DOKUMENTÁCIA BEZPEČNOSTNÝCH OPATRENÍ

NA OCHRANU OSOBNÝCH ÚDAJOV

pri ich spracúvaní prevádzkovateľom

OBEC MAKOV

Vypracovaná vo vzťahu k povinnosti ochrany osobných údajov v zmysle GDPR - Nariadenie Európskeho parlamentu a Rady (EÚ) č. 2016/679 a Zákona 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov pri prevádzke informačných systémov

(2018)

Obsah

Úvod

Obec má ako orgán verejnej moci (OVM) svoje kompetencie zabezpečované jednotlivými referátmi Obecného úradu a ním priamo riadenými organizáciami a zariadeniami. Realizácia ich aktivít je prakticky nemožná bez podpory informačných a komunikačných technológií tvoriacich dôležitú súčasť informačných systémov (ďalej len "IS") obce. Spoľahlivá a správna činnosť IS je teda nevyhnutným predpokladom a základnou požiadavkou pre plnenie úloh samosprávy i preneseného výkonu štátnej správy.

Na značnú časť údajov, ktorou sú osobné údaje fyzických osôb, uchovávaných a spracovávaných v IS prevádzkovateľa:

Obec Makov
Makov č.60, 023 56 Makov
IČO: 00314129
(ďalej len „obec"),

sa s účinnosťou od 25.5.2018 vzťahuje:

- **NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679** z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) – tzv. **GDPR (Global Data Protection Regulation), ktoré je priamo vykonateľným nariadením s územnou pôsobnosťou v priestore Európskej únie a niektorých štátov európskeho hospodárskeho priestoru,** (Island, Nórsko Lichtenštajnsku).

- **Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, ktorého územnou pôsobnosťou je priestor slovenskej republiky.**

Uvedené nariadenie GDPR ako aj Zákon č.18/2018 Z.z. priamo i nepriamo vymedzujú práva fyzických osôb, ktorých osobné údaje sú spracovávané, ako aj práva a povinnosti obce, ako prevádzkovateľa IS obsahujúcich osobné údaje, pričom sa vzťahujú na spracúvanie osobných údajov, vykonávané úplne alebo čiastočne automatizovanými prostriedkami a na spracúvanie inými než automatizovanými prostriedkami v prípade osobných údajov, ktoré tvoria súčasť informačného systému alebo sú určené na to, aby tvorili súčasť informačného systému.

Úlohy ktoré plnia jednotlivé organizačné zložky obecného úradu, si vyžadujú primerané zaistenie dôvernosti, integrity, autenticity a dostupnosti spracovávaných údajov. Správna a spoľahlivá činnosť IS je preto nemysliteľná bez náležitého zaistenia ochrany spracovávaných a uchovávaných údajov, a to ako pred úmyselnými, tak aj neúmyselnými aktivitami a prejavmi vyššej moci.

Na vecnú a technologickú stránku prevádzky rozhodujúcich aplikácií IS obce sa vzťahujú najmä nasledujúce zákony s územnou pôsobnosťou v Slovenskej republike, ako aj k nim príslušné vyhlášky a výnosy:

zákon č. 40/1964 Zb. Občiansky zákonník v znení n. p.,
zákon č. 71/1967 Zb. o správnom konaní v znení n. p.,
zákon č. 50/1976 Zb. o územnom plánovaní a stavebnom poriadku v znení n. p.
zákon č. 105/1990 Zb. o súkromnom podnikaní občanov v znení n. p.,
zákon č. 369/1990 Zb. o obecnom zriadení v znení n. p.,
zákon č. 455/1991 Zb. o živnostenskom podnikaní v znení n. p .,
zákon č. 564/1991 Zb. o obecnej polícii v znení n. p.,
zákon č. 279/1993 Z. z. o školských zariadeniach v znení n. p.,
zákon č. 42/1994 Z. z. o civilnej ochrane obyvateľstva v znení n. p.,
zákon č. 152/1994 Z. z. o sociálnom fonde,
zákon č. 154/1994 Z. z. o matrikách v znení n. p.,
zákon č. 145/1995 Z. z. o správnych poplatkoch v znení n. p.,
zákon č. 162/1995 Z. z. o katastre nehnuteľností a o zápise vlastníckych a iných práv k nehnuteľnostiam v znení n. p.,
zákon č. 253/1998 Z. z. o hlásení pobytu občanov SR a registri obyvateľov SR v znení n. p.,
zákon č. 241/2001 Z. z. o ochrane utajovaných skutočností v znení n. p.,
zákon č. 311/2001 Z. z. Zákonník práce v znení n. p.,
zákon č. 599/2001 Z. z. o osvedčovaní listín a podpisov na listinách obvodnými úradmi a obcami,
zákon č. 282/2002 Z. z., ktorým sa upravujú niektoré podmienky držania psov,
zákon č. 319/2002 Z. z. o obrane SR,
zákon č. 387/2002 Z. z. o riadení štátu v krízových situáciách mimo času vojny a vojnového stavu,
zákon č. 395/2002 Z. z. o archívoch a registratúrach,
zákon č. 431/2002 Z. z. o účtovníctve,
zákon č. 461/2003 Z. z. o sociálnom poistení v znení n. p.,
zákon č. 523/2003 Z. z. o verejnom obstarávaní v znení n. p.,
zákon č. 552/2003 Z. z. o výkone práce vo verejnom záujme,
zákon č. 553/2003 Z. z. o odmeňovaní zamestnancov pri výkone práce vo verejnom záujme v znení n. p.,
zákon č. 596/2003 Z. z. o štátnej správe v školstve a školskej samospráve,
zákon č. 523/2004 Z. z. o rozpočtových pravidlách verejnej správy v znení n. p.,
zákon č. 582/2004 Z. z. o miestnych daniach a miestnom poplatku v znení n. p.,
zákon č. 459/2005 Z. z. o zdravotnom poistení v znení n. p.,
zákon č. 570/2005 Z. z. o brannej povinnosti v znení n. p.,
zákon č. 124/2006 Z. z. o bezpečnosti a ochrane zdravia pri práci v znení n. p.,
zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy v znení n.p.,
zákon č. 448/2008 Z. z. o sociálnych službách v znení n. p.,
zákon č. 8/2009 Z. z. o cestnej premávke v znení n. p.,
zákon č. 563/2009 Z. z. o správe daní (daňový poriadok) v znení n. p.,
zákon č. 571/2009 Z. z. o rodičovskom príspevku v znení n. p.,
zákon č. 9/2010 Z. z. o sťažnostiach v znení n. p.,
zákon č. 546/2010 Z. z.. ktorým sa dopĺňa zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony,
zákon č. 179/2011 Z. z. o hospodárskej mobilizácii,
zákon č. 417/2013 Z. z. o pomoci v hmotnej núdzi v znení n. p.,

zákon č. 485/2013 Z. z. ktorým sa mení a dopĺňa zákon č. 448/2008 Z. z. o sociálnych službách a o zmene a doplnení zákona č. 455/1991 Zb. o živnostenskom podnikaní (živnostenský zákon) v znení neskorších predpisov v znení n. p.
Zákon č. 305/2013 Z.z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente),
Vyhláška MFSR č. 25/2014 Z.z. o integrovaných obslužných miestach a podmienkach ich zriaďovania, označovania, prevádzky a o sadzobníku úhrad.
zákon č. 182/2014 Z. z. o podmienkach výkonu volebného práva v znení n. p.,
zákon č. 124/2015 Z. z., ktorým sa mení a dopĺňa zákon Národnej rady Slovenskej republiky č. 154/1994 Z. z. o matrikách v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony,
zákon č. 126/2015 Z. z. o knižniciach v znení n. p.,

Pri vykonávaní kompetencií stanovených v hore uvedenej legislatíve ako aj v súvisiacich právnych predpisoch je obzvlášť potrebné zabezpečiť bezpečnosť informácií pričom pod bezpečnosťou informácií sa rozumie zachovanie:

- dôvernosti – zaistenie toho, aby informácia bola dostupná iba osobám oprávneným pre prístup,
- integrity – zabezpečenie správnosti a kompletnosti informácií a metód spracovania,
- autenticity – zabezpečenie toho, aby spracovávané údaje boli hodnoverné a pravé
- dostupnosti – zaistenie toho, aby informácie a s nimi späté aktíva boli prístupné autorizovaným užívateľom podľa ich potreby.

Pri zabezpečovaní bezpečnosti informácií, hlavne osobných údajov fyzických osôb, pri ich spracúvaní musia byť dodržané zásady spracúvania definované GDPR ako sú:

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

Rovnako potrebné je zabezpečiť zákonnosť spracúvania v tom zmysle, že osobné údaje možno spracúvať iba ak sa spracúvanie vykonáva na základe aspoň jedného zo zákonom stanoveného zoznamu právnych základov.

Zaistenie bezpečnosti informácií, (hlavne osobných údajov), v IS obce nie je jednorazová záležitosť, ale dlhodobý a systematický proces zameraný na dosiahnutie primeranej úrovne zabezpečenia a následné udržiavanie dosiahnutého stavu, ako aj primerané reagovanie na zmeny v podmienkach a požiadavkách na ich bezpečnosť v IS obce, vyvolané vývojom v oblasti informačných a komunikačných technológií, informačnej bezpečnosti, ako aj zmenami v štruktúre a úlohách obce.

Dlhodobé zaistenie bezpečnosti informácií v IS obce vyžaduje trvalú pozornosť vedenia a všetkých zainteresovaných zložiek, pričom ich bezpečnosť v IS musí byť založená na reálne uskutočniteľných bezpečnostných opatreniach, ktoré sú vhodnou kombináciou bezpečnostných prostriedkov, prevádzkových procedúr, vnútornej legislatívy, administratívnych, organizačných a personálnych opatrení, ako aj opatrení v oblasti kontroly.

Dosiahnutie a udržanie primeranej úrovne bezpečnosti informácií v IS obce závisí nielen od existencie bezpečnostných prostriedkov, ale aj od kvality ich implementácie, správneho použitia na správnom mieste, správneho prevádzkovania a pravidelného overovania ich funkčnosti. Aktuálnu úroveň ich bezpečnosti je potrebné preverovať jednak v pravidelných intervaloch a jednak po výskyte bezpečnostných incidentov.

Cieľom úsilia o zaistenie bezpečnosti IS obce je vytvorenie a prevádzkovanie takého systému, v ktorom je zaistená:

- ochrana informácií, (hlavne osobných údajov), ktoré sú v IS obce spracovávané a uchovávané tak, aby nedošlo k ujme na užitočnosti informácií, ktoré poskytujú, a aby nedošlo k úniku týchto informácií neoprávneným osobám a ich následnému protiprávnemu použitiu,
- poskytovanie služieb IS pre obec a jej klientov v požadovanej kvalite, sortimente a čase, a to aj v prípade značných odchýlok okolia IS od normálneho stavu.

Základným bezpečnostným cieľom pre zaistenie bezpečnosti informácií v IS je predovšetkým:

- predchádzanie vzniku situácií kritických pre činnosť IS v zmysle realizácie vymedzených možných závažných hrozieb pre IS,
- včasné identifikovanie vzniku kritickej situácie,
- v prípade výskytu kritickej situácie minimalizácia vzniknutých škôd a dopadov na funkčnosť IS,
- včasné obnovenie prevádzky (funkčnosti) a požadovaných bezpečnostných parametrov IS a efektívne zotavenie sa z následkov kritickej situácie,
- identifikácia príčin a spôsobu vzniku kritickej situácie, ako aj stanovenie prípadnej osobnej zodpovednosti za vznik kritickej situácie,
- analýza príčin vzniku kritickej situácie a bezodkladné úpravy bezpečnostných opatrení za účelom minimalizácie možnosti jej opakovaného výskytu.

Predpokladané bezpečnostné opatrenia

Systém zaistenia bezpečnosti IS by mal byť tvorený vhodnou kombináciou opatrení nasledovného charakteru:

- odstrašujúce opatrenia, zamerané na to, aby potenciálny protivník upustil od úmyslu viesť cielený útok na IS,
- preventívne opatrenia, zamerané na zabránenie vykonania útoku na IS, resp. na zmenšenie pravdepodobnosti výskytu iných možných hrozieb, vrátane chýb a omylov používateľov IS s dôsledkami na jeho bezpečnosť,
- detekčné a reakčné opatrenia, zamerané na včasné odhalenie príznakov útoku na IS, resp. výskytu udalosti ohrozujúcej IS obce a na rýchle vykonanie vhodných obranných akcií,
- korekčné opatrenia, zamerané na rýchle a podľa možnosti úplné zotavenie sa IS z následkov úspešného útoku či dôsledkov inej udalosti, ktorá ohrozila prevádzku IS.

Prijaté bezpečnostné opatrenia musia byť adekvátne potenciálnym stratám, vzniknutým v dôsledku chýb, omylov, ale aj cieľavedomej činnosti zameranej proti záujmom prevádzkovateľa IS, ako aj stratám vzniknutým v dôsledku pôsobenia vyššej moci. Navyše by mali spĺňať nasledovné požiadavky:

- byť zamerané tak na ochranu pred cieľavedomým útokom "zvonku", ako aj na ochranu pred chybami, omylmi alebo zneužitím pridelených oprávnení používateľmi IS (pod útokom sa rozumie cieľavedomá činnosť osoby alebo skupiny osôb usilujúcich sa poškodiť miestnu samosprávu, alebo získať neoprávnený prospech pre seba alebo pre tretiu stranu),
- zabezpečiť ochranu, minimálne na úrovni včasnej detekcie prekonania existujúcich ochranných bariér, aj pred systematickým a premysleným útokom priemerne až nadpriemerne kvalifikovaného útočníka,
- bezpečnostné opatrenia musia chrániť nielen dôležité atribúty údajov IS, ale aj tzv. „metaúdaje", teda aj údaje umožňujúce prechod cez bezpečnostné opatrenia (parametre bezpečnostných prostriedkov, prístupové heslá, šifrovacie kľúče a pod.),
- bezpečnostné opatrenia musia tvoriť ucelený systém, v ktorom neexistuje bod, ktorého zablokovanie (nefunkčnosť) by zapríčinilo nefunkčnosť celého systému ochrany,
- opatrenia pre zaistenie bezpečnosti IS sa musia včas prispôsobovať závažným zmenám podmienok, za ktorých boli navrhované.

Princípy bezpečnostnej politiky pri prijímaní bezpečnostných opatrení sa v zásade musia primeraným spôsobom aplikovať aj na prípadné zmeny v náplni úloh a zmeny v organizačnej štruktúre, ako aj zmeny v technickom a programovom zabezpečení IS, ktoré si v budúcnosti vynútia potreby samosprávy.

S ohľadom na základné poslanie obce ako OVM považuje jej vedenie za základné aktíva v IS predovšetkým:

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

Dôležitými atribútmi údajov, spracovávaných a uchovávaných v IS obce, sú predovšetkým:

- dôvernosť – stav, v ktorom je údaj utajený, známy iba vymedzenému okruhu subjektov; strata tohto atribútu znamená, že údaj je prezradený (únik informácie), teda že sa stane známym mimo vymedzeného okruhu subjektov,
- integrita – údaj je celistvý, v pôvodnom, nezmenenom stave, je neporušený; strata tohto atribútu znamená, že údaj (informácia) je neúplný, nie je v pôvodnom stave, bol (neoprávnene) zmenený,
- autenticita – stav, v ktorom je údaj pravdivý, skutočný, zodpovedajúci skutočnosti, nespochybniteľného pôvodu, teda je správnou reprezentáciou toho, čo je úmyslom, aby reprezentoval; strata tohto atribútu znamená, že údaj je nesprávny, nezodpovedá skutočnosti, ktorú by mal reprezentovať, je "falošný" (sfalšovaný),
- dosiahnuteľnosť – stav, v ktorom je údaj k dispozícii, schopný bezprostredného použitia na nejaký účel; strata tohto atribútu znamená, že údaj nie je tam, kde je očakávaný, nie je schopný okamžitého použitia.

Za najzávažnejšie hrozby pre aktíva v IS sú považované predovšetkým:
- možnosť úniku a zneužitia osobných údajov nachádzajúcich sa v IS,
- možnosť neoprávnenej manipulácie s osobnými údajmi v IS,

- nenávratné zničenie alebo poškodenie osobných údajov v IS,
- cielené úmyselné zmeny, alebo vnášanie nepravých, neautentických údajov do IS.

Medzi základné bezpečnostné opatrenia patrí pravidelná kontrola integrity a aktuálnosti (z hľadiska požiadaviek bezpečnosti) programového vybavenia a vybraných dôležitých údajov minimálne na vybraných kľúčových komponentoch IS.
V prípade prepájania komunikačných sietí je potrebné použiť spoľahlivé oddeľovacie bezpečnostné prvky (firewall) a zároveň explicitne stanoviť:

- aký typ prístupu, aké údaje a aké služby sú povolené v smere z vonkajšej siete do vnútornej siete,
- aký typ prístupu, aké údaje a aké služby sú povolené v smere z vnútornej siete do vonkajšej siete,
- zodpovednosť za kontrolu nastavenia príslušných parametrov, ako aj kontrolu a vyhodnocovanie bežnej prevádzky firewall,
- základné postupy v prípade zistených útokov na firewall.

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.

Pri nastavovaní parametrov bezpečnostných prvkov použitých v IS obce je nevyhnutné dôsledne uplatňovať bezpečnostný princíp, podľa ktorého je zakázané všetko, čo nie je explicitne povolené.

Pri prideľovaní prístupových práv k IS obce je nevyhnutné dôsledne uplatňovať nasledovné bezpečnostné princípy:
- princíp najmenších možných privilégií
- princíp rozdelenia povinností a zodpovednosti.

Zároveň musia byť stanovené jednoznačné pravidlá pre časovo obmedzené prideľovanie prístupových práv a pre postup včasného odnímania (rušenia) prístupových práv k IS obce.
Je potrebné riešiť prideľovanie a osobitne odnímanie prístupových práv vo väzbe na prácu personálnych útvarov (predovšetkým v prípade rozviazania pracovného pomeru s pracovníkom – používateľom IS).

Vnútorné smernice na jednotlivých pracoviskách stanovia jednoznačné zásady postupu používateľov IS obce pri takých činnostiach a udalostiach, ktoré vplývajú na bezpečnosť a spoľahlivú prevádzku informačného systému. Vnútorné smernice by mali pokrývať minimálne nasledovné oblasti súvisiace s prevádzkou IS.

<u>základná ochrana komponentov informačného systému by mala dodržiavať:</u>

- zásady pre fyzické umiestnenie prvkov výpočtovej a komunikačnej techniky informačného systému z hľadiska ich bezpečnosti a zaistenia podmienok pre ich spoľahlivú prevádzku,
- zásady pre bežnú manipuláciu s kľúčovými prvkami výpočtovej a komunikačnej techniky (kto je oprávnený akú činnosť vykonávať),

- zásady pre manipuláciu s kľúčovými dokumentmi IS obce (kto a s akými dokumentmi je oprávnený sa oboznámiť, kto a aké zmeny a za akých podmienok smie vykonať, ako majú byť dokumenty uložené, ako sa môže s nimi manipulovať),
- zásady riadenia a monitorovania prístupu pracovníkov (vrátane externých návštevníkov) do jednotlivých častí pracovných priestorov (budovy) ku kľúčovým prostriedkom výpočtovej a komunikačnej techniky systému (kto, za akých podmienok má povolený prístup ku ktorým komponentom),
- kompetencie, zásady a postup pri inštalácií nového a pri úpravách pôvodného programového vybavenia systému,
- kompetencie, zásady a postup pri údržbe technických prostriedkov systému,

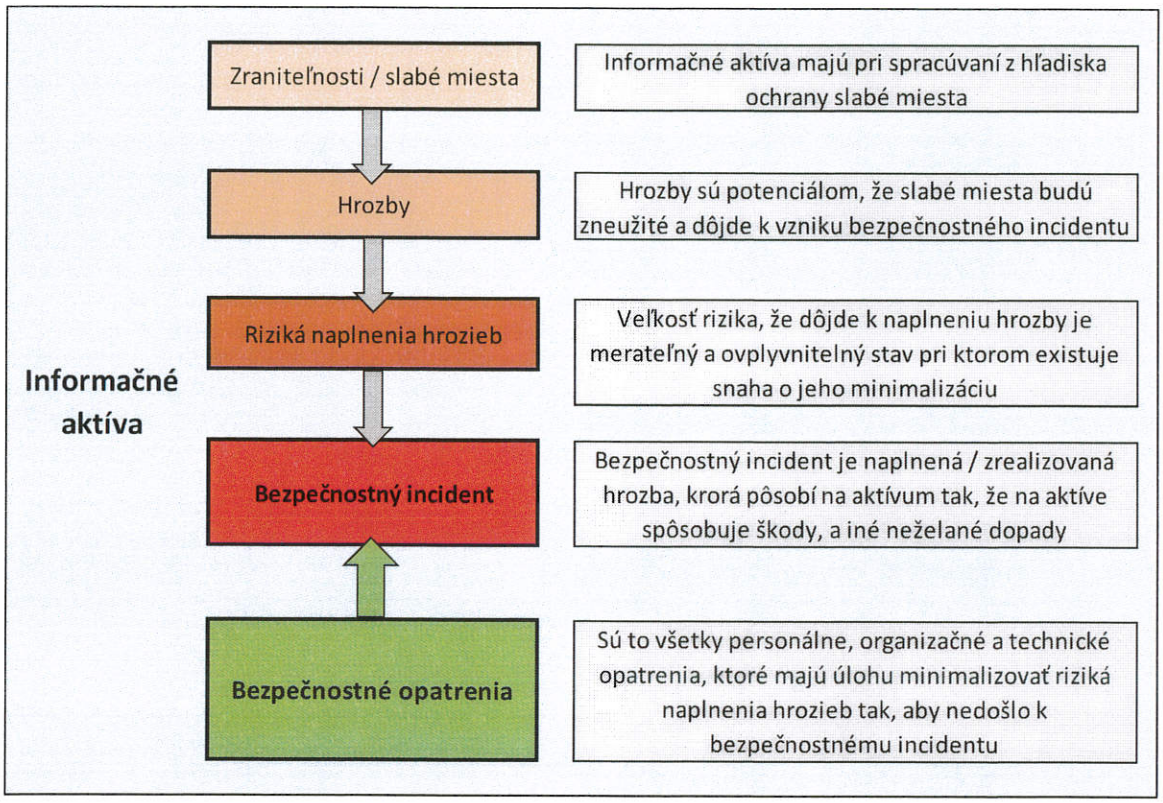
bežná prevádzka informačného systému si vyžaduje:

- dodržiavanie zásad spracúvania v zmysle nariadenia GDPR,
- vedenie dokumentácie spracovateľských činností a spracovateľských operácií,
- vypracovaný postup pri hlásení, prešetrovaní a riešení bezpečnostne významných udalostí (bezpečnostných incidentov),
- zásady výberu/prideľovania, používania a ochrany osobných identifikačných prvkov a prvkov na overovanie totožnosti používateľov IS (heslá, čipové karty a pod.),
- zásady distribúcie tlačových zostáv, generovaných systémom, ich ochrana, skladovanie a likvidácia,
- zásady a postup pri príjme a používaní médií s údajmi v elektronickej forme od externých subjektov (procedúry overenia autenticity prijatých údajov, antivírová kontrola médií pred ich vložením do počítačových systémov organizácie a podobne),
- zásady pre kontrolu prístupu externých kooperujúcich subjektov k službám informačného systému (poskytnutie prístupového hesla, jeho následná zmena a podobne),

Analýza bezpečnosti informačných aktív v IS a posúdenie rizík

1. Identifikácie a vymedzenia

Nasledovný graf zobrazuje **informačné aktíva**, na ktoré cez ich **zraniteľnosti/slabé miesta** z hľadiska zabezpečenia ochrany pôsobia **hrozby,** ktoré s určitou pravdepodobnosťou **rizika naplnenia hrozieb** sa naplnia, čím vznikne **bezpečnostný incident** s následnými dopadmi. Preto aby sa hrozby nenaplnili-nevznikol bezpečnostný incident a riziko ich naplnenia bolo čo najnižšie, naopak na informačné aktíva pôsobia **bezpečnostné opatrenia**.



Preto je potrebné pre podmienky prevádzkovateľa IS s informačnými aktívami vykonať nasledovné identifikácie a vymedzenia:

1.1. Identifikácia základných informačných aktív v IS

Ako základné aktíva v IS obce sú identifikované:

- 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. Identifikácia zraniteľnosti informačných aktív

V súčasnosti je činnosť útvarov prakticky všetkých pracovísk IS obce vo veľkej miere závislá od správnej a neprerušenej činnosti IS obce. Negatívne vplyvy na činnosť jednotlivých útvarov, súvisiace s IS obce môžu byť zapríčinené:

- poruchami v údajoch, s ktorými tieto pracoviská pracujú a z ktorých vychádzajú pri prijímaní jednotlivých rozhodnutí,
- poruchami v činnosti prostriedkov, ktoré podporujú prácu s kľúčovými údajmi (spracovanie, prezentácia, prenos údajov)

Slabým miestom informačných aktív v podmienkach obce sú:
- slabé miesta priamo v IS, hlavne v tom ako sú navrhnuté ich programové aplikácie a ako sú navrhnuté a chránené k nim prislúchajúce databázy,
- slabé miesta v bezpečnostných procedúrach IS,
- slabé miesta v bezpečnostných opatreniach – personálnych, technických aj organizačných

1.3. Identifikácia hrozieb

V nadväznosti na identifikované informačné aktíva a ich slabé miesta je potrebné vykonať identifikáciu hrozieb, ktoré by pri zneužití slabých miest informačných aktív mohli týmto aktívam hroziť.

Katalóg hrozieb podľa ISO27005 uvádza hrozby:
- fyzické poškodenie
- prírodné udalosti
- strata dôležitých služieb
- narušenie spôsobené žiarením
- kompromitácia informácii
- technické zlyhanie
- nepovolené aktivity
- kompromitácia funkcií

V podmienkach prevádzkovateľa sú to hlavne hrozby:

- **možnosť úniku a zneužitia osobných údajov** nachádzajúcich sa v IS (ISO27005: kompromitácia informácii),
- **možnosť neoprávnenej manipulácie** s osobnými údajmi v IS (ISO27005: nepovolené aktivity)
- **nenávratné zničenie alebo poškodenie** osobných údajov v IS (ISO27005: fyzické poškodenie, prírodné udalosti, technické zlyhanie),
- **cielené úmyselné zmeny, alebo vnášanie nepravých, neautentických údajov** do IS. (ISO27005: nepovolené aktivity)

1.4. Riziká naplnenia hrozieb

Riziko je odhadom pravdepodobnosti možného pôsobenia konkrétnej hrozby na konkrétne aktívum vo vzťahu k predpokladanému dopadu na aktívum. Posudzuje sa veľkosť rizika pre každú identifikovanú hrozbu a každý IS samostatne s následným zhrnutím a identifikovaním najväčších rizík.

1.5. Identifikácia dopadov na informačné aktíva a na práva dotknutých osôb (teda osôb, ktorým aktíva - osobné údaje patria)

Identifikácia dopadov na aktíva v dôsledku straty dôvernosti, integrity, autenticity a dostupnosti:

- porušenie povinností stanovených nariadením č. **2016/679 EP a Rady EÚ a** zákonom č. 18/2018 Z. z. o ochrane osobných údajov a možné súvisiace sankcie,
- porušenie práv dotknutých osôb pri nezákonnom spracúvaní ich osobných údajov, alebo pri nedostatočnej ochrane ich osobných údajov v zmysle narušenia ich osobnej integrity, dôstojnosti, dobrého mena a podobne, ktorého dôsledkom môžu byť nielen sankcie regulačného orgánu, ale aj súdne spory s dotknutými osobami,
- v prípade súčasného poškodenia alebo zničenia záložných kópií prácna rekonštrukcia údajov (so zvýšenou pravdepodobnosťou chýb),
- v prípade poškodenia, zlyhania, alebo odcudzenia výpočtovej techniky omeškanie spracovania osobných údajov a nadväzujúcich činností,
- narušenie práce pracoviska, v prípade niektorých aplikácií prácna rekonštrukcia údajov (nedostatočné, resp. žiadne údaje v listinnej forme),
- obmedzenie schopnosti pracoviska včas plniť svoje úlohy.

1.6. Identifikácia informačných systémov

1. Matrika / CISMA
2. Evidencia obyvateľstva / REGOB+CO+RA+IOMO
3. Miestne dane
4. Poplatky
5. Kataster obce
6. Účtovníctvo a majetok + RIS.SAM
7. Mzdy a personalistika
8. Stavebný úrad + drobné stavby
9. Aktivačná činnosť formou menších obecný služieb
10. Osvedčovanie podpisov a listín
11. Poberatelia dávok v hmotnej núdzi
12. Rybárske lístky
13. Výrub stromov
14. Obecná knižnica
15. Evidencia hrobových miest
16. Jednotný informačný systém hospodárskej mobilizácie (JISHM)
17. Evidencia samostatne hospodáriacich roľníkov
18. Evidencia informovaných súhlasov dotknutých osôb
19. Kamerové systémy
20. Elektronická schránka na IS verejnej správy (VS) na ÚPVS
21. Bezpečnosť a ochrana zdravia pri práci (BOZP) a protipožiarna ochrana (PO)
22. Nájomné byty - evidencia nájomných bytov a ich nájomcov
23. Registratúrne stredisko (archív)
24. ZPS - sociálna agenda - osobné spisy prijímateľov sociálnej služby

25. ZPS - sociálna agenda - evidencia prijímateľov sociálnej služby
26. ZPS - sociálna agenda - zdravotná starostlivosť
27. ZPS - Stravovacia jednotka
28. ZPS - registratúrne stredisko (archív).

2. Posúdenie rizík naplnenia identifikovaných hrozieb

2.1 Stanovenie metriky pre hodnotenie

Pre stanovenie úrovne rizika sa použije nasledovný index:

Riziko	Zodpovedajúca číselná hodnota	Očakávané nápravné bezpečnostné opatrenia
Extrémne vysoké	od 81 do 100	Nápravné opatrenia sú nevyhnutné a je nutné prijať ich bezodkladne. Treba zvážiť aj možnosť odstavenia systému.
Veľmi vysoké	od 56 do 80	Nápravné opatrenia sú nevyhnutné a je nutné prijať ich bezodkladne. Treba zvážiť aj možnosť odstavenia systému.
Vysoké	od 40 do 55	Nápravné opatrenia sú nevyhnutné a je nutné ich prijať v čo najkratšom čase.
Stredné	od 20 do 39	Treba stanoviť, či je nutné prijať nápravné opatrenia, alebo či v minulosti prijaté opatrenia sú ešte potrebné. Prípadne je možné toto riziko akceptovať.
Malé	od 0 do 19	Nie je nutné prijať nápravné opatrenia

Stanovenie pravdepodobnosti rizika:

Pravdepodobnosť			
Hodnota	**Slovne**	**% výskytu**	**Popis**
1	Vysoká	50 – 250	Zdroj hrozby je vysoko motivovaný a je dostatočne technicky zdatný. Realizované bezpečnostné opatrenia na prevenciu identifikovaného slabého miesta sú neúčinné. V minulosti bolo dané slabé miesto často zneužité.
0,7	Stredná	5 – 50	Zdroj hrozby je vysoko motivovaný a je dostatočne technicky zdatný. Realizované bezpečnostné opatrenia na prevenciu identifikovaného slabého miesta čiastočne bránia úspešnému zneužitiu slabého miesta. V minulosti bolo dané slabé miesto niekedy zneužité.
0,4	Malá	1 – 5	Zdroj hrozby nemá dostatočnú motiváciu ani zručnosti. Realizované bezpečnostné opatrenia na prevenciu identifikovaného slabého miesta predchádzajú zabraňujú naplneniu hrozby. V minulosti bolo dané slabé miesto ojedinele zneužité.
0,2	Veľmi malá	0 – 1	Zdroj hrozby nemá dostatočnú motiváciu ani zručnosti. Realizované bezpečnostné opatrenia na prevenciu identifikovaného slabého miesta predchádzajú zabraňujú naplneniu hrozby. V minulosti nebolo dané slabé miesto zneužité.

Definícia dopadov:

Hodnota	Opis dopadu	Finančný dopad	Prevádzkový dopad	Legislatívny dopad	Strata dôvery
100	katastrofický	Viac ako 100000 €	prevádzkovateľ / všetky osobné údaje dotknutých osôb	porušenie internej smernice / legislatívy /začatie správneho konania smerujúceho k opatreniam na nápravu / uloženiu pokuty /pozastavenie - ukončenie činnosti kľúčových služieb	intenzívna nepriaznivá publicita na národnej úrovni
80	značný	10000 – 100000 €	prevádzkovateľ / veľká časť osobných údajov dotknutých osôb	porušenie internej smernice / legislatívy /začatie správneho konania smerujúceho k opatreniam na nápravu / uloženiu pokuty /pozastavenie - ukončenie činnosti časti služieb	intenzívna nepriaznivá publicita na národnej úrovni
60	stredný	1000 - 10000 €	prevádzkovateľ / malá časť dotknutých osôb	porušenie internej smernice / legislatívy /začatie správneho konania smerujúceho k opatreniam na nápravu / uloženiu pokuty	určitá nepriaznivá publicita na národnej úrovni
40	malý	501 – 1000 €	viacero oddelení (IS) v rámci prevádzkovateľa	porušenie internej smernice / legislatívy / začatie správneho konania smerujúceho k opatreniam na nápravu	závažné prekážky v komunikácii v rámci prevádzkovateľa
20	zanedbateľný	1 - 500 €	1 oddelenie (IS) v rámci prevádzkovateľa	porušenie internej smernice / legislatívy	určité prekážky v komunikácii v rámci prevádzkovateľa

Matica pre stanovenie úrovne rizika:

Úroveň rizika	Dopad				
Pravdepodobnosť rizika	Zanedbateľný (20)	Malý (40)	Stredný (60)	Značný (80)	Katastrofický (100)
Vysoká (1)	20x1,0=20	40x1,0=40	60x1,0=60	80x1,0=80	100x1,0=100
Stredná (0,7)	20x0,7=14	40x0,7=28	60x0,7=42	80x0,7=56	100x0,7=70
Malá (0,4)	20x0,4=8	40x0,4=16	60x0,4=24	80x0,4=32	100x0,4=40
Veľmi malá (0,2)	20x0,2=4	40x0,2=8	60x0,2=12	80x0,2=16	100x0,2=20

2.2 Posúdenie úrovne rizík naplnenia hrozieb v jednotlivých IS

Postup pri výpočte úrovne rizika:

- každej z identifikovaných hrozieb sa určí pomocou zistených parametrov spracovávania osobných údajov v IS jej pravdepodobnosť naplnenia v rozsahu 0,0 – 1,0 (podobne ako je znázornené v matrici pre stanovenie úrovne rizika),

- pre každú hrozbu sa zároveň stanoví odhad dopadu v rozsahu 20 – 100 individuálne pre každý IS, podľa okolností a parametrov spracovávania osobných údajov v IS (podobne ako je znázornené v matrici pre stanovenie úrovne rizika),

- Úroveň rizika naplnenia identifikovanej hrozby je potom násobok pravdepodobnosti naplnenia tejto hrozby a dopadu v rozsahu 0 - 100

Príklad:

Úroveň rizika = Identifikovaná hrozba x (váhy parametrov v IS) x dopad

Tento spôsob (odhadu) sa využije pre posúdenie úrovní rizík naplnenia všetkých identifikovaných hrozieb, postupne pre všetky IS v ktorých sa vykonávajú spracovateľské operácie s osobnými údajmi.

Posúdenie úrovne rizík naplnenia identifikovaných hrozieb v jednotlivých IS je samostatnou prílohou k tomuto dokumentu

3. Bezpečnostné opatrenia

3. 1 Technické opatrenia - navrhované a realizované v podmienkach prevádzkovateľa

3.1.1 Technické opatrenia realizované prostriedkami fyzickej povahy

3.1.1.1 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.

3.1.1.2 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.

3.1.1.3 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.

3.1.1.4 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.

3.1.1.5 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.

3.1.1.6 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.

3.1.2 Ochrana pred neoprávneným prístupom

3.1.2.1 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.

3.1.2.2 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.

3.1.3 Riadenie prístupu oprávnených osôb

3.1.3.1 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).

3.1.3.2 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.

3.1.4 Ochrana proti škodlivému kódu

3.1.4.1 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.

3.1.4.2 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 doplňaný 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.

3.1.4.3 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.

3.1.4.4 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.

3.1.5 Sieťová bezpečnosť

3.1.5.1 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.

3.1.5.2 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.

3.1.5.3 **K ochrane vonkajšieho a vnútorného prostredia počítačovej komunikácie sa využijú prostriedky sieťovej bezpečnosti podľa bodu 3.5.1**

3.1.5.4 **Prevádzkovateľ zabezpečí obmedzenia prístupu a ich kontrolu podľa bodu 3.5.1 Prostredníctvom firewall a nastavení sieťovej komunikácie v rámci antivírusového programu musí byť zabezpečená ochrana proti tzv. hackerským útokom.**

3.1.6 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.

3.1.6.1 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.

3.1.6.2 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.

3.1.6.3 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.

3.1.6.4 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.

3.1.7 Likvidácia osobných údajov a dátových nosičov

3.1.7.1 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.

3.1.7.2 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.

3.1.8 Aktualizácia operačného systému (OS) a softwarových komponentov IS

3.1.8.1 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.

3.2 Organizačné opatrenia - navrhované a realizované v podmienkach prevádzkovateľa

3.2.1 Personálne opatrenia

3.2.1.1 Prevádzkovateľ, alebo ním určená poverená osoba vykoná oboznámenie poverených oprávnených osôb s bezpečnostnou politikou prevádzkovateľa ešte pred uskutočnením prvej spracovateľskej operácie.

3.2.1.2 Prevádzkovateľ poverením oboznámi oprávnené osoby o ich právach, povinnostiach a zodpovednosti, ktoré vyplývajú z nariadenia GDPR a zo zákona č. 18/2018 Z.z.

3.2.1.3 Poverenie každej oprávnenej osoby bude individuálne s vymedzením osobných údajov, ku ktorým má oprávnená osoba v rámci plnenia si svojich pracovných povinností prístup.

3.2.1.4 Poverenie každej oprávnenej osobe určí postupy pri narábaní s osobnými údajmi.

3.2.1.5 Poverenie každej oprávnenej osobe vymedzí zakázané postupy pri narábaní s osobnými údajmi.

3.2.1.6 Poverenie každej oprávnenej osobe vymedzí zodpovednosti za porušenie GDPR resp. zákona č. 18/2018 Z.z.

3.2.1.7 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.

3.2.1.8 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.

3.2.1.9 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.

3.2.1.10 Prevádzkovateľ zabezpečí aj následné vzdelávanie oprávnených osôb v oblasti práva a informačných technológií.

3.2.1.11 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.

3.2.2 Vedenie zoznamu aktív a jeho aktualizácia

3.2.2.1 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.**

3.2.3 Riadenie prístupu poverených oprávnených osôb k osobným údajom

3.2.3.1 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.

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

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

prístupové práva
- 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,

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

3.2.3.5 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.

3.2.4 Organizácia spracúvania osobných údajov

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

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

3.2.4.3 Prevádzkovateľ musí stanoviť režim upratovania chránených priestorov.

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

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

3.2.4.6 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.

3.2.5 Likvidácia osobných údajov

3.2.5.1 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.

3.2.6 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 3.2.6 zrealizované vykonaním oboznámenia poverenej zodpovednej osoby s bezpečnostnou politikou prevádzkovateľa.**

3.2.7 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.

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

3.2.7.2 Informovanie oprávnených osôb o kontrolnom mechanizme – rozsahu, spôsobu a periodicity uskutočňovania kontroly.
V podmienkach prevádzkovateľa sú opatrenia 3.2.7 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.

Obec Makov dňa 24.05.2018

Martin Pavlík - starosta obce

(štatutár prevádzkovateľa) podpis: .....