1. Bezpečnostné opatrenia

1. 1 Technické opatrenia - navrhované a realizované v podmienkach prevádzkovateľa

1.1.1 Technické opatrenia realizované prostriedkami fyzickej povahy

1.1.1.1 Zabezpečenie objektu pomocou mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov musia byť realizované pomocou bezpečnostných mreží a bezpečnostných zámkov na vstupných dverách, resp. elektronickým zabezpečovacím systémom a elektronickou požiarnou signalizáciou. Týmto zabezpečením vznikne „chránený priestor“ pre prevádzku IS.

V podmienkach prevádzkovateľa je opatrenie zrealizované a pravidelne sa preveruje funkčnosť prostriedkov zabezpečenia.

1.1.1.2 Chránený priestor IS, ktorý je zabezpečený mechanickými a technickými prostriedkami zabezpečenia musí byť oddelený od nechráneného priestoru stavebnou zábranou, teda stenou, mrežou, priehradkou a pod.)

V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že chránené priestory IS sú v uzavretých a uzamykateľných kanceláriách, v ktorých vnútri sú od nechráneného priestoru oddelené priehradkou.

1.1.1.3 IS môže byť fyzicky umiestnený výhradne v chránenom priestore tak, aby bol k nemu zamedzený prístup zo strany neoprávnených osôb.

V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že všetky IS sú prevádzkované v uzavretých a uzamykateľných kanceláriách, ktoré sú od nechráneného priestoru oddelené priehradkou za ktorú nemajú prístup neoprávnené osoby, resp. ho majú len v sprievode a pod kontrolou príslušnej oprávnenej osoby.

1.1.1.4 Fyzické nosiče osobných údajov ,(listinné dokumenty, elektromagnetické a elektronické nosiče – diskety, USB pamäte, CD, DVD, Blu-ray disky, prenosné externé pevné disky, elektronické úložiska údajov – sieťové NAS systémy a pod.), musia byť uložené v chránených priestoroch v uzamykateľných skriniach, alebo trezoroch a to na odlišnom mieste od miesta prevádzky IS.

V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že fyzické nosiče osobných údajov – teda pamäťové média na ktoré boli formou zálohovania dát IS nahrané dáta obsahujúce osobné údaje, sú evidované podľa jednotlivých IS a dátumu vykonania zálohy, v uzamykateľnej skrini na samostatnom mieste ktoré je chráneným priestorom.

1.1.1.5 Zobrazovacie jednotky hardwarových komponentov , (monitory, LCD , TV-výstupy) musia byť v chránenom priestore natočené tak, aby sa zamedzilo aj náhodnému odpozeraniu osobných údajov z poza stavebnej zábrany neoprávnenou osobou. Rovnako aj dočasné pokladanie listinných dokumentov v chránenom priestore pri ich spracovávaní, alebo pred ich archiváciou, či skartovaním môže byť vykonávané iba tak, aby bolo vylúčené, čo i len náhodné odpozeranie osobných údajov, ktoré obsahujú.

V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že všetky zobrazovacie jednotky technických prostriedkov IS sú orientované

tak, aby nebolo možné vidieť nimi zobrazovaný obsah zo strany nechráneného priestoru oddeleného pultovou priehradkou.

1.1.1.6 Prevádzkovateľ IS musí disponovať v rámci chráneného priestoru aspoň jedným zariadením na skartovanie listinných dokumentov a byť preukázateľne schopný likvidovať jednorazové fyzické nosiče osobných údajov (diskety, CD, DVD, Blu-ray disky a pod.)
V podmienkach prevádzkovateľa je opatrenie zrealizované skartovačom.

1.1.2 Ochrana pred neoprávneným prístupom

1.1.2.1 Fyzické nosiče osobných údajov ako sú listinné dokumenty, tlačové zostavy a pod. prevádzkovateľ musí ukladať v zabezpečenom priestore tak, aby sa k nim zamedzil prístup neoprávnených osôb.
V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že sú fyzické nosiče osobných údajov ukladané v chránenom priestore v uzamykateľných skriniach.

1.1.2.2 Prístupu tretích strán k IS musí byť zamedzené v najväčšej možnej miere a pre odôvodnenú potrebu takéhoto prístupu musia byť jasne stanovené, prehľadné a kontrolovateľné pravidlá.
V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že všetky IS sú prevádzkované v uzavretých a uzamykateľných kanceláriách, ktoré sú od nechráneného priestoru oddelené priehradkou za ktorú nemajú prístup neoprávnené osoby, resp. ho majú len v sprievode a pod kontrolou príslušnej oprávnenej osoby.

1.1.3 Riadenie prístupu oprávnených osôb

1.1.3.1 Oprávnené osoby pre prístup k IS, resp. k spracovávaniu osobných údajov v IS musia mať pred samotným prístupom k IS zabezpečenú :

- identifikáciu - jednoznačné identifikovanie oprávnenej osoby pomocou identifikátora (napr. identifikačného kľúča zvereného oprávnenej osobe, resp. uloženého na GRID karte alebo elektronickom zariadení – „token“).
- autentizáciu - overenie identity jedinečným príznakom, osobné heslo, osobný certifikát vystavený na konkrétnu osobu
- autorizáciu – povolenie prístupu, alebo iného procesu vykonávaného v IS na základe identifikácie, resp. autentizácie.

V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že všetky IS, v ktorých sú osobné údaje spracovávané automatizovaným, alebo poloautomatizovaným spôsobom v elektronickej forme pomocou technických prostriedkov IS (počítačov – staníc PC) sa vyžaduje prístupové heslo pri zapnutí stanice PC a pri spustení softwarového komponentu IS. Pre vzdialený prístup k IS JISHM a jeho softwarovému komponentu „EPSIS“ prostredníctvom siete Internet, resp. k IS Schránka ÚPVS sa využíva bezpečnostný certifikát uložený

v elektronickom identifikačnom zariadení – „token“ (eID karta-OP, resp. MQC).

1.1.3.2 Softwarový komponent IS musí zaznamenávať všetky vstupy (log in) a ukončenia vstupov (log out) oprávnenej osoby do IS a do záznamu doplniť časový údaj.
V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že pre IS, v ktorých sú osobné údaje spracovávané automatizovaným spôsobom túto funkcionalitu zabezpečuje softwarový komponent IS.

1.1.4 Ochrana proti škodlivému kódu

1.1.4.1 Ochrana proti škodlivému kódu pri automatizovanom alebo polo automatizovanom spracovávaní osobných údajov v IS na stanici PC musí byť zabezpečená pomocou antivírusového a antispamového programu, ktorý bude detekovať a zneškodňovať škodlivý kód :
- v rámci stanice PC,
- v súboroch prijímaných v rámci verejnej počítačovej siete (internet),
- v súboroch prijímaných v rámci lokálnej počítačovej siete prevádzkovateľa (LAN),
- v súboroch z elektronickej pošty,
- v súboroch na nosičoch dát)

V podmienkach prevádzkovateľa je opatrenie zrealizované nainštalovaním antivírusového software.

1.1.4.2 Ochrana pred nevyžiadanou poštou, (SPAM), musí byť zabezpečená pomocou antivírusového a antispamového programu, ktorý bude detegovať nevyžiadanú poštu v poštovom klientovi, (Outlook, Outlook Express, a pod.), na základe tzv. čiernej listiny, teda zoznamu nežiaducich odosielateľov a poštových rozosielacích robotov. Tento zoznam bude interaktívne dopĺňaný na základe aktualizácie znalostnej knižnice výrobcu antispamového programu ako aj na základe rozhodnutí oprávnenej osoby – príjemcu pošty.
V podmienkach prevádzkovateľa je opatrenie zrealizované nainštalovaním antivírusového software.

1.1.4.3 Oprávnené osoby môžu na staniciach PC v rámci svojich oprávnení používať výhradne legálne a prevádzkovateľom schválené softwarové komponenty IS. Nie je prípustné používanie akéhokoľvek software nainštalovaného z prenosných nosičov dát, stiahnutých z verejne prístupnej, alebo lokálnej počítačovej siete bez súhlasu prevádzkovateľa.
V podmienkach prevádzkovateľa je opatrenie zrealizované upozornením príslušných oprávnených osôb (používateľov IS) na neprípustnosť používania nelegálneho a prevádzkovateľom neschváleného software. Dodržiavanie opatrenia sa kontroluje zo strany správcu aktív prevádzkovateľa pravidelne 1 krát za mesiac, zo strany zodpovednej osoby 1x ročne. O kontrolách sa vykonajú záznamy v dokumentácii.

1.1.4.4 Pre sťahovanie súborov z verejne prístupnej počítačovej siete (internetu) musia byť prevádzkovateľom stanovené a všetkými oprávnenými osobami dodržiavané pravidlá tak, aby boli sťahované iba súbory potrebné pre udržanie funkcionality softwarových komponentov IS, (aktualizácie aplikačných programov a ich databáz).

Taktiež je nevyhnutné zabezpečiť plnú účinnosť ochrany poskytovanej firewallom, predovšetkým realizovať opatrenia zaisťujúce, že všetka komunikácia bude vedená výlučne cez firewall a nebudú vytvorené podmienky pre obchádzanie tohto pravidla.
V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že potrebné aktualizácie si za podmienky pripojenia stanice PC k sieti internet vykonávajú softwarové komponenty IS automatizovane. Zo siete internet je zakázané sťahovať dáta , ktoré nesúvisia s náplňou práce oprávnených osôb v príslušných IS. Komunikácia je zabezpečená cez firewall, ktorý je súčasťou nainštalovaného antivírusového software.

1.1.5 Sieťová bezpečnosť

1.1.5.1 Prevádzkovateľ musí zabezpečiť kontrolu, obmedzenie, alebo zamedzenie možnosti prepojenia IS v ktorom sú spracúvané osobné údaje s verejne prístupnou sieťou, (internet). V konkrétnom prípade prevádzkovateľa je nevyhnutné zabezpečiť obmedzenia prístupu a ich kontrolu prostredníctvom firewall. alebo nastavení sieťovej komunikácie v rámci antivírusového programu tým, že prístup k zvoleným internetovým doménam, alebo FTP serverom bude zakázaný.
V podmienkach prevádzkovateľa je opatrenie zrealizované používaním firewall, ktorý je súčasťou nainštalovaného antivírusového software.

1.1.5.2 Prevádzkovateľ musí evidovať všetky fyzické body pripojenia k lokálnej a verejne prístupnej počítačovej sieti a vykonať zabezpečenie ochrany pred prístupom prostredníctvom WiFi bez použitia prístupového hesla.
V podmienkach prevádzkovateľa je opatrenie zrealizované používaním chráneného prístupu do bezdrôtovej siete prostredníctvom zaheslovania prístupu šifrovaným kľúčom, resp. „nezviditeľnením“ už pripojených staníc PC prostredníctvom sieťových nastavení a nastavení nainštalovaného antivírusového software.

1.1.5.3 **K ochrane vonkajšieho a vnútorného prostredia počítačovej komunikácie sa využijú prostriedky sieťovej bezpečnosti podľa bodu 1.5.1**

1.1.5.4 Prevádzkovateľ zabezpečí obmedzenia prístupu a ich kontrolu podľa bodu 1.5.1 Prostredníctvom firewall a nastavení sieťovej komunikácie v rámci antivírusového programu musí byť zabezpečená ochrana proti tzv. hackerským útokom.

1.1.6 Zálohovanie

Prevádzkovateľ pre zálohovanie a archiváciu údajov a médií musí určiť:
- ktoré údaje podliehajú zákonnej povinnosti ich archivácie, a po akú dobu,
- kto zodpovedá za vytvorenie záložných kópií a údajov informačného systému,
- kto zodpovedá za vytvorenie archívnych kópií a údajov informačného systému,
- intervaly, v ktorých je potrebné vytvoriť záložné, resp. archívne kópie údajov informačného systému,
- zásady pre výber médií pre záložné kópie a pre archívne kópie údajov informačného systému,

- zásady rotácie médií pre záložné kópie údajov (koľko verzií záložných údajov sa uchováva v danom čase),
- odporúčaný, resp. záväzný postup pri vytváraní záložných a archívnych kópií údajov,
- postup pri obnovovaní údajov informačného systému zo záložnej kópie údajov,
- postup pri načítaní údajov z archívnej kópie,
- zásady ochrany záložných a archívnych kópií údajov na mieste ich skladovania (vrátane ochrany počas prenosu na toto miesto),
- zásady pre vyraďovanie nepotrebných alebo poškodených médií a postup likvidácie údajov na vyraďovaných médiách,
- zásady označovania médií so záložnými a archívnymi kópiami údajov a vedenia príslušnej evidencie o používaní archívnych kópií,

1.1.6.1 Test funkcionality nosiča dát, (USB pamäte, CD, DVD, BluRay disky a pod.), sa musí vykonať vždy po vykonaní zálohy dát IS na tento nosič.
V podmienkach prevádzkovateľa je opatrenie zrealizované testom funkcionality oprávnenou osobou, ktorá zálohu vykonala.

1.1.6.2 Prevádzkovateľ musí stanoviť periodicitu vytvárania záložných kópii dát, pričom sa jednotlivé zálohy môžu vytvárať oprávnenými osobami ručne, alebo prostredníctvom špecializovaného programu, pričom sa musí zamedziť neoprávnenému prístupu k dátam záložnej kópie.
V podmienkach prevádzkovateľa je toto zrealizované tak, že záložné kópie sú vykonávané priamo softwarovými komponentmi IS a tieto kópie následne ukladané na dátové nosiče osobných údajov.

1.1.6.3 V zvolenej periodicite musí prevádzkovateľ zabezpečiť vykonanie testu obnovy IS zo záložnej kópie.
V podmienkach prevádzkovateľa je opatrenie zrealizované testom funkcionality IS zo záložnej kópie oprávnenou osobou, ktorá zálohu vykonala.

1.1.6.4 Nosiče dát so záložnými kópiami dát IS musia byť uložené na bezpečnom mieste a to v chránených priestoroch v uzamykateľných skriniach alebo trezoroch, a to na odlišnom mieste od miesta prevádzky IS.
V podmienkach prevádzkovateľa je opatrenie zrealizované tak, že sú nosiče dát s osobnými údajmi ukladané v chránenom priestore v uzamykateľných skriniach.

1.1.7 Likvidácia osobných údajov a dátových nosičov

1.1.7.1 Bezpečné mazanie záložných kópií dát IS z dátových nosičov sa vykoná formou prepisu a formátovania.
V podmienkach prevádzkovateľa je opatrenie zrealizované oprávnenou osobou, ktorá zálohu vykonala.

1.1.7.2 Prípadná likvidácia fyzických nosičov dát sa vykoná skartovačom alebo ručne podľa bodu 3.1.6 týchto opatrení (ničenie fyzických nosičov dát).
V podmienkach prevádzkovateľa je opatrenie zrealizované oprávnenou osobou, ktorá zálohu vykonala.

1.1.8 Aktualizácia operačného systému (OS) a softwarových komponentov IS

1.1.8.1 Prevádzkovateľ zabezpečí na všetkých pracovných staniciach IS, resp. dátovom serveri zapnutie automatických aktualizácií z internetových domén dodávateľov operačného systému a aplikačného programu IS. Prípadne aktualizácie zabezpečí z inštalačných nosičov dát od dodávateľa. V pravidelných intervaloch bude zabezpečená kontrola týchto aktualizácií.
V podmienkach prevádzkovateľa je opatrenie zrealizované správcom informačných technológii.

1.2 Organizačné opatrenia - navrhované a realizované v podmienkach prevádzkovateľa

1.2.1 Personálne opatrenia

1.2.1.1 Prevádzkovateľ, alebo ním určená poverená osoba vykoná oboznámenie poverených oprávnených osôb s bezpečnostnou politikou prevádzkovateľa ešte pred uskutočnením prvej spracovateľskej operácie.
1.2.1.2 Prevádzkovateľ poverením oboznámi oprávnené osoby o ich právach, povinnostiach a zodpovednosti, ktoré vyplývajú z nariadenia GDPR a zo zákona č. 18/2018 Z.z.
1.2.1.3 Poverenie každej oprávnenej osoby bude individuálne s vymedzením osobných údajov, ku ktorým má oprávnená osoba v rámci plnenia si svojich pracovných povinností prístup.
1.2.1.4 Poverenie každej oprávnenej osobe určí postupy pri narábaní s osobnými údajmi.
1.2.1.5 Poverenie každej oprávnenej osobe vymedzí zakázané postupy pri narábaní s osobnými údajmi.
1.2.1.6 Poverenie každej oprávnenej osobe vymedzí zodpovednosti za porušenie GDPR resp. zákona č. 18/2018 Z.z.

1.2.1.7 Poverené oprávnené osoby budú v poverení oboznámené o postupoch spojených s automatizovaným, alebo poloautomatizovaným spracovaním osobných údajov a o súvisiacich právach a povinnostiach oprávnenej osoby v chránenom priestore IS aj mimo neho.
V podmienkach prevádzkovateľa sú opatrenia 3.2.1.1 až 3.2.1.2 zrealizované vykonaním oboznámenia pri poverení, o čom je vyhotovený písomný záznam.

1.2.1.8 Písomné poverenie zodpovednej osoby.
Prevádzkovateľ ako orgán verejnej moci (OVM) opatrenie zrealizuje v zmysle nariadenia GDPR a Zák.č.18/2018 Z.z. povinne a poverí zodpovednú osobu najneskôr ku dňu účinnosti týchto právnych noriem. Poverenú zodpovednú osobu písomne nahlási Úradu na ochranu osobných údajov SR v predpísanom rozsahu.

1.2.1.9 Prevádzkovateľ prostredníctvom osoby, ktorá má podľa organizačnej štruktúry prevádzkovateľa na starosti problematiku ochrany osobných údajov, alebo prostredníctvom zodpovednej osoby oboznámi poverené oprávnené osoby s bezpečnostnou dokumentáciou spracovateľských činností, bezpečnostnými opatreniami na ochranu osobných údajov ako aj smernicou bezpečnostnej politiky.

1.2.1.10 Prevádzkovateľ zabezpečí aj následné vzdelávanie oprávnených osôb v oblasti práva

a informačných technológií.

1.2.1.11 Po ukončení pracovného pomeru oprávnenej osoby prevádzkovateľ zabezpečí ukončenie oprávnenia zamedzením ďalšieho prístupu k osobným údajom a oboznámi oprávnenú osobu o zákonnej, prípadne aj zmluvnej povinnosti mlčanlivosti, ako aj právnych následkoch jej porušenia.

V podmienkach prevádzkovateľa sú opatrenia 2.1.4 až 2.1.6 zrealizované vykonaním oboznámenia pri poverení, o čom je vyhotovený písomný záznam.

1.2.2 Vedenie zoznamu aktív a jeho aktualizácia

1.2.2.1 Prevádzkovateľ vymedzí zoznam aktív IS, vedie jeho evidenciu a zabezpečuje aktualizáciu.

V podmienkach prevádzkovateľa sú základnými aktívami IS obce predovšetkým:

- **osobné údaje, uchovávané a spracovávané v IS obce, v zmysle zachovania ich dôležitých atribútov ako je správnosť, aktuálnosť, integrita, autenticita a dôvernosť,**
- **schopnosť poskytovať bez zbytočného odkladu a v náležitej kvalite a presnosti služby nevyhnutné pre plnenie svojich úloh a úloh organizačných jednotiek v jej pôsobnosti,**
- **schopnosť poskytovať vybrané osobné údaje v náležitej kvalite (aktuálnosť, neporušenosť, autenticita) vybraným externým subjektom, predovšetkým určeným orgánom verejnej správy.**

1.2.3 Riadenie prístupu poverených oprávnených osôb k osobným údajom

1.2.3.1 Prevádzkovateľ zabezpečí kontrolu vstupu do chránených priestorov IS technickými aj personálnymi opatreniami tak, aby sa v chránených priestoroch pohybovali len k tomu poverené oprávnené osoby.

1.2.3.2 Pridelí povereným oprávneným osobám zo strany prevádzkovateľa kľúče od chránených priestorov a bezpečne uložiť rezervné kľúče.

1.2.3.3 Pridelí povereným oprávneným osobám oprávnenia v oblasti automatizovaného spracovávania osobných údajov v rozsahu ich rolí.

<u>prístupové práva</u>

- zásady pre prideľovanie prístupových práv,
- kto je oprávnený prideľovať, upravovať a odnímať prístupové práva oprávnenému používateľovi systému,
- postup pri prideľovaní, zmene či odňatí prístupových práv pracovníkovi – kto, kedy, ako žiada, kto schvaľuje,
- zásady dočasných zmien v pridelených prístupových právach (dôvody, postup, zodpovednosť za včasné ukončenie dočasného pridelenia),
- zásady vedenia evidencie pridelených prístupových práv,

1.2.3.4 Spravovať prístupové heslá k jednotlivým softwarovým komponentom a databázam IS, pridelené príslušným oprávneným osobám, tak aby nedošlo k kompromitácií, alebo strate.

1.2.3.5 Zabezpečiť vzájomnú zastupiteľnosť oprávnených osôb pre prípad práceneschopnosti, alebo rozviazania pracovného pomeru.

V podmienkach prevádzkovateľa sú opatrenia 3.2.3 zrealizované vykonaním oboznámenia pri poverení, o čom je vyhotovený písomný záznam.

1.2.4 Organizácia spracúvania osobných údajov

1.2.4.1 Prevádzkovateľ musí stanoviť pravidlá spracúvania osobných údajov v chránenom priestore.

1.2.4.2 V prípade prítomnosti inej ako poverenej oprávnenej osoby v chránenom priestore IS zabezpečiť nepretržitú prítomnosť oprávnenej osoby , ktorá vykoná dohľad nad ochranou osobných údajov.

1.2.4.3 Prevádzkovateľ musí stanoviť režim upratovania chránených priestorov.

1.2.4.4 Prevádzkovateľ musí stanoviť pravidlá spracúvania osobných údajov pre spracúvanie mimo chránených priestorov.

1.2.4.5 manipulácia s fyzickými nosičmi dát, listinami, fotografiami a pod.

1.2.4.6 manipulácia s prenosnými hardwarovými prostriedkami (NTB, Tablet, a pod) manipulácia s prenosnými dátovými nosičmi

V podmienkach prevádzkovateľa sú opatrenia 3.2.4 zrealizované vykonaním oboznámenia poverenej zodpovednej osoby s bezpečnostnou politikou prevádzkovateľa a hlavnými zásadami pri spracúvaní osobných údajov ako sú:

- zásada zákonnosti,
- zásada obmedzenia účelu,
- zásada minimalizácie osobných údajov,
- zásada správnosti,
- zásada minimalizácie uchovávania,
- zásada integrity a dôvernosti,
- zásada zodpovednosti,

o čom je vyhotovený písomný záznam.

1.2.5 Likvidácia osobných údajov

1.2.5.1 Prevádzkovateľ musí určiť postupy bezpečnej likvidácie listín s osobnými údajmi, bezpečnej elektronickej likvidácie (mazania), resp. pseudonymizácie osobných údajov a fyzickej likvidácie pamäťových nosičov dát. Vymedzí pri tom zodpovednosť jednotlivých oprávnených osôb za túto likvidáciu.

V podmienkach prevádzkovateľa sú opatrenia 3.2.5 zrealizované vykonaním oboznámenia poverenej oprávnenej osoby s bezpečnostnou politikou prevádzkovateľa.

1.2.6 Bezpečnostné incidenty

- priority v prípade ohrozenia prevádzky jednotlivých organizačných útvarov prevádzkovateľa, resp. nutnosti pracovať v redukovanom režime (prerušenie dodávky elektrickej energie, prerušenie komunikačných liniek, poškodenie alebo zničenie kľúčových prvkov informačného systému, vyčerpanie systémových zdrojov, absencia kľúčových pracovníkov),
- "technická" pripravenosť (zabezpečenie náhradných komponentov, zdrojov a komunikačných liniek),
- postup v prípade vyčerpania systémových zdrojov,
- postup v prípade neprítomnosti kľúčových pracovníkov – oprávnené osoby IS,
- postup v prípade živelnej pohromy (napr. požiar, zatopenie),
- testovanie havarijného plánu – intervaly, spôsob,

- spôsob vykonania zmien v havarijnom pláne.

Prevádzkovateľ musí:

- stanoviť postupy pri ohlasovaní bezpečnostných incidentov IS Úradu na ochranu osobných údajov (do 72 hodín) , dotknutým osobám v prípade vysokého rizika dopadu bezpečnostného incidentu na ich práva,
- stanoviť postupy pri ohlasovaní zistených zraniteľných miest v oblasti bezpečnosti ochrany osobných údajov v IS v rámci prevádzkovateľa,
- zabezpečiť evidenciu bezpečnostných incidentov a nápravných opatrení,
- stanoviť postupy pri riešení jednotlivých druhov bezpečnostných incidentov,

- zabezpečiť identifikáciu, evidenciu a odstraňovanie dopadov bezpečnostných incidentov,
- stanoviť postupy pri haváriách a iných mimoriadnych situáciách,
- stanoviť postupy pri poruche, údržbe, alebo oprave hardwarových komponentov IS – teda technických prostriedkov automatizovaného spracovania osobných údajov (napríklad - ochrana osobných údajov na pevnom disku pri oprave počítača). **V podmienkach prevádzkovateľa sú opatrenia 1.2.6 zrealizované vykonaním oboznámenia poverenej zodpovednej osoby s bezpečnostnou politikou prevádzkovateľa.**

1.2.7 Kontrolná činnosť

Systém vnútorných smerníc musí byť členený tak, aby zaistil príslušné usmernenie v oblasti bezpečnosti IS obce pre oprávnené osoby IS obce. Vnútorné smernice musia špecifikovať ich základné povinnosti a činnosti vzhľadom k zaisteniu bezpečnej a spoľahlivej prevádzky IS obce minimálne na nasledovné oblasti:

- identifikácia dôležitých aktív IS v oblasti pôsobnosti používateľa IS obce,
- legislatívne minimum súvisiace s ochranou IS a jeho údajov,
- základné zásady fyzickej a režimovej ochrany,
- zásady správneho používania prostriedkov na overovanie totožnosti,
- základné prevádzkové procedúry používateľa IS, vrátane zásad manipulácie s externými médiami (obzvlášť z cudzích zdrojov) a s výstupmi IS (zostavy, výkresy, …),
- zásady činnosti používateľa IS obce v prípade mimoriadnej udalosti resp. bezpečnostného incidentu.

1.2.7.1 Kontrolná činnosť prevádzkovateľa je zameraná na dodržiavanie smernice a prijatých bezpečnostných opatrení s určením jej formy a periodicity realizácie.

1.2.7.2 Informovanie oprávnených osôb o kontrolnom mechanizme – rozsahu, spôsobu a periodicity uskutočňovania kontroly.

V podmienkach prevádzkovateľa sú opatrenia 1.2.7 zrealizované vykonaním oboznámenia poverenej zodpovednej osoby s bezpečnostnou politikou prevádzkovateľa.

Následne je zo strany prevádzkovateľa v pravidelných intervaloch 1 krát za 3 mesiace, ale tiež náhodne vykonávaná kontrola dodržiavania bezpečnostnej politiky zo strany poverených oprávnených osôb.