzťahu.

Výnimky zo záväzkov mlčanlivosti

Povinnosť mlčanlivosti všeobecne neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona; tým nie sú dotknuté ustanovenia o mlčanlivosti podľa osobitných predpisov. Povinnosť mlčanlivosti sa nepoužije vo vzťahu k úradu pri plnení jeho úloh podľa zákona o ochrane osobných údajov.

3.4.2 Vrátenie aktív prevádzkovateľovi

Aby došlo k vráteniu všetkých aktív, ktoré boli pracovníkovi zverené resp. používal ich, určený pracovník Obec Okoličná na Ostrove podľa zavedeného inventárneho záznamu preverí, či zo strany odchádzajúceho pracovníka došlo k vráteniu všetkých aktív. Zároveň urobí záznam do preberacieho protokolu o vrátení aktíva.

V prípade, ak pracovník niektoré z aktív odkupuje (napr. PC, USB) je dôležité zabezpečiť, aby všetky informácie, ako aj osobné údaje boli z daného aktíva presunuté do organizácie a následne z aktíva, ktoré je predmetom odkúpenia bezpečne odstránené.

3.4.3 Odňatie prístupových práv do informačného systému

Jednou z bezpečnostných požiadaviek, ktorej dodržiavanie je potrebné zabezpečiť je, že všetky informačné systémy, ktoré súvisia so spracúvaním informácií musia byť chránené pred neoprávneným vstupom a to aj prostredníctvom vhodnej politiky hesiel. Po skončení pracovného pomeru je nutné pridelené prístupové práva odňať. Taktiež zabezpečiť odňatie práv pre tzv. fyzický prístup, to znamená odňatie kľúčov, identifikačných kariet a pod. Súčasne zabezpečiť, aby odchádzajúci pracovník bol odstránený z evidencií aktuálnych pracovníkov.
V prípade, ak pracovník disponoval tzv. skupinovým heslom, toto v závislosti od konkrétneho prípadu:

a) zmeniť,
b) odchádzajúceho jednotlivca odstrániť zo všetkých zoznamov, ktoré zabezpečujú skupinový prístup,
c) zabezpečiť informovanie ostatných pracovníkov príp. externých subjektov, aby už nezdieľali informácie s odchádzajúcim jednotlivcom.

O odňatí práv vyhotoví zodpovedný pracovník záznam.

3.4.3.1 Odňatie prístupových práv pred skončením pracovného pomeru

Odňatie prístupových práv ešte pred ukončením pracovného pomeru je potrebné zvážiť vždy, vzhľadom na závažnosť rizikových faktorov, ktorými sú najmä:

- v prípade, ak rozviazanie pracovného pomeru iniciuje Obec Okoličná na Ostrove môže mať odchádzajúci jednotlivec tendenciu poškodiť aktíva prevádzkovateľa a pod.,
- v prípade, ak rozviazanie pracovného pomeru je na žiadosť jednotlivca, je možné, že tento bude chcieť informácie zhromažďovať a následne v budúcnosti neoprávnene využiť,
- hodnota prístupových práv a celková zodpovednosť daného jednotlivca ešte počas trvania pracovného, zmluvného či obdobného pracovného pomeru.

3.5 Opatrenia vo vzťahu k externým subjektom

Cieľom prijatých opatrení je minimalizovať riziká spojené s prístupom externých subjektov k aktívam Obec Okoličná na Ostrove
Za týmto účelom v súlade s procesom riadenie bezpečnostných rizík
Obec Okoličná na Ostrove vyhodnocuje aj riziká týkajúce sa minimálne:

a) aktív, ku ktorým má tretí subjekt prístup,

b) typu prístupu k aktívam,
c) opatrení prevádzkovateľa, ktoré prijal s cieľom zabrániť prístupu k tým aktívam, ku ktorým by externý subjekt prístup nemal mať,
d) požiadaviek na pracovníkov, spôsob ich práce, overenia,
e) dopad na bezpečnosť v prípade náhlej absencie externého subjektu.

V prípade, ak externým subjektom bude sprostredkovateľ v zmysle zákona o ochrane osobných údajov, Obec Okoličná na Ostrove.v rámci výberu sprostredkovateľa preverí jeho odbornú, technickú, organizačnú a personálnu spôsobilosť a celkovú schopnosť zaručiť bezpečnosť spracúvaných osobných údajov. Následne je nutné všetky identifikované riziká premietnuť do zmluvy medzi Obec Okoličná na Ostrove a externým subjektom.
Po vykonaní bezpečnostnej analýzy určený pracovník prehodnotí už prijaté opatrenia v tejto oblasti, prípadne navrhne nové.

3.5.1 Zmluva medzi Obec Okoličná na Ostrove a externým subjektom

Všetky služby, ktoré sú dodávané externými subjektami musia byť podložené zmluvou. Táto musí spĺňať minimálne bezpečnostné požiadavky v súlade s bezpečnostnou politikou

Obec Okoličná na Ostrove

Zmluva tak musí minimálne obsahovať:

Záväzok externého subjektu o tom, že tých svojich pracovníkov, ktorí budú mať prístup k aktívam Obec Okoličná na Ostrove

a) poučí v súlade s bezpečnostnou politikou. O poučení vedie písomný záznam a v prípade požiadavky ho predloží určenému pracovníkovi.
b) Záväzok udržiavania bezpečnostného povedomia svojich pracovníkov.
c) Povinnosť pracovníkov externého subjektu ohlasovať zraniteľnosti, ako aj bezpečnostné incidenty, spôsob oznamovania a následne aj spôsob vyšetrovania.
d) Podrobný popis služby, ktorá bude externým subjektom dodávaná, požiadavky, po splnení ktorých bude služba prijatá a naopak, nesplnením ktorých bude odmietnutá.
e) Kritériá a spôsob merania kvality dodávaných služieb, ako aj spôsob, akým bude externý subjekt upozornený v prípade, ak bude zistené neplnenie požiadavky na službu.
f) Právo Obec Okoličná na Ostrove na pravidelné monitorovanie a preskúmavanie spracúvania osobných údajov v podmienkach sprostredkovateľa.

3.5.2 Zmluva medzi Obec Okoličná na Ostrove a jeho sprostredkovateľom

V prípade, ak je externým subjektom sprostredkovateľ podľa zákona o ochrane osobných údajov, potom musí písomná zmluva obsahovať najmä:

- údaje o zmluvných stranách (ďalej len „identifikačné údaje“);
  a1) titul, meno, priezvisko, dátum narodenia a adresu trvalého pobytu, ak ide o fyzickú osobu,
  a2) názov, právnu formu, adresu sídla a identifikačné číslo, ak ide o právnickú osobu,
  a3) obchodné meno, adresu miesta podnikania a identifikačné číslo, ak ide o fyzickú osobu – podnikateľa,
- deň, od ktorého je sprostredkovateľ oprávnený začať so spracúvaním osobných údajov v mene prevádzkovateľa,
- účel spracúvania osobných údajov,
- názov informačného systému,
- zoznam osobných údajov, ktoré sa budú spracúvať; zoznam osobných údajov možno nahradiť rozsahom osobných údajov podľa § 10 ods. 4 zákona o ochrane osobných údajov,
- okruh dotknutých osôb,
- podmienky spracúvania osobných údajov vrátane zoznamu povolených operácií s osobnými

údajmi,
- vyhlásenie prevádzkovateľa, že pri výbere sprostredkovateľa dbal na jeho odbornú, technickú, organizačnú a personálnu spôsobilosť a jeho schopnosť zaručiť bezpečnosť spracúvaných osobných údajov
- súhlas prevádzkovateľa na spracúvanie osobných údajov sprostredkovateľom prostredníctvom inej osoby (subdodávateľa).
- dobu, na ktorú sa zmluva uzatvára,
- dátum uzatvorenia zmluvy a podpisy zmluvných strán.

Preveriť náležitosti písomnej zmluvy v zmysle zákona o ochrane osobných údajov je potrebné aj vtedy, ak Obec Okoličná na Ostrove je v pozícii sprostredkovateľa a vykonáva operácie spracúvania osobných údajov pre iného prevádzkovateľa.

Inventárny záznam pre aktíva typu AI:

Por. č.	Popis aktíva	Kritické aktívum áno/nie	Označenie aktíva	Umiestnenie aktíva	umiestnenie informácií k obnove	Záznam o likvidácii	Vlastník aktíva
1.							

Inventárny záznam pre aktíva typu AII a AIII:

Por. č.	Popis aktíva	Dodávateľ (e-mail, tel. kontakt)	Kritické aktívum áno/nie	Umiestnenie súvisiacich sieťových prvkov	Záznam o likvidácii (dátum)	Vlastník aktíva (meno, priezvisko, podpis)
1.						

Inventárny záznam pre aktíva typu AIV:

Por. číslo:
Názov aktíva:
Dodávateľ (názov, kontakt):
Jedinečné označenie aktíva:
Hodnota aktíva:
Umiestnenie inštalácií (jedinečné označenia aktív):
Umiestnenie originálnej verzie:
Aktívum podlieha zmenám (áno/nie) a typ zmeny (manuálna/automatická): Aktívum je z kategórie kritické (áno/nie):
Dátum vykonania zmien a popis zmien:
Vlastník aktíva (meno, priezvisko, podpis):
Záznam o likvidácii aktíva:

Inventárny záznam pre aktíva typu AV:

Por. číslo:
Názov aktíva:
Dodávateľ (názov, kontakt):
Jedinečné označenie aktíva:
Hodnota aktíva:
Umiestnenie aktíva:
Aktívum bude vynášané mimo priestorov prevádzkovateľa (áno/nie):
Umiestnenie informácií k obnove aktíva:
Aktívum je z kategórie kritické (áno/nie):
Povolené zariadenia na čítanie prenosných médií (áno/nie):
Vlastník aktíva (meno, priezvisko, podpis):
Záznam o likvidácii aktíva:

Inventárny záznam pre aktíva typu AVI:

Por. číslo:
Názov aktíva:
Dodávateľ:
Jedinečné označenie aktíva:
Umiestnenie aktíva:
Údaje, ktoré sú zaznamenávané (názov IS):
Aktívum je (denné zaznamenávanie, zálohovacie, archivovacie):
Umiestnenie informácií k obnove aktíva: Aktívum bude vynášané mimo priestorov prevádzkovateľa (áno/nie):
Aktívum je z kategórie kritické (áno/nie):
Vlastník aktíva (meno, priezvisko, podpis):
Záznam o likvidácii aktíva:

4 Riadenie aktív prevádzkovateľa

4.1 Všeobecný popis procesu riadenia aktív prevádzkovateľa

Cieľ procesu: Zabezpečenie preukázateľného riadenia aktív Obec Okoličná na Ostrove, ktoré súvisia so spracúvaním osobných údajov tak, aby bola zabezpečená ich primeraná ochrana.

Vstupy do procesu: Záznamy o bezpečnostných incidentoch, záznamy z interných kontrolných činností, požiadavka nápravných alebo preventívnych opatrení, požiadavka pracovníka, dlhodobé ciele prevádzkovateľa, neplnenie požiadaviek aktíva.

Výstupy z procesu: Riadené aktíva s preukázateľne vedenou evidenciou a pridelenou zodpovednosťou.

Príčiny neriadenosti: Nedostatočne špecifikované požiadavky na aktíva, zmluvy s tretími stranami zabezpečujúce dodávky aktív v oblasti ručenia za kvalitu dodaného aktíva, neriadené aktíva v dôsledku nedôslednosti pracovníka.

Monitorovacie kritériá: Bezpečnostné incidenty (ako napr. krádež aktíva, strata) zistené kontrolnou činnosťou, záznamy o aktívach.

Metódy riadenia: Preskúmavanie manažmentom organizácie, kontroly, interné kontrolné činnosti.

Profit z riadeného procesu: pokles nákladov do aktív v dôsledku ich poškodení, lepšie zaobchádzanie s aktívami, kratšia reakčná doba v prípade vzniku bezpečnostného incidentu a jednoduchšie následné prešetrenie incidentu, pokles pravdepodobnosti prístupu neoprávnených osôb k informáciám prevádzkovateľa.

Súvisiace formuláre:

- preberací protokol aktíva
- inventárne záznamy pre jednotlivé typy aktív

4.2 Aktíva prevádzkovateľa

Všetky aktíva sú začlenené podľa spoločných vlastností do tzv. typov

aktív Obec Okoličná na Ostrove, tak eviduje nasledovné typy aktív, ktoré sú predmetom tabuľky.

Tabuľka: Typy a názov aktív prevádzkovateľa

Označenie typu aktíva	**Názov typu aktíva** **Príklady náplne pre daný typ aktíva**	
AI	Osobné údaje a ostatné informácie spracúvané manuálne – v listinnej podobe	- servisné manuály - log záznamy
AII	procesy a služby podporujúce spracúvanie osobných údajov - dodávky tepla - dodávky elektrickej energie - dodávky vody	
AIII	procesy a služby podporujúce spracúvanie osobných údajov	- komunikačné služby prostredníctvom mobilu - zabezpečenie služby pripojenia do siete internet a pod.
AIV	softvér	- firewall

		- antivírusový softvér - operačný softvér - aplikačný softvér a pod.
AV	hardvér	- prenosné PC - stolové PC - mobilné zariadenia - tlačiarne - skenery - skartovacie zariadenia - smerovače - prepínače - ostatné sieťové zariadenia
AVI	prenosné médiá	- pásky - CD a DVD - flash disky - prenosné pevné disky

4.2.1 Kritické aktíva

Okrem uvedených typov aktív prevádzkovateľ definuje aj označenie tzv. kritického aktíva, ktorým môže byť aktívum ktoréhokoľvek typu, jeho zlyhanie, neplnenie požiadaviek, strata, poškodenie, krádež a pod. má/môže mať však zásadný dopad na dostupnosť, integritu či celkovú bezpečnosť spracúvaných údajov.

4.2.2 Vlastník aktíva

Vlastník aktíva zodpovedá za kontrolu, korektné používanie a prácu s aktívom a za jeho celkovú bezpečnosť.

4.2.3 Inventárny zoznam aktív

S cieľom poskytnúť všetkým aktívam primeranú úroveň ochrany, Obec Okoličná na Ostrove

vedie a udržuje o nich inventárny zoznam podľa jednotlivých typov aktív. Inventárny zoznam aktíva musí obsahovať minimálne informácie, ktoré sú nevyhnutné na proces obnovy po bezpečnostnom incidente, ako aj ďalšie potrebné informácie.

Pre aktívum AI:

- popis aktíva,
- informácia o tom, či patrí aktívum do kategórie kritických aktív,
- označenie aktíva,
- umiestnenie aktíva,
- umiestnenie informácií k jeho obnove,
- záznam o likvidácii aktíva (ak je to potrebné),
- vlastníctvo aktíva a vlastnoručný podpis vlastníka aktíva (formulár s názvom „inventárny záznam pre aktívum typu AI“).

Pre aktíva AII a AIII:

- popis podporného procesu a služby,
- dodávateľ (ak je dodávaný externe) a kontaktné informácie,
- informácia o tom, či patrí aktívum do kategórie kritických aktív,
- umiestnenie súvisiacich sieťových prvkov,
- záznam o likvidácii aktíva (zrušenie zmluvného vzťahu),

- vlastníctvo aktíva a vlastnoručný podpis vlastníka aktíva (formulár s názvom „inventárny záznam aktíva typu AII a AIII“).

Pre aktívum AIV:

- názov aktíva,
- dodávateľ (ak je dodávaný externe) a kontaktné informácie,
- hodnota aktíva,
- umiestnenie inštalácií,
- umiestnenie originálnej verzie a dohody o licenciách,
- informácia o tom, či patrí aktívum do kategórie kritických aktív,
- jedinečné označenie aktíva,
- informácia o tom, či aktívum podlieha zmenám (manuálna, automatická),
- záznam o likvidácii aktíva,
- vlastníctvo aktíva a vlastnoručný podpis vlastníka aktíva (formulár s názvom „inventárny záznam pre aktíva typu AIV“).

Pre aktívum AV:

- názov aktíva,
- dodávateľ aktíva a kontaktné údaje,
- hodnota aktíva,
- umiestnenie aktíva,
- umiestnenie informácií k obnove aktíva,
- informácia o tom, či patrí aktívum do kategórie kritických aktív,
- jedinečné označenie aktíva,
- informácia o tom, či aktívum bude vynášané mimo priestorov prevádzkovateľa (áno/nie),
- povolené zariadenia na čítanie prenosných médií,
- záznam o likvidácii aktíva,
- vlastníctvo aktíva a vlastnoručný podpis vlastníka aktíva (formulár s názvom „inventárny záznam pre aktíva typu AV“).

Pre aktívum AVI:

- názov aktíva,
- dodávateľ aktíva a kontaktné údaje,
- umiestnenie aktíva,
- typ informácií, ktoré budú na ňom zaznamenávané (z ktorých informačných systémov),
- umiestnenie informácií k obnove aktíva,
- informácia o tom, či patrí aktívum do kategórie kritických aktív,
- informácia o tom, či pôjde o aktívum pridelené pracovníkovi na denné zaznamenávanie výsledkov svojej činnosti, či pôjde o zálohovacie aktívum alebo archívne aktívum,
- jedinečné označenie aktíva,
- informácia o tom, či aktívum bude vynášané mimo priestorov prevádzkovateľa (áno/nie),
- záznam o likvidácii aktíva,
- vlastníctvo aktíva a vlastnoručný podpis vlastníka aktíva (formulár s názvom „inventárny záznam pre aktíva typu AVI“).

Inventárny zoznam o všetkých aktívach je potrebné udržiavať aktualizovaný.

O všetkých zmenách týkajúcich sa aktíva, vlastník aktíva informuje konateľa spoločnosti.

4.2.4 Preberací protokol aktíva

Pre aktíva, ktoré sú zverené konkrétnemu pracovníkovi je potrebné vyhotoviť preberací protokol (formulár s názvom „preberací protokol aktíva“). Jeho súčasťou je:

- názov aktíva,
- meno a priezvisko pracovníka,
- zoznam povoleného a nainštalovaného softvéru,
- poučenie pracovníka o manipulácii s aktívom,
- dátum,
- podpis pracovníka, ktorému bude aktívum zverené,
- podpis kompetentného pracovníka.

Ak je to možné, každé aktívum by malo byť už na prvý pohľad jednoznačne identifikovateľné svojím jedinečným označením.

4.2.5 Používanie aktív

Každý pracovník musí byť poučený o prijateľnom používaní aktíva ešte skôr, ako bude mať k aktívu prístup. Za vykonané poučenia zodpovedá konateľ spoločnosti, ktorý môže poučenie delegovať na konkrétneho pracovníka v závislosti od typu aktíva.

4.2.6 Zaradenie aktíva do procesu (subprocesu)

Všetky aktíva, ktoré majú byť používané v podmienkach organizácie musia byť pred samotným zaradením do používania autorizované kompetentným pracovníkom v súlade so subprocesom riadenie zmien.

5 Proces kontrolná činnosť a preskúmavanie vedením organizácie.

Proces pozostáva z dvoch subprocesov a to:

- subproces kontrolná činnosť
- a subproces preskúmavanie vedením organizácie.

Pod pojmom kontrolná činnosť budeme pre potreby tohto procesu rozumieť kontrolnú činnosť, ktorú si vykonáva sama organizácia, určený pracovník/pracovníci, zodpovedná osoba.

5.1 Všeobecný popis subprocesu kontrolná činnosť

Cieľ subprocesu: Pravidelnými kontrolovaním zabezpečiť odhaľovanie nezhôd pri spracúvaní osobných údajov.

Vstupy do procesu: Záznamy týkajúce sa kontrolovaného procesu, záznamy o bezpečnostných incidentoch, príslušné bezpečnostné opatrenie (vo forme dokumentácie), zamýšľaná zmena, ktorá bola testovaná a prevádzkovateľ ju chce implementovať do riadnej prevádzky, prizvané oprávnené osoby a ostatní pracovníci (napríklad vlastník procesu) a pod.

Výstupy zo subprocesu: Identifikované zraniteľnosti v procesoch a dokumentáciách, doporučené návrhy na zlepšenie.

Príčiny neriadenosti subprocesu: Nedostatočne vedené záznamy, nevhodné monitorovacie systémy, nekompetentnosť pracovníkov (kontrolóra), nedostatočná interná komunikácia, nesprávna analýza údajov a nedostatočné zistenia nezhôd, nedostatočná podpora pre výkon kontrolnej činnosti, nedodržiavanie harmonogramu kontrolnej činnosti.

Monitorovacie kritériá subprocesu: Protokoly z predchádzajúcej kontrolnej činnosti a z nich vyplývajúce doporučenia, plnenie plánov kontrolnej činnosti, záznamy z jednotlivých procesov.

Metódy riadenia subprocesu: Vykonávanie pravidelnej kontrolnej činnosti podľa určeného harmonogramu, vzdelávanie a príprava pracovníkov pre výkon kontrolných činností.

Profit z riadeného procesu: Minimalizácia nákladov na nápravné opatrenia, trvalé zlepšovanie priebehu procesov.

Súvisiace formuláre:

- ročného harmonogramu kontrolných činností
- operačný plán kontrolnej činnosti
- protokol z kontrolnej činnosti
- záznam z kontrolnej činnosti

5.2 Ročný plán kontrolnej činnosti

Vypracuje ročný harmonogram pre postupné vykonanie kontrol tak, aby došlo k prevereniu všetkých procesov, ktoré ovplyvňujú spracúvanie osobných údajov.

Záznam harmonogramu ročného plánu kontrolnej činnosti obsahuje minimálne:

- dátum a názov kontrolovaného procesu,
- určenie kontrolóra (formulár s názvom „ročný harmonogram kontrolnej činnosti pre rok...“).

Harmonogram vo forme ročného plánu kontrolnej činnosti schváľuje vedenie organizácie.

5.3 Typy kontrolných činností

Podľa dôvodov pre vykonanie kontrolných činností pôjde o:

- Kontrolnú činnosť podľa schváleného harmonogramu, čo je riadna a predpokladaná kontrolná činnosť.
- Následnú kontrolnú činnosť, ktorou je kontrola vykonaná v prípade, ak počas kontroly došlo k identifikáciám významných nezhôd v procesoch alebo v dokumentácii a jeho realizáciou dochádza k preverovaniu plnenia nápravných opatrení v určenom termíne.
- Mimoriadnu kontrolnú činnosť, ktorou je kontrola vykonávaná zodpovednou osobou podľa zákona č.18/2018 Z.z. o ochrane osobných údajov, kedy zodpovedná osoba pred začatím spracúvania osobných údajov v informačnom systéme posúdi, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb. Ďalej v prípade výskytu bezpečnostného incidentu, alebo testovania kritického aktíva, ktoré plánuje organizácia implementovať do riadnej prevádzky.

5.4 Príprava kontrolnej činnosti (platí pre všetky typy kontrolných činností)

Operačný plán kontrolnej činnosti

Operačný plán kontrolnej činnosti je plán, pre kontrolovanie konkrétneho procesu. Určuje:

- názov kontrolovaného procesu,
- cieľ kontroly,
- dôvod kontroly,
- dátum konania kontroly,
- predpokladané trvanie kontroly,
- predpokladané potrebné zdroje,
- určenie vrchného kontrolóra (formulár s názvom „operačný plán kontrolnej činnosti“).

Pri kontrolovaní kontrolór zabezpečuje:

- záznamy z predchádzajúcich kontrolných činností,
- záznamy o plnení predchádzajúcou kontrolou doporučených opatrení a schválených preventívnych a nápravných opatreniach,
- formuláciu vhodných otázok (tieto sa vlastníkovi procesu a subprocesu vopred neoznamujú)
- oboznámenie vlastníka procesu a subprocesu o zameraní kontroly, čase konania kontroly, predpokladanom trvaní kontroly, vyžadovanej dokumentácii, ak je to potrebné o prítomnosti ostatných pracovníkov,
- príslušnú legislatívu (ak upravuje činnosť kontrolovaného procesu a subprocesu) záznamy o bezpečnostných incidentoch a ostatné dokumenty, ktoré súvisia s kontrolovaným procesom.

5.5 Vykonanie kontrolnej činnosti

V úvodnom stretnutí kontrolór oboznámi pracovníkov o:

- cieľoch kontroly,
- predmete kontroly,
- spôsobe vykonania kontroly,
- rozsahu a kritériách kontroly.

Počas priebehu kontrolnej činnosti, kontrolór formou dialógu kladie otázky. K odpovediam je potrebné požadovať dokladovanie tvrdení (dôkazy). Na základe týchto dôkazov kontrolór zisťuje, či sú požiadavky plnené alebo nie. Výsledky si zaznamenáva s čo najpresnejším popisom. Tieto musí vedieť kontrolór vždy dokázať.

5.6 Záver kontrolnej činnosti

Na záver kontrolnej činnosti kontrolór začlení dosiahnuté nezhody podľa ich závažnosti ako:

- Významné nezhody, kedy reálny priebeh procesu alebo dokumentácia neplní požiadavky a to tak, že by mohlo dôjsť k ohrozeniu bezpečnosti spracúvaných osobných údajov.
- Malé nezhody, čo sú minimálne odchýlky v procesoch alebo dokumentácii, ktoré však nemajú vplyv na bezpečnosť spracúvaných osobných údajov.

Vedúci kontrolór (v prípade jednočlenného tímu kontrolór) vypracuje:

- záznam z kontrolnej činnosti – v prípade, ak kontrolnou činnosťou neboli zistené žiadne nedostatky (formulár s názvom „záznam z kontrolnej činnosti“),
- protokol z kontrolnej činnosti – v prípade, ak kontrolnou činnosťou boli zistené nedostatky (formulár s názvom „protokol z kontrolnej činnosti“).

5.7 Všeobecný popis subprocesu preskúmavanie manažmentom Obec Okoličná na Ostrove

Cieľ subprocesu: Preskúmavaním dosiahnuť prijatie vhodných preventívnych a nápravných opatrení, ktoré zabezpečia trvalé zlepšovanie celkového spracúvania osobných údajov.

Vstupy do procesu: Identifikované možnosti zmien v procesoch a dokumentáciách, záznamy z priebehu procesov, porušenia pracovnej disciplíny, nedodržiavanie zmluvných dojednaní s externým subjektom, potreba zmeny zmluvného vzťahu s externým subjektom, kvalitatívna bezpečnostná analýza, návrhy na zlepšenie formou nápravných alebo preventívnych opatrení.

Výstupy z procesu: Schválené návrhy na zlepšenie formou nápravných alebo preventívnych opatrení.

Príčiny neriadenosti: Nedostatočne vedené záznamy z procesov, nevhodné monitorovacie systémy, nekompetentnosť pracovníkov, nedostatočná interná komunikácia, komunikačné bariéry, nesprávna analýza údajov.

Monitorovacie kritériá: Efektivita nápravných a preventívnych opatrení.

Metódy riadenia: Podpora vykonávania pravidelnej kontrolnej činnosti, podpora vykonávania bezpečnostných analýz, vzdelávanie a príprava pracovníkov, pracovné porady.

Profit z riadeného subprocesu: Zlepšovanie pracovného prostredia vplyvom lepšej komunikácie, minimalizácia nákladov na nápravné opatrenia, trvalé zlepšovanie priebehu procesov.

5.8 Koncepcia subprocesu preskúmavanie vedením

5.8.1 Vo vzťahu ku kontrolným činnostiam

Protokol z kontrolnej činnosti je predmetom preskúmavania.

Ak kontrolou došlo k identifikácii nezhôd v priebehu procesu alebo na strane dokumentácie,vedenie formuluje vhodné opatrenia. Tieto sú nápravného alebo preventívneho charakteru, ktoré v určenom termíne navrhne implementovať.

Záznam z výsledku preskúmavania
Z výsledku preskúmavania je potrebné vyhotoviť písomný záznam a uchovať ho. Tento obsahuje minimálne informácie v tomto rozsahu:

- dôvod preskúmavania,
- identifikované nezhody a doporučenia (v prípade kontrolnej činnosti),
- navrhované nápravné a preventívne opatrenia zo strany manažmentu,
- časový harmonogram na ich implementáciu,
- dátum pre vykonanie následnej kontroly.

5.8.2 Vo vzťahu k riadeniu aktív

Požiadavku pre obstaranie aktíva predkladá vlastník typu aktíva (pri podrobnejšom členení vlastník konkrétneho aktíva), podľa príslušnej evidencie aktív. V požiadavke uvedie minimálne tieto informácie:

- dôvod pre obstaranie nového aktíva,
- požiadavky, ktoré by malo nové aktívum plniť,
- typ a označenie nového aktíva, odhadovaná cena obstarania, spôsob obstarania,
- dátum,
- meno vlastníka typu aktíva, ktorý požiadavku predkladá.

Ak obstaranie nového aktíva súvisí s likvidáciou predchádzajúceho, je potrebné predložiť likvidačný záznam aktíva.

Po predložení požiadavky na obstaranie aktíva vedenie organizácie posúdi jej opodstatnenosť a navrhne jej schválenie alebo ju zamietne, prípadne navrhované riešenie upraví tak, aby plnilo požiadavku procesu alebo subprocesu. Obstaraním poverí konkrétneho pracovníka.

6 Riadenie bezpečnostných incidentov

6.1 Všeobecný popis procesu riadenie bezpečnostných incidentov

Cieľ procesu: Zabezpečiť, aby zraniteľnosti, hrozby a samotné bezpečnostné incidenty boli oznamované riadeným spôsobom, čo zabezpečí primeranú a najmä rýchlu reakciu pre prijatie vhodných opatrení.

Vstupy do procesu: Informácie od externých dodávateľov, vlastných pracovníkov a pod.

Výstupy z procesu: Účinné nápravné opatrenia, záznam o bezpečnostnom incidente

Príčiny neriadenosti: Nepravdivé alebo žiadne vstupné informácie, nedostatočné alebo žiadne plány kontinuity činností, nedostatočné zdroje (pracovníci, aktíva a pod.), nedostatočné nápravné opatrenie a jeho implementácia, nedostatočné identifikovanie zdroja bezpečnostného incidentu, čo môže spôsobiť jeho opätovný vznik, nekompetentní pracovníci.

Monitorovacie kritériá: Rýchlosť rozpoznania bezpečnostného incidentu, rýchlosť reakcie naň, čas uvedenia systému do stavu ako pred incidentom, náklady na celkové zvládnutie bezpečnostného incidentu.

Metódy riadenia: Vzdelávanie pracovníkov o možných hrozbách, ich prejavoch a činnostiach súvisiacich s reakciou na incident, preskúmavanie záznamov z bezpečnostných incidentov, preverovanie účinnosti implementovaných nápravných opatrení prípadne preventívnych opatrení.

Profit z riadeného procesu: Minimalizácia počtu bezpečnostných incidentov, minimalizácia nákladov na obnovu systému.

Súvisiace formuláre:

- kontaktné údaje pracovníkov pri rozpoznaní bezpečnostného incidentu,
- vzor oznámenia zmeny tretej strane,
- priebežné zaznamenávanie údajov pri bezpečnostnom incidente.6.2Preventívna príprava pracovníkov

Všetci interní pracovníci ako aj pracovníci externých subjektov, ktorí majú prístup k aktívam by mali vedieť rozpoznať:

- možnú zraniteľnosť systému,
- bezpečnostný incident.

Za týmto účelom je potrebné vykonávať pravidelné školenia pracovníkov. V tejto súvislosti sú pracovníci oboznámení aj:

- o najpravdepodobnejších hrozbách (napríklad ako výsledok procesu riadenie bezpečnostných rizík),
- o možných zraniteľnostiach, ktoré by hrozba mohla využiť,
- o tom ako sa hrozba prejavuje,
- o tom aké činnosti vykonať po spozorovaní incidentu,
- o tom koho kontaktovať a akým spôsobom,
- o tom aké dopady na integritu a dostupnosť spracúvania osobných údajov by prejav hrozby znamenal,
- o tom ako a aké záznamy vytvoriť.

6.3 Rozpoznanie hrozby, zraniteľnosti alebo bezpečnostného incidentu

K rozpoznaniu hrozby, zraniteľnosti alebo bezpečnostného incidentu môže dôjsť na úrovni:

- externých subjektov,
- iných fyzických osôb,
- vlastných pracovníkov,
- automaticky monitorovacích systémov.

6.3.1 Externý subjekt

Vo vzťahu k externým subjektom je Obec Okoličná na Ostrove obvykle ako „nákupca“.
Ide o dodávky elektrickej energie, dodávky tepla, dodávky vody ako aj ostatných služieb.
U týchto subjektov je nutné preveriť zmluvné ošetrenie povinnosti externého subjektu oznamovať akékoľvek prerušenia dodávaných služieb, ktoré by mohli ohroziť dostupnosť a integritu spracúvania osobných údajov a to v určenej lehote a na kontaktné miesta definované prevádzkovateľom. Lehota pre oznámenie musí byť dostatočne dlhá na to, aby mohlo dôjsť k prijatiu vhodných opatrení na minimalizáciu dopadu.

6.3.2 Iné fyzické osoby

Fyzické osoby (ako napríklad zákonní zástupcovia detí a žiakov) musia mať možnosť oznamovať bezpečnostné incidenty čo najjednoduchším spôsobom. Za týmto účelom možno použiť tzv. kontaktné miesta, ktorými sú:

- e-mailová adresa, na ktorú je možné zaslať e-mail so žiadosťou o nápravu, kontakt na zodpovednú osobu
- telefonicky kontakt
- osobne v kancelárskych priestoroch organizácie.
- Informácie o kontaktných miestach môžu byť fyzickej osobe poskytnuté aj ako súčasť zmluvy, alebo prostredníctvom webového sídla prevádzkovateľa, zodpovednej osoby

6.3.3 Vlastní pracovníci

Vo všeobecnosti sú definované nasledujúce okruhy hrozieb, ktoré môžu spôsobiť narušenie integrity a dostupnosti spracúvania osobných údajov:

- prírodná katastrofa,
- ľudská chyba,
- úmyselný útok,
- technická alebo programová porucha,
- externé zlyhanie.
-

Prejavy týchto hrozieb sú bližšie špecifikované v procese riadenie bezpečnostných rizík. V závislosti od typu hrozieb pracovníci informujú prostredníctvom definovaných informačných kanálov zodpovedajúcich pracovníkov Obec Okoličná na Ostrove

Po rozpoznaní hrozby, zraniteľnosti alebo incidentu si pracovník v čo najkratšom čase zaznamená podrobnosti týkajúce sa nezhody. Ide najmä o informácie týkajúce sa:

- času kedy došlo k rozpoznaniu,
- prejavov nezhody (správy na monitore, stav zariadenia, poškodenie zabezpečenia priestorov a pod.).

Oznámenie príslušným pracovníkom
Prevádzkovateľ udržuje poradie a zoznam tých pracovníkov s príslušnou zodpovednosťou, ktorých je nutné v čo najkratšom čase kontaktovať v prípade, ak dôjde k rozpoznaniu bezpečnostnej hrozby, zraniteľnosti alebo bezpečnostného incidentu (formulár s názvom „kontaktné údaje pracovníkov pri rozpoznaní bezpečnostného incidentu“).

6.4 Kontaktovanie príslušných orgánov

V prípade, ak vyšetrovanie bezpečnostného incidentu môže súvisieť s trestnoprávnou zodpovednosťou, je potrebné kontaktovať príslušný orgán. Za týmto účelom Obec Okoličná na Ostrove vedie zoznam kontaktov, ktoré sú voľne dostupné v kancelárskych priestoroch organizácie.

6.5 Oznamovanie zmien tretím stranám

Ak prevádzkovateľa upozorní dotknutá osoba alebo ak si dotknutá osoba uplatní u prevádzkovateľa svoje právo, prípadne ak prevádzkovateľ sám zistí, že poskytol tretej strane nesprávne, neúplné alebo neaktuálne osobné údaje, alebo ich poskytol bez právneho základu, je povinný bez zbytočného odkladu písomne oznámiť to každému, komu ich poskytol.

Prevádzkovateľ v oznámení uvedie:

- aké opatrenia na nápravu vykonal,
- najmä či osobné údaje blokoval, doplnil, opravil, aktualizoval alebo zlikvidoval,
- a aké opatrenia žiada prijať od tretej strany.

Vzor oznámenia zmeny tretej strane je predmetom prílohy.

6.6 Zber údajov a priebežné zaznamenávanie

Zaznamenávanie údajov je potrebné pre prijatie vhodných priebežných opatrení, ako aj následnej analýzy priebehu bezpečnostného incidentu s cieľom zamedzenia opätovnému výskytu a to:

- kým bol bezpečnostný incident rozpoznaný,
- kedy došlo k rozpoznaniu resp. zisteniu (dátum a čas),
- kedy došlo k vzniku incidentu,
- čo uvedená nezhoda (incident) spôsobila,
- kde došlo k jej prejavu a ako sa prejavila,
- pravdepodobný dôvod bezpečnostného incidentu,
- prípadne ďalšie podrobnejšie informácie o incidente (formulár s názvom „priebežné zaznamenávanie údajov pri bezpečnostnom incidente“).

6.7 Vykonanie priebežných opatrení (dočasných)

Ak je to nutné, zodpovedný pracovník Obec Okoličná na Ostrove.implementuje opatrenia pre zamedzenie ďalších dôsledkov incidentu, ako aj možnosti jeho opakovania.

6.8 Obnova systému

Cieľom obnovy systému je zabezpečiť jeho návrat do stavu pred vznikom bezpečnostného incidentu. Tieto sú zdokumentované v plánoch kontinuity činností.

6.9 Vyhotovenie a uchovanie záznamu

Do priebežného záznamu o priebehu bezpečnostného incidentu sú následne doplnené:

- dátum a čas, kedy došlo k obnove prevádzky použitím priebežných opatrení,
- dátum a čas, kedy došlo k úplnej obnove,
- vykonané nápravné opatrenia,
- aké opatrenia podnik prijal na zamedzenie opakovaného výskytu (formulár s názvom „priebežné zaznamenávanie údajov pri bezpečnostnom incidente“).

Úplný záznam o bezpečnostnom incidente je potrebné ukladať na určenom bezpečnom mieste, aby sa zabránilo neoprávnenej manipulácii (pozmeňovaniu), strate a pod. Jeho využitie je v časti poučenia z bezpečnostného incidentu alebo ako dôkaz, ak bol bezpečnostný incident spôsobený porušením zmluvy (pre potreby kompenzácie), či pre prípad občianskeho alebo trestného konania.

6.10 Poučenie z bezpečnostného incidentu

Najneskôr po uplynutí 5 pracovných dní je potrebné zanalyzovať celkový priebeh, ako aj riešenie bezpečnostného incidentu a podľa možností jednoznačne identifikovať zdroj, resp. čím/kým bol bezpečnostný incident spôsobený. Následná analýza si vyžaduje:

- prítomnosť všetkých pracovníkov, ktorých sa incident týkal
- a záznamy z bezpečnostného incidentu.

Analýzou reakcie na bezpečnostný incident postupne preskúmať:

- činnosti, ktoré boli vykonané a či to bolo správne, v prípade ak nie, aký bol dôvod,
- či došlo k včasnému rozpoznaniu a následnému oznamovaniu,
- či implementované opatrenia boli „pripravené“ a sú súčasťou plánov riadenia kontinuity činností alebo išlo o chaotickú reakciu,
- či mala organizácia v danej situácii k dispozícii dostatočné zdroje,
- navrhované nápravné opatrenia a lehotu na ich zavedenie do praxe.

Určený pracovník na záver vyhotoví správu, ktorú predloží vedeniu organizácie.
Po uplynutí určenej lehoty pre prijatie nápravných opatrení preverí ich účinnosť.

6.11 Oznámenie porušenia ochrany osobných údajov úradu v zmysle zákona č. 18/2018 Z.z.§ 40

(1)
Prevádzkovateľ je povinný oznámiť úradu porušenie ochrany osobných údajov do 72 hodín po tom, ako sa o ňom dozvedel; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby.
(2)
Ak prevádzkovateľ nesplní oznamovaciu povinnosť podľa odseku 1, musí zmeškanie lehoty zdôvodniť.
(3)
Sprostredkovateľ je povinný oznámiť prevádzkovateľovi porušenie ochrany osobných údajov bez zbytočného odkladu po tom, ako sa o ňom dozvedel.
(4)
Oznámenie podľa odseku 1 musí obsahovať najmä
a)opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
b)kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
c)opis pravdepodobných následkov porušenia ochrany osobných údajov,
d)opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.
(5)
Prevádzkovateľ je povinný poskytnúť informácie podľa odseku 4 v rozsahu, v akom sú mu známe v čase oznámenia podľa odseku 1; ak v čase oznámenia podľa odseku 1 nie sú prevádzkovateľovi známe všetky informácie podľa odseku 4, poskytne ich bezodkladne po tom, čo sa o nich dozvie.
(6)
Prevádzkovateľ je povinný zdokumentovať každý prípad porušenia ochrany osobných údajov podľa

odseku 1 vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

6.12 Oznámenie porušenia ochrany osobných údajov dotknutej osobe č. 18/2018 Z.z.§ 41

(1)
Prevádzkovateľ je povinný bez zbytočného odkladu oznámiť dotknutej osobe porušenie ochrany osobných údajov, ak takéto porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby.
(2)
Oznámenie podľa odseku 1 musí obsahovať jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov a informácie a opatrenia podľa § 40 ods. 4 písm. b) až d).

(3)
Oznámenie podľa odseku 1 sa nevyžaduje, ak
a)prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a uplatnil ich na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä šifrovanie alebo iné opatrenia, na základe ktorých sú osobné údaje nečitateľné pre osoby, ktoré nie sú oprávnené mať k nim prístup,
b)prevádzkovateľ prijal následné opatrenia na zabezpečenie vysokého rizika porušenia práv dotknutej osoby podľa odseku 1,
c)by to vyžadovalo neprimerané úsilie; prevádzkovateľ je povinný informovať verejnosť alebo prijať iné opatrenie na zabezpečenie toho, že dotknutá osoba bude informovaná rovnako efektívnym spôsobom.
(4)
Ak prevádzkovateľ ešte porušenie ochrany osobných údajov neoznámil dotknutej osobe, úrad môže po zvážení pravdepodobnosti porušenia ochrany osobných údajov vedúceho k vysokému riziku požadovať, aby tak urobil, alebo môže rozhodnúť, že je splnená niektorá z podmienok uvedených v odseku 3.

7 Riadenie dostupnosti

7.1 Všeobecný popis procesu riadenia dostupnosti

Cieľ procesu: Zdokumentovať a udržiavať vhodné plány kontinuity činností (havarijné plány) v závislosti od aktív a hrozieb.

Vstupy do procesu: Bezpečnostný incident, aktíva Obec Okoličná na Ostrove dodávatelia, používatelia.

Výstupy z procesu: Plán kontinuity činností (havarijný plán)

Príčiny neriadenosti: Nedostatočné testovanie plánu, veľmi všeobecný plán, neaktuálny plán, nedostatočné zdroje (pracovníci, aktíva a pod.), nedostatočné identifikovanie zdroja bezpečnostného incidentu, čo môže spôsobiť jeho opätovný vznik, charakter bezpečnostného incidentu, zastaralé alebo nefunkčné zálohovacie alebo archívne médiá, nedostatočne definované role a zodpovednosti.

Monitorovacie kritériá: Rýchlosť reakcie a čas úplnej obnovy do stavu ako pred incidentom, náklady na celkové zvládnutie bezpečnostného incidentu, výskyt neriadených činností v prípade vzniku bezpečnostného incidentu.

Metódy riadenia: Pravidelné testovanie a aktualizovanie plánov obnovy, vzdelávania pracovníkov o možných hrozbách, ich prejavoch a činnostiach, ktoré vedú k stavu obnovy, preskúmavanie záznamov z bezpečnostných incidentov.

Profit z riadeného procesu: Bezpečnostný incident zvládnutý v čo najkratšom čase s minimálnymi následkami s použitím minimálnych zdrojov.

7.2 Definovanie cieľa plánu kontinuity

Cieľ plánu kontinuity činností je vždy závislý od konkrétneho aktíva. Preto je potrebné identifikovať tie, ktoré majú vplyv na základné kvalitatívne kritériá spracúvania osobných údajov. V rámci procesu riadenie bezpečnostných rizík označené ako kritické aktíva.
Každé aktívum môže byť vyradené z činnosti inou hrozbou, čo má vplyv na zadefinovanie celkového plánu (napr. neplnenie požiadaviek aktíva vplyvom jeho krádeže, alebo vplyvom výpadku dodávok elektrickej energie). Preto pre každý typ hrozby, ktorej odstránenie následkov si vyžaduje špecifické služby je potrebné určiť samostatný plán.

7.3 Určenie potrebných pracovníkov a aktív

Aby mohli byť vykonané priebežné opatrenia a opatrenia pre úplnú obnovu, je potrebné definovať:

- Pracovníkov, ktorých zaangažovanosť je nutná.
- Dodávateľov, ktorých je potrebné kontaktovať pre potreby zásahu.
- Náhradné aktíva a ich umiestnenie. V tejto časti tak dochádza k výberu stratégie zabezpečenia náhradného aktíva a to:
    - Dohodou s dodávateľom aktíva, ktorý v prípade vzniku bezpečnostného incidentu v podmienkach prevádzkovateľa zabezpečí v špecifikovanej dobe náhradu aktíva alebo zásah.
    - Záložným aktívom, ktoré prevádzkovateľ zabezpečí nákupom, prenájmom alebo jeho zapožičaním.
    - Zariadením, ktoré je schopné prebrať na seba funkcie a plniť požiadavky poškodeného aktíva.

7.4 Určenie priebežných opatrení

V tejto časti je potrebné (ak si to vyžaduje charakter bezpečnostného incidentu) čo najpodrobnejšie zdokumentovať a chronologicky zoradiť tie činnosti, ktoré:

- je nutné vykonať pre zamedzenie ďalších dôsledkov incidentu,
- je nutné vykonať, aby bola zabezpečená činnosť v núdzovom režime.

Zároveň je potrebné určiť vykonávateľov jednotlivých činností.

7.5 Určenie opatrení pre úplnú obnovu

Následne je nutné v chronologickom poradí zdokumentovať činnosti, ktoré zabezpečia úplnú obnovu tak, ako pred vznikom bezpečnostného incidentu s identifikáciou jednotlivých vykonávateľov činností.

7.6 Určenie vlastníka plánu

Vlastník plánu zodpovedá za aktuálnosť plánu, vedie evidenciu o použití plánu, zodpovedá za testovanie a celkovú praktickú použiteľnosť.

7.7 Testovanie plánu kontinuity

Aby bola zabezpečená trvalá vhodnosť plánu je nutné vykonávať jeho testovanie. Pre každý plán je potrebné určiť interval jeho testovania. Súčasťou je aj:

- testovanie obnovy zo záložných a archívnych médií,
- koordinácia potrebných pracovníkov,
- dostupnosť aktív,
- overenie aktuálnosti.

7.8 Riadenie kontinuity činností v podmienkach Obec Okoličná na Ostrove

S cieľom zabrániť prerušeniu prevádzkových aktivít, ktoré súvisia so spracúvaním osobných údajov, boli špecifikované v časti riadenia aktív tie aktíva, ktoré súvisia a majú vplyv na bezpečnosť osobných údajov.

- **Vlastník aktíva (VA)** je v podmienkach Obec Okoličná na Ostrove

jednotlivec, ktorý zodpovedá za kontrolu, údržbu a bezpečnosť aktíva.
Používateľ (PA) je pracovník resp. oprávnená osoba, ktorý v rámci plnenia svojich pracovných povinností využíva a stará sa o aktívum každý deň. Zodpovednosť zostáva na pleciach vlastníka aktíva.
Aktívum je určené svojím vlastníkom a/alebo používateľom.

7.8.1 Aktívum AI

- Popis aktíva AI: Osobné údaje spracúvané manuálnym spôsobom – výstupné tlačové zostavy obsahujúce osobné údaje (napr. kópie výkazov, výplatné pásky), obchodné zmluvy, pracovné zmluvy, pedagogická agenda a ostatná agenda.

Umiestnenie aktíva AI: Do uzamykateľných skríň v kancelárskych priestoroch;samostatného archívneho priestoru v organizácii.

- Príklady bezpečnostného incidentu: Zničenie písomností, strata, krádež, úmyselné – neúmyselné poškodenie.
- Povinnosti vlastníka aktíva: vlastník aktíva zodpovedá za manipuláciu s aktívom; vedie evidenciu a zoznam zakladačov (proces riadenie aktív) dohliada nad vyraďovaním záznamov v súlade s osobitným zákonom;
- Povinnosti používateľov: oprávnené osoby – používatelia sú povinné postupovať v súlade so zdokumentovanými bezpečnostnými opatreniami;
- Činnosti v prípade bezpečnostného incidentu: V prípade zistenia neobvyklej situácie alebo vzniku bezpečnostného incidentu (napríklad strata, poškodenie, krádež a pod.) používateľ o ňom neodkladne informuje vlastníka aktíva (v prípade jeho neprítomnosti svojho priameho nadriadeného); tento navrhne nápravné opatrenia a ďalší postup v súlade s bezpečnostným opatrením riadenia bezpečnostných incidentov.

7.8.2 Aktívum AII a AIII

- Popis aktíva AII: procesy a služby – technické služby podporujúce spracovanie osobných údajov ako napr. vykurovanie, dodávky elektrickej energie.
- Popis aktíva AIII: procesy a služby – technické služby podporujúce spracovanie osobných údajov – komunikačné služby – dátové služby, hlasové služby, mobilná komunikácia.
- Umiestnenie aktív: Nakoľko ide o podporné služby, tieto sú súčasťou kancelárskych priestorov organizácie.
- Príklady bezpečnostného incidentu: výpadok/strata podporných služieb; škody spôsobené tretími stranami; hurikán; zásah bleskom; chyba údržby; kolísavosť elektrickej energie; porušenie zmluvných záväzkov; úmyselné poškodenie;
- Povinnosti používateľov: Oprávnené osoby – používatelia sú povinné postupovať v súlade so zdokumentovanými bezpečnostnými opatreniami a pri svojej práci chrániť majetok organizácie;
- Činnosti v prípade bezpečnostného incidentu: V prípade, ak výpadok služby nebol zo strany dodávateľa avizovaný, oprávnená osoba telefonicky kontaktuje dodávateľa s cieľom zistenia dôvodu nedostupnosti a doby nedostupnosti podpornej služby. O zisteniach neodkladne informuje priameho nadriadeného, ktorý navrhne následný postup.

Dodávaná služba	Názov organizácie	Telefonický kontakt	e-mailový kontakt
Elektrická energia			
Dodávky tepla			
Pripojenie do siete internet			
Služby mobilnej komunikácie			

7.8.3 Aktívum AIV

- Popis aktíva AIV: (software): operačný systém, aplikačný softvér, antivírový softvér, softvér zabezpečujúci PC pred neoprávneným vstupom zo siete internet
- Umiestnenie aktíva AIV: Aktíva sú umiestnené v kancelárskych priestoroch (súčasť stolových počítačov, notebookov a pod.)
- Príklady bezpečnostného incidentu: prezradenie hesiel; odpočúvanie; chyby komunikačných služieb; aplikovanie neautorizovaného alebo netestovaného kódu; nelegálne použitie softvéru; chyba údržby; chyba softvéru; neautorizovaný prístup; neautorizovaná alebo neúmyselná modifikácia; použitie sieťových zariadení neautorizovaným spôsobom; použitie softvéru neautorizovanými používateľmi; úmyselné poškodenie;
- Povinnosti používateľov: Oprávnené osoby – používatelia sú povinní postupovať v súlade so zdokumentovanými bezpečnostnými opatreniami a pri svojej práci chrániť majetok prevádzkovateľa.
- Činnosti v prípade bezpečnostného incidentu: V prípade výskytu neočakávaného javu si používateľ okamžite zaznamená typ nedosiahnutej zhody alebo prieniku, vyskytujúcej sa poruchy, správy na obrazovke, typ zvláštneho chodu systému; používateľ nepodniká žiadne nápravné kroky, ale jav resp. udalosť okamžite nahlási svojmu priamemu nadriadenému.
- V prípade jeho neprítomnosti alebo na základe jeho pokynu, je potrebné kontaktovať organizáciu, ktorá zabezpečuje pre prevádzkovateľa údržbu hardvérových a softvérových prostriedkov, prípadne interného pracovníka zodpovedného za údržbu a servis HD a SW.

V prípade napadnutia škodlivými kódmi:
Ak sa s PC pracovať dá, po zachytení škodlivého kódu je potrebné pristúpiť ihneď k riešeniu:

- spustenie hĺbkovej kontroly antivírovým softvérom,
- liečenie alebo vymazanie vírusu,
- reštartovanie operačného systému,
- identifikovanie zdroja škodlivého kódu a vykonanie jeho eliminácie,
- vykonanie opätovnej hĺbkovej antivírusovej kontroly.

V prípade poškodenia databáz:

- reštartovanie aplikácie,
- preskúmanie chybového hlásenia,
- obnovenie databázy zo zálohy v prípade veľkého poškodenia,
- opätovné spustenie aplikácie a kontrola databázy.

V prípade poškodenie aplikácie:

- zmazanie alebo odinštalovanie aplikácie,
- reštart počítača,
- inštalácia aplikácie,
- overenie funkčnosti.

7.8.4 Aktívum AV

- Popis aktíva AV: (fyzické položky): počítače, server a pod.
- Umiestnenie aktíva AV: Aktíva AV sú umiestnené v kancelárskych priestoroch organizácie.
- Príklady bezpečnostného incidentu: škody spôsobené tretími stranami; požiar; povodeň; poškodenie vodou; chyba hardvéru; zásah bleskom; chyba údržby; kolísavosť elektrickej energie; krádež; neautorizovaný fyzický prístup; vandalizmus; úmyselné poškodenie;
- Povinnosti vlastníka aktíva:

a) vlastník aktíva zodpovedá za manipuláciu s aktívami v súlade so zdokumentovanými bezpečnostnými opatreniami;

b) vlastník aktíva je povinný dbať na to, aby obstarávaný softvér, ktorý bude inštalovaný na aktíva bol obstaraný prostredníctvom známych a renomovaných zdrojov, aby sa predišlo porušeniu autorských práv;

c) vlastník aktíva vedie zoznam, kde sú identifikované všetky aktíva AV s požiadavkou na ochranu práv duševného vlastníctva;

d) vlastník aktíva udržuje dôkazy a údaje o vlastníctve licencií, originálnych inštalácií, manuálov a pod. v aktívach AV

e) vlastník aktíva vedie evidenciu používateľov aktív AV

f) vlastník aktíva vykonáva, alebo zabezpečí vykonanie kontroly, že sú inštalované len softvéry a licencované produkty; o výsledkoch kontroly vykoná písomný záznam;

g) vlastník aktíva príjme, alebo zabezpečí prijatie takých opatrení, ktoré zabránia vytváraniu kópií softvéru a jeho používanie bude v súlade s autorským právom;

- Povinnosti používateľov: Oprávnené osoby – používatelia sú povinné postupovať v súlade so zdokumentovanými bezpečnostnými opatreniami.
- Činnosti v prípade bezpečnostného incidentu:

Server – hardvérová chyba

1. zistenie chybného komponentu
2. jeho výmena za nový

A:

A 1) inštalácia nového ovládača k danému komponentu

A 2) reštart systému

B:

B 1) inštalácia operačného systému servera

B2) iniciovanie konfiguračného CD

B3) inštalácia DB

3. alternatívne kontaktovať dodávateľskú organizáciu zabezpečujúcu služby údržby HW a SW.

PC – hardvérová chyba

1. kontrola korektného zapojenia kabeláže
2. zistiť, čo pravdepodobne spôsobuje poruchu prvku a kontaktovať svojho nadriadeného, pripadne pracovníka zodpovedného za údržbu HW a SW
3. alternatívne kontaktovať dodávateľskú organizáciu zabezpečujúcu služby údržby HW a SW.

7.8.5 Aktívum AVI

- Popis aktíva AVI: (fyzické položky): Zálohovacie a archívne médiá

Umiestnenie aktíva AVI: Aktíva sú umiestnené v kancelárskych priestoroch organizácie alebo v externých bezpečných miestach určených vedením organizácie.

- Príklady bezpečnostného incidentu: Zničenie záznamov; poškodenie dátových nosičov; prezradenie hesiel; prach; zemetrasenie; požiar; povodeň; zásah bleskom; strata; krádež;

vandalizmus; úmyselné poškodenie.

- Povinnosti vlastníka aktíva:
  a) vlastník aktíva zodpovedá za manipuláciu s aktívami v súlade so zdokumentovanými bezpečnostnými opatreniami;
  b) vlastník aktíva zodpovedá za dodržiavanie politiky zálohovania;
  c) vlastník aktíva vedie dôslednú evidenciu vytvorených záložných a archívnych kópií spolu s označením miesta ich uloženia;
  d) vlastník aktíva zabezpečí pravidelné preverenie funkčnosti kópií;
  e) vlastník aktíva v pravidelných intervaloch vykonáva kontrolu kópií, či nedošlo k ich strate;
  f) vlastník aktíva zabezpečí, aby archívne zálohy boli ukladané v dostatočnej vzdialenosti od hlavného pracoviska, aby unikli akémukoľvek poškodeniu haváriou na hlavnom pracovisku;
  g) vlastník aktíva zabezpečí, aby údaje boli chránené šifrovaním;

d) Povinnosti používateľov: Oprávnené osoby – používatelia sú povinné postupovať v súlade so zdokumentovanými bezpečnostnými opatreniami.

e) Činnosti v prípade bezpečnostného incidentu: V prípade zistenia neobvyklej situácie alebo vzniku bezpečnostného incidentu, používateľ o ňom neodkladne informuje vlastníka aktíva; v prípade jeho neprítomnosti/nedostupnosti svojho priameho nadriadeného. Táto osoba vykoná prešetrenie bezpečnostného incidentu.

8 Proces pre riadenie prevádzky

Proces riadenie prevádzky pozostáva z nasledujúcich subprocesov:

8.1 riadenie zmien,
8.2 zálohovanie a archivovanie,
8.3 údržba zariadení,
8.4 manipulácia s médiami,
8.5 likvidácia aktív.

8.1 Subproces riadenie zmien

8.1.1 Všeobecný popis subprocesu riadenie zmien

Cieľ subprocesu: Pomocou subprocesu riadenie zmien zabezpečiť, aby boli zmeny vykonávané na aktívach tak, aby ich implementáciou nedošlo k ich poškodeniu, či zlyhaniu a v konečnom dôsledku narušeniu dostupnosti, integrity a celkovej bezpečnosti spracúvaných osobných údajov.

Vstupy do subprocesu: Dodávateľom informačného systému (ďalej len ako „IS“) predložená zmena, bezpečnostný incident, zraniteľnosť IS, externé hrozby, likvidácia aktíva, obstaranie nového aktíva.

Výstupy zo subprocesu: Riadené zmeny na aktívach, ktoré zabezpečia plnenie bezpečnostných požiadaviek a ich implementácia neohrozí dostupnosť, integritu a pod..

Príčiny neriadenosti subprocesu: Neoverený zdroj zmeny, nedôslednosť zo strany pracovníka pri nedostatočnom testovaní, nekompetentnosť, automaticky implementovaná zmena.

Monitorovacie kritériá subprocesu: Záznamy o vykonaných zmenách na aktívach, mimoriadne kópie (predpoklad kolízneho stavu IS), trend výskytu bezpečnostných incidentov spôsobených zastaralosťou operačného systému, škodlivými kódmi, prípadne inými vplyvmi, kedy vhodná zmena v IS mohla týmto predchádzať, protokol z mimoriadnej kontrolnej činnosti.

Metódy riadenia subprocesu: Testovanie zamýšľanej zmeny, preverovanie predkladaných zmien, zvažovanie dopadu zmien, mimoriadna kontrolná činnosť.

Profit z riadeného subprocesu: Minimalizácia počtu zmien, ktorých implementácia by mohla spôsobiť

narušenie dostupnosti a integrity a pod., znižovanie nákladov pri odstraňovaní následkov bezpečnostných incidentov spôsobených neriadenými zmenami.

Súvisiace formuláre: nie sú definované.

8.1.2 Riadenie zmien

Prevádzkový softvér

Zmeny prevádzkových knižníc softvéru, aplikácií a programov vykonávavedením organizácie schválený pracovník alebo pracovník externej organizácie. Tento rozhodne o spôsobe zmien (manuálne, automatické) s ohľadom na predmet zmeny. Organizácia vedie presný zoznam tých aktív, na ktorých je nutné vykonávať zmeny. Sú súčasťou procesu riadenie aktív.
Všetky zmeny môžu byť implementované len po dôkladnom zvážení dopadu prípadnej zmeny.

Určený pracovník sleduje:

- výrobcom predkladané zmeny,
- skúsenosti iných používateľov prostredníctvom určených a schválených zdrojov informácií,
- dobu, počas ktorej výrobca garantuje podporu softvéru vo forme aktualizácií.

Pred implementáciou závažnej zmeny je potrebné zabezpečiť uchovanie predošlej verzie s cieľom návratu v prípade zlyhania systému v dôsledku zmeny (mimoriadne zálohy).
Softvérové záplaty (patch) a aktualizácie antivírusového softvéru sú aplikované automaticky, s cieľom zvýšenia bezpečnosti.

Upgrade operačného systému (OS)

Určený pracovník vykoná upgrade OS len vtedy, ak pôvodná verzia nespĺňa požiadavky prevádzkovateľa. Upgrade sa nevykonáva len z dôvodov jeho samotnej existencie bez ďalšieho preskúmania prípadne testovania zmien.

Testovanie zmien

Zmeny nesmú byť testované na kritických aktívach, ani tých aktívach, ktoré obsahujú pre organizáciu citlivé informácie a osobné údaje. Ak by malo dôjsť k testovaniu na takomto aktíve, je potrebné citlivé informácie a osobné údaje z aktíva presunúť alebo bezpečne zlikvidovať. Testovanie vykonáva len určený pracovník. Výsledkom testovania je rozhodnutie či zmenu prijať a implementovať na ďalšie určené aktíva (do procesov) alebo zamietnuť a ponechať pôvodný, nezmenený stav. O zmene je potrebné vždy vykonať záznam.
Pred implementáciou zmeny, ktorá sa týka kritických aktív sa odporúča vykonať mimoriadnu kontrolnú činnosť.

8.2 Subproces zálohovanie a archivovanie

8.2.1 Všeobecný popis subprocesu zálohovanie a archivovanie

Cieľ subprocesu: Pomocou subprocesu zálohovanie a archivovanie zabezpečiť riadené vytváranie kópií z IS tak, aby v prípade vzniku neočakávaného javu, či priamo bezpečnostného incidentu ich použitím bol zabezpečený návrat do stavu, ktorý spĺňa kritérium dostupnosti a integrity.

Vstupy do subprocesu: IS, požiadavka na zmenu IS, pracovníci, dátové nosiče pre vytváranie kópií, prostredie.

Výstupy zo subprocesu: Riadené funkčné kópie.

Príčiny neriadenosti subprocesu: Prostredie, ktoré nespĺňa dostatočné bezpečnostné požiadavky pre uchovávanie kópií, stav dátového nosiča, nespokojný pracovník (aj v prípade externých subjektov), výpadok podporných služieb počas priebehu subprocesu, strata.

Monitorovacie kritériá subprocesu: Záznamy zo subprocesu (dodržiavanie intervalov pre vykonávanie kópií a pod.), počet záznamov o stave systému, kedy jeho obnova nebola možná, nakoľko chýbala funkčná kópia a pod.

Metódy riadenia subprocesu: Aktualizácia subprocesu, pravidelné preverovanie funkčnosti vyhotovených archívnych kópií.

Profit z riadeného subprocesu: Rýchly návrat IS do stavu, kedy spracúvanie osobných údajov spĺňa požiadavku integrity a dostupnosti.

Súvisiace formuláre: nie sú definované

8.2.2 Zálohovanie a archivovanie

Podľa záznamu z procesu riadenie aktív určení pracovníci vykonávajú:

- mimoriadne,
- zálohovacie (nazývané aj ako prevádzkové),
- a archívne kópie.

Intervaly pre vytváranie prevádzkových a archívnych kópií

Mimoriadna kópia je vytváraná vždy, ak sú na aktíve vykonané zmeny, ktoré by mohli spôsobiť narušenie integrity a dostupnosti spracúvania osobných údajov.
Všeobecne podľa spôsobu vytvorenia zálohy pôjde o:

- automaticky alebo manuálne vytvorenú,
- o úplnú alebo rozdielovú zálohu .
- Zodpovedný pracovník určuje typ média, na ktoré budú kópie vyhotovené.

Zabezpečovanie vytvorených kópií

Po vykonaní kópie, v prípade ak jej predmetom sú pre organizáciu citlivé informácie, ako aj osobné údaje, je potrebné túto zabezpečiť pred neoprávneným sprístupnením.
Zároveň je potrebné zabezpečiť dostupnosť softvéru, umožňujúceho opätovné obnovenie systému pomocou záložnej a archívnej, či mimoriadnej kópie.

Obnovenie údajov

Pre potreby obnovy údajov informačných systémov zo záložných, archívnych, či mimoriadnych kópií zodpovedný pracovník definuje pre každé jemu zverené aktívum plán obnovy.

Označovanie vytvorených kópií a evidencia

Pracovník označí novovytvorenú kópiu spôsobom, ktorý zabezpečí jej rýchlu a jednoznačnú identifikáciu v systéme. Ak aplikácia ponúkne možnosť automatického označenia kópie, pracovník môže potvrdiť túto možnosť. Kópiu uloží do určenej zložky.
V prípade archívnych kópií pracovník vyhotoví záznam o jej vytvorení.

Preverovanie funkčnosti

Pracovník, zodpovedný za vytváranie archívnych kópií zabezpečí pravidelné preverenie v intervaloch jedenkrát za rok. O výsledkoch preskúšania vyhotoví písomný záznam. V prípade, že niektoré médium bolo poškodené, zabezpečí vyhotovenie funkčnej kópie tak, aby v prípade potreby bola možná obnova funkčnosti informačného systému.

Likvidácia
Archívne alebo zálohovacie kópie, ktoré boli poškodené, alebo bol ukončený účel spracúvania údajov, ktoré obsahuje, určený pracovník bezpečne a spoľahlivo zlikviduje (tak, aby nebolo možné dáta akýmkoľvek spôsobom znova obnoviť). Použije pri tom špeciálny, na to určený schválený softvér alebo mechanické poškodenie dátového nosiča.

8.3 Subproces údržba zariadení

8.3.1 Všeobecný popis subprocesu údržba zariadení

Cieľ subprocesu: Pomocou subprocesu údržba zariadení zabezpečiť, aby aktíva
Obec Okoličná na Ostrove boli správne udržiavané.
Vstupy do subprocesu: Aktíva, pracovníci, prostredie, bezpečnostný incident.

Výstupy zo subprocesu: Záznam o vykonanej pravidelnej preventívnej údržbe, záznam o vyradení zariadenia, funkčné požiadavky spĺňajúce zariadenie. Príčiny neriadenosti subprocesu: Nedodržiavanie intervalov pre vykonanie preventívnej údržby, nekompetentnosť pracovníkov, nedôslednosť vykonanej údržby, nedostatočné zdroje organizácie. Monitorovacie kritériá subprocesu: Bezpečnostné incidenty spôsobené poruchou zariadenia, výška nákladov vynaložených na údržbu (externé subjekty), doba bezporuchovej prevádzky zariadenia. Metódy riadenia subprocesu: Preventívne údržby vykonávané v určených intervaloch, vzdelávanie pracovníkov.

Profit z riadeného subprocesu: Minimalizácia nákladov na opravu zariadenia, minimalizácia bezpečnostných incidentov spôsobených poruchou zariadenia, predchádzanie vzniku bezpečnostných incidentov.

Súvisiace formuláre:

- záznam o údržbe technického zariadenia,
- záznam o premiestnení aktíva za účelom údržby alebo opravy.

8.3.2 Údržba zariadení

Ku všetkým obstaraným technickým zariadeniam (aktívam) je potrebné uchovávať sprievodnú dokumentáciu týkajúcu sa okrem iného aj výrobcom odporúčaných servisných intervalov. Sprievodná dokumentácia je ukladaná u vedúceho zamestnanca. V elektronickej podobe je súčasťou aplikácie. V súlade s ňou určení pracovníci organizácie, prípadne autorizovaný personál (v závislosti od aktíva, zmluvných podmienok a pod.) vykonávajú preventívnu údržbu zariadení.

Záznam o údržbe
Ku každému takto udržiavanému aktívu prevádzkovateľ vedie záznam. Záznam obsahuje:

- úplný názov, inventárne označenie zariadenia a dátum obstarania,
- umiestnenia (adresa, poschodie, kancelária, prípadne iný podrobný popis),
- predpokladaný termín (prípadne interval) vykonávania preventívnej údržby,
- kto zodpovedá za vykonanie údržby (aj v prípade externých subjektov),
- zoznam o všetkých predpokladaných poruchách, ktoré môžu na zariadení nastať,
- popis činností, ktoré je potrebné minimálne na zariadení vykonať (formulár s názvom „záznam o údržbe technického zariadenia“).

Základné činnosti údržby
Medzi tieto činnosti patrí:

- audio – vizuálna obhliadka zariadenia,
- odstránenie prachu zvnútra zariadenia,

- kontrola pohyblivých častí,
- kontrola inštalovaného softvéru a jeho preverenie podľa konkrétneho preberacieho protokolu.

Pri záložných zdrojoch (UPS):

- Kontrola kapacity batérií.
- Po ich výmene kalibrácia. Kalibrácia je vykonávaná v intervaloch určených dokumentáciou výrobcu.

Následne pracovník zodpovedný za vykonanie údržby zaznamená:

- dátum vykonania údržby,
- popis činností vykonaných na zariadení,
- záznam o poruche, ak nastala,
- podpis pracovníka, ktorý údržbu vykonal.

Premiestnenie aktíva z dôvodu údržby alebo opravy

Ak aktívum obsahuje osobné údaje, tieto je potrebné v prípade, ak sa o ich údržbu stará externý subjekt zlikvidovať alebo riziko súvisiace s prístupom k nim premietnuť do zmluvných podmienok medzi Obec Okoličná na Ostrove a externým subjektom.

Ak je potrebné zariadenie premiestniť (prevziať mimo obvyklých priestorov) za účelom údržby/opravy, ktorú nie je možné vykonať priamo na mieste, určený pracovník o tomto vykoná záznam. V zázname uvedie:

- dátum,
- dôvod premiestnenia,
- predpokladané činnosti, ktoré budú na zariadení vykonané,
- predpokladaný dátum vrátenia zariadenia,
- v prípade, ak zariadenie obsahuje citlivé informácie je potrebné preveriť, či externý subjekt na základe zmluvy má oprávnenie toto zariadenie prevziať,
- ak je zariadenie nahradené iným, uvedie sa jeho názov a typ, prípadne ďalšie podmienky jeho používania (formulár s názvom „záznam o premiestnení aktíva za účelom údržby alebo opravy“).

Vo všetkých prípadoch, žiadnou z činností, ktorá bude vykonaná na zariadení, nesmie dôjsť k porušeniu záručných, poistných alebo iných zmluvných podmienok.

8.4 Subproces manipulácia s médiami

8.4.1 Všeobecný popis subprocesu manipulácia s médiami

Cieľ subprocesu: Pomocou subprocesu manipulácia s médiami zabezpečiť ochranu informácií, ako aj osobných údajov a chrániť ich pred poškodením, neoprávneným sprístupnením a pod.

Vstupy do subprocesu: Prevádzkové a archívne médiá.

Výstupy zo subprocesu: Riadené používanie médií.

Príčiny neriadenosti subprocesu: Médium, ktoré nebolo schválené, nedodržiavanie požiadaviek na bezpečné uloženie, používanie médií pre súkromné účely, nekompetentnosť pracovníkov, škodlivý kód, strata, krádež či iný bezpečnostný incident.

Monitorovacie kritériá subprocesu: Riadený inventárny záznam o aktívach

Metódy riadenia subprocesu: Schvaľovanie používania určeným pracovníkom, poučenie pracovníkov o používaní aktíva, kontroly používania aktív.

Profit z riadeného subprocesu: Ochrana aktíva a s tým súvisiacich informácií.

Súvisiace formuláre: nie sú definované.

8.4.2 Riadenie subprocesu manipulácia s médiami

Všetky aktíva prevádzkovateľa, ako aj médiá musia byť riadené a súčasťou inventárneho zoznamu. Zaradenie média do používania schvaľuje určený pracovník, ktorý tiež dbá na to:

- aby počet aktív bol primeraný požiadavkám jednotlivých procesov a nedochádzalo tak k nadbytočnosti a zvyšovaniu rizika straty, či neoprávneného sprístupnenia osobných údajov, ktoré sú aktívom uchovávané (udržiavanie minimálneho počtu aktív)
- či je médium spoľahlivé, či bude vyhovovať očakávaným požiadavkám
- či neobsahuje škodlivý kód (ako aj následné pravidelné preverovanie)
- aby citlivé informácie, ako aj osobné údaje, ktoré sú alebo budú predmetom aktíva, boli chránené pred neoprávneným sprístupnením
- aby pracovníci, ktorým je aktívum zverené boli poučení o jeho používaní aj s ohľadom na bezpečnostné hrozby týkajúce sa daného typu aktíva.

Priebežné revidovanie záznamov

Údaje, ktoré sú zaznamenávané na opakovateľne používané médiá musia byť priebežne revidované. V prípade, ak už nie sú potrebné, musia byť bezpečne zlikvidované. Za priebežnú likvidáciu zodpovedá pracovník, ktorému bolo aktívum zverené.
Na médiá môžu byť zaznamenané len tie údaje, ktoré súvisia s výkonom pracovných povinností pracovníka.

Používanie médií mimo priestorov organizácie

Informácia o všetkých prenosných médiách, ktoré sú vynášané mimo priestorov
Obec Okoličná na Ostrove musí byť súčasťou inventárneho záznamu.
Prevádzkové a archívne médiá je potrebné ukladať do zabezpečených priestorov a zabezpečených objektov. V prípade archívnych kópií a súvisiacich médií je potrebné zabezpečiť ich uloženie tak, aby neboli ukladané spolu.
Médiá môžu byť pripájané len k povoleným a schváleným aktívam.

8.5 Subproces likvidácia aktív

8.5.1 Všeobecný popis subprocesu likvidácia aktív

Cieľ subprocesu: Pomocou subprocesu likvidácia aktív zabezpečiť bezpečný spôsob likvidácie údajov ešte pred vyradením, predchádzanie možnosti neoprávneného sprístupnenia a dodržiavanie legislatívnych požiadaviek v prípade dodržiavania lehôt uloženia.

Vstupy do subprocesu: Prevádzkové a archívne médiá, technické zariadenia, ktoré neplnia požiadavky, ktoré sa od nich očakávajú, spracúvané údaje.

Výstupy zo subprocesu: Likvidácia údajov tak, aby nedošlo k ich opätovnému obnoveniu, zneužitiu, neoprávnenému sprístupneniu, záznam o vyradení aktíva.

Príčiny neriadenosti subprocesu: Nedodržiavanie lehôt uloženia, nedodržiavanie spôsobov likvidácie, nepreverenie aktíva, či neobsahuje citlivé údaje pred jeho odovzdaním alebo sprístupnením tretej strane (externému subjektu), príjemcovi, nedostatočné zmluvné ošetrenia vo vzťahu k tretím stranám a ich prístupu k citlivým informáciám prevádzkovateľa.

Monitorovacie kritériá subprocesu: Riadený inventárny záznam o aktívach, kontroly používaných aktív, bezpečnostné incidenty spôsobené neoprávneným sprístupnením citlivých údajov.

Metódy riadenia subprocesu: Využívanie bezpečného spôsobu likvidácie skartovacími strojmi a bezpečnostnými aplikáciami, poučenie pracovníkov o likvidácii a súvisiacich hrozbách.

Profit z riadeného subprocesu: Ochrana aktíva organizácie a s tým súvisiacich osobných údajov.

Súvisiace formuláre: nie sú definované.

8.5.2 Likvidácia aktív

Likvidácia je záverečnou fázou aktíva a jej vykonaniu obvykle predchádza subprocesu riadenie zmien.

8.5.2.1 Spôsob likvidácie

Spôsob likvidácie je závislý od typu aktíva a od dôvodu likvidácie:

f) v prípade papierových médií pracovníci k likvidácii povinne používajú skartovacie stroje,

g) v prípade elektronických informácií sú tieto likvidované použitím bezpečných aplikácií špeciálne určených na zmazanie dát, alebo mechanickým poškodením dátového nosiča.

9 Riadenie bezpečnostných rizík

9.1 Všeobecný popis procesu riadenia bezpečnostných rizík

Cieľ procesu: Zavedený proces, ktorý zabezpečí v maximálnej miere identifikovateľnosť hrozieb, ktoré by mohli mať dopad na bezpečnosť spracúvaných osobných údajov.

Vstupy do procesu: Externé prostredie organizácie, nové trendy v oblasti informačných technológií, charakter organizácie, aktíva organizácie, ako aj možné hrozby a ich pravdepodobnosť vzniku, existujúce opatrenia a zraniteľnosti, následky, bezpečnostné incidenty.

Výstupy z procesu: Správa z vykonanej analýzy pre ďalšie preskúmanie, formulované nápravné a preventívne opatrenia, identifikované zraniteľnosti, následky a možné hrozby, výsledná miera rizika.

Príčiny neriadenosti: Nedostatočne zdokumentované bezpečnostné incidenty, nedostatočný odhad hrozieb a následná kvalitatívna analýza, nedostatočná evidencia aktív (neriadené aktíva), neodhadnuté hrozby prostredia, nedostatočná kvalifikačná úroveň pracovníkov, nedostatočná implementácia prijatých nápravných a preventívnych opatrení, nevhodné monitorovacie systémy, nedostatočná interná komunikácia a komunikačné bariéry, nesprávna analýza údajov, nedostatočná podpora a angažovanosť.

Monitorovacie kritériá: Implementované preventívne opatrenia.

Metódy riadenia: Kvalitatívna analýza rizík s následným návrhom preventívnych opatrení.

Profit z riadeného procesu: Klesajúci trend bezpečnostných incidentov, zníženie investícií do následných nápravných opatrení, dobré meno organizácie.

Súvisiace formuláre:

- správa z vykonanej bezpečnostnej analýzy rizík prevádzkovateľa.

9.2 Výklad základných pojmov

- Následok je výsledok udalosti ovplyvňujúci cieľ.
- Opatrenie je zákrok, ktorý upravuje riziko.
- Udalosť je výskyt alebo zmena určitého súboru okolností.
- Úroveň rizika je veľkosť rizika vyjadrená ako kombinácia následkov a ich pravdepodobnosti.
- Pravdepodobnosť je možnosť, že sa niečo stane.
- Zvyškové riziko je riziko, ktoré zostane po ošetrení rizík.
- Riziko je miera neistoty dosiahnutia cieľa.
- Analýza rizika je proces na pochopenie pôvodu rizika a zistenie úrovne rizika.
- Posúdenie rizika je celkový proces identifikácie rizika, analýzy rizika a vyhodnotenie rizika.
- Kritériá rizika sú referenčné hodnoty, podľa ktorých sa hodnotí závažnosť rizík.
- Vyhodnotenie rizika je výsledok porovnania výsledkov analýzy rizík s kritériami rizika na určenie, či riziko alebo jeho hodnota sú prijateľné alebo tolerovateľné.
- Identifikácia rizík je proces vyhľadávania, rozpoznávania a opisovania rizík.
- Riadenie rizík sú koordinované aktivity na riadenie organizácie s ohľadom na riziká.
- Ošetrenie rizík je proces na úpravu rizík.

9.3 Bezpečnostná analýza

Cieľom riadenia rizík je prostredníctvom analýzy rizík vykonať:
a)identifikáciu aktív, nedostupnosťou ktorých dôjde k ohrozeniu kontinuity a bezpečnosti spracúvania osobných údajov,
b)identifikáciu zraniteľných miest systému
c)navrhnúť vhodné opatrenia (preventívneho a nápravného charakteru), prostredníctvom ktorých dôjde k minimalizácii výskytu bezpečnostných incidentov.

Za vykonanie bezpečnostnej analýzy zodpovedá určený pracovník a je vykonávaná:
a) po výskyte závažného bezpečnostného incidentu,
b) v prípade mimoriadnych zmien v procesoch, ktoré by mohli ohroziť bezpečnosť spracúvaných osobných údajov.

9.4 Kvalitatívna bezpečnostná analýza

V podmienkach Obec Okoličná na Ostrove bude implementovaný postup pre vykonanie analýzy kvalitatívnej – kedy táto pre vyjadrenie jednotlivých hodnôt využíva slovné pomenovania.
Kvalitatívna analýza bude vykonaná:
1. identifikáciou rizika,
2. analýzou rizika,
3. vyhodnotením rizika,
4. ošetrením rizika s predložením výsledkov na preskúmanie vedeniu.

9.4.1 Identifikácia rizika

Identifikácia rizika znamená:

- identifikovať aktíva = v tejto časti je potrebné identifikovať všetky tie aktíva, ktoré súvisia so spracúvaním osobných údajov. Identifikácia sa vykonáva fyzickým zisťovaním a inventárnym záznamom z procesu riadenie aktív.
- identifikovať hrozby = v tejto časti bezpečnostnej analýzy je potrebné identifikovať všetky hrozby, ktoré by mohli spôsobiť narušenie základných bezpečnostných požiadaviek na spracúvanie osobných údajov (integrita, dostupnosť, bezpečnosť) a to pre každé aktívum

zvlášť (resp. pre každý typ aktíva zvlášť). Vstupom do tejto časti sú aj:

- a) predpokladané hrozby,
- b) bezpečnostné incidenty, ktoré už v podmienkach organizácie nastali,
- c) vlastníci aktív, procesov a subprocesov.
- identifikovať opatrenia = teda všetky tie opatrenia, ktoré už prevádzkovateľ prijal alebo plánuje prijať s cieľom zníženia pravdepodobnosti akéhokoľvek bezpečnostného incidentu.
- Vstupom do tejto časti sú aj existujúca dokumentácia a záznamy o prijatých a predpokladaných opatreniach.
- identifikovať zraniteľnosti = kde zraniteľnosťou budeme rozumieť slabé miesto v systéme, ktoré by hrozba mohla využiť pre poškodenia (zníženie) kvality spracúvania osobných údajov. Zdrojom zraniteľností môžu v podmienkach prevádzkovateľa byť procesy a subprocesy, pracovníci (aj externí), fyzické prostredie, konfigurácie systémov, hardvér, softvér a komunikačné zariadenia, tretie subjekty (konkurencia, používatelia a pod.).Vstupom do tejto časti sú aj zoznam hrozieb, zoznam aktív organizácie identifikované opatrenia.
- identifikovať následky = znamená definovať možné poškodenia aktív, zlyhania dostupnosti spracúvaných osobných údajov, či iné možné neželané stavy, ktoré by aktivovaním hrozby mohli nastať. Vstupom do tejto časti je aj:
- zoznam aktív,
- zoznam procesov a subprocesov,
- zoznam hrozieb,
- identifikované zraniteľnosti a pod.

9.4.2 Analýza rizika

Analýza rizika znamená:

a) identifikácia kritických aktív = ohodnotenie aktíva podľa kritickosti s ohľadom na jeho dôležitosť pri spracúvaní osobných údajov, pričom organizácia berie do úvahy najmä pôvodnú cenu aktíva a náklady, ktoré vzniknú v dôsledku straty dôvernosti, integrity a dostupnosti ako výsledok bezpečnostného incidentu a pod. Záznam o kritickom aktíve je vedený v dokumentácii procesu riadenia aktív.

b) posúdenie a vyjadrenie následkov = pre vyjadrenie následku vznikom hrozby bude použitá kvalitatívna stupnica, kedy:
   - hodnota 0 bude priradená následkom v prípade veľmi nízkeho porušenia procesov a subprocesov v časti prevádzkovateľa, kedy prevádzkovateľ disponuje dostatočnými zdrojmi pre okamžitú možnosť obnovy bez vplyvu na bezpečnosť spracúvaných osobných údajov.
   - hodnota 1 bude priradená následkom v prípade nízkeho porušenia procesov a subprocesov v časti prevádzkovateľa, kedy obnova vyžaduje dočasné zastavenie časti procesov a subprocesov, čo by mohlo znamenať malé finančné straty.
   - hodnota 2 bude priradená následkom v prípade stredného porušenia, obvykle spôsobeného porušeniami pravidiel bezpečnostnej politiky prevádzkovateľa (napr. zo strany pracovníkov).
   - hodnota 3 bude priradená následkom v prípade vysokého porušenia, ktoré by mohlo znamenať vážne problémy pri dosahovaní cieľov pri spracúvaní osobných údajov, ako aj zastavenie niektorých procesov prevádzkovateľa s dopadom na tretie strany a externé subjekty (klienti, dodávatelia a pod.); tento následok by tiež mohol znamenať čiastočné narušenie dobrého mena prevádzkovateľa.
   - hodnota 4 bude priradená následkom v prípade veľmi vysokého porušenia; následok by mohol znamenať porušenie dobrého mena dlhodobejšieho rázu.

c) posúdenie a vyjadrenie pravdepodobnosti, že hrozba nastane = pre vyjadrenie pravdepodobnosti bude použité päť úrovňové členenie, kedy:
   - hodnota 0 bude priradená pravdepodobnosti v prípade, ak je výskyt hrozby veľmi nízky resp.

veľmi nepravdepodobný

- hodnota 1 bude priradená pravdepodobnosti v prípade, ak v podmienkach prevádzkovateľa zatiaľ k výskytu posudzovanej hrozby nedošlo, ale za istých okolností hrozba nastať môže; vyjadrenie pravdepodobnosti bude ako nízke, resp. nepravdepodobné
- hodnota 2 bude priradená pravdepodobnosti v prípade, ak je možné, že hrozba nastane a v podmienkach prevádzkovateľa už k bezpečnostnému incidentu súvisiacemu s výskytom posudzovanej hrozby došlo; vyjadrenie pravdepodobnosti bude ako stredné, resp. možné
- hodnota 3 bude priradená pravdepodobnosti v prípade, ak bezpečnostný incident v podmienkach prevádzkovateľa vplyvom hrozby zaznamenal častý výskyt; pravdepodobnosť bude vyjadrená ako vysoká, resp. pravdepodobná
- hodnota 4 bude priradená pravdepodobnosti v prípade, ak bezpečnostný incident v podmienkach prevádzkovateľa vplyvom hrozby je pravidelný a opakujúci sa; pravdepodobnosť bude ako veľmi vysoká, resp. častá

d) určenie rizika zvolenou metódou = výsledné riziko vyhodnotíme na základe matice. Riziková stupnica bude vyjadrená nasledovne:

- nízke riziko: 0 – 2,
- stredné riziko: 3 – 5,
- vysoké riziko: 6 – 8.

matica pre určenie rizika	Vyjadrenie pravdepodobnosti	Veľmi nízka Veľmi nepravdepodobné	Nízka (nepravdepodobné)	Stredná (možné)	Vysoká (pravdepodobné)	Veľmi vysoká (častá)
Vyjadrenie následkov	Veľmi nízky (0)	0	1	2	3	4
	Nízky (1)	1	2	3	4	5
	Stredný (2)	2	3	4	5	6
	Vysoký (3)	3	4	5	6	7
	Veľmi vysoký (4)	4	5	6	7	8

9.4.3 Vyhodnotenie rizika

V tejto fáze dôjde k zoradeniu identifikovaných a posudzovaných hrozieb podľa vyhodnotenej miery rizika, ako aj zvyškových rizík.

9.4.4 Ošetrenie rizika

Podľa zoradeného zoznamu je potrebné rozhodnúť o tom, akým spôsobom dôjde k úprave rizík. Prevádzkovateľom určený pracovník vypracuje správu, v ktorej okrem vyhodnotenia rizika:

- navrhne možné preventívne a nápravné opatrenia (napríklad ako formulácia bezpečnostných cieľov)
- prípadne spôsob, ako by mohlo dôjsť k prenosu rizika či vyhnutiu sa riziku (formulár s názvom „správa z vykonanej bezpečnostnej analýzy rizík“).