PRÍLOHY

GDPR

vzory a tlačivá

V rámci technických a organizačných opatrení na zabezpečenie spracúvania osobných údajov k zavedeniu štandardnej ochrany osobných údajov dotknutých osôb v zmysle zákona č.18/2018 Z.z.

ITAK s.r.o..

Baštová 38, 945 01 Komárno

OBSAH :

- **Formulované bezpečnostné ciele, ako výsledok kvalitatívnej analýzy**
- **Evidencia vytvorených prístupov do informačných systémov**
- **Vzor oznámenia zmeny tretej strane**
- **Preverenie spôsobilosti sprostredkovateľa**
- **Vzor zmluvy medzi prevádzkovateľom a sprostredkovateľom**
- **Preberací protokol aktíva**
- **Evidencia chránených priestorov typu I**
- **Inventárny záznam pre aktíva typu AI**
- **Inventárny záznam pre aktíva typu AII a AIII**
- **Inventárny záznam pre aktíva typu AIV**
- **Inventárny záznam pre aktíva typu AV**
- **Inventárny záznam pre aktíva typu AVI**
- **Záznam o premiestnení aktíva za účelom údržby alebo opravy**
- **Evidencia vydaných kľúčov od priestorov prevádzkovateľa**
- **Záznam o údržbe technického zariadenia**
- **Záznam o informovaní pracovníka o povinnosti mlčanlivosti**
- **Prehľad používaných bezpečnostných opatrení**
- **Evidencia IS osobných údajov (vzor)**
- **Poskytnutie informácií dotknutej osobe**
- **Súhlas s poskytnutím osobných údajov**
- **Poskytnutie informácií dotknutej osobe podľa §20 ods. 2 písm. f) zák. č. 18/2018 Z. z.**
- **Poskytnutie informácií dotknutej osobe podľa §21 zákona č. 18/2018 Z. z.**
- **Preukázanie príslušnosti oprávnenej osoby**
- **Kontrolná činnosť**
- **Ročný harmonogram kontrolnej činnosti**
- **Operačný plán kontrolnej činnosti**
- **Protokol z kontrolnej činnosti**
- **Priebežné zaznamenávanie údajov pri bezpečnostnom incidente (BI)**
- **Bezpečnostné incidenty (postupy)**
- **Metóda hodnotenia závažnosti porušenia bezpečnosti OÚ (SE)**
- **Návrhy na vypracovanie-aktualizáciu-zrušenie-opatrení**
- **Záznam o vykonanom školení pracovníkov**

Formulované bezpečnostné ciele, ako výsledok kvalitatívnej analýzy

1. ….

Dátum formulácie cieľa: .....

Zodpovednosť za plnenie: .....

Termín plnenia: .....

2. ….

Dátum formulácie cieľa: .....

Zodpovednosť za plnenie: .....

Termín plnenia: .....

3. ….

Dátum formulácie cieľa: .....

Zodpovednosť za plnenie: .....

Termín plnenia: .....

4. ….

Dátum formulácie cieľa: .....

Zodpovednosť za plnenie: .....

Termín plnenia: .....

Evidencia vytvorených prístupov do informačných systémov

Tab. A
I. Poradové číslo vytvoreného používateľského prístupu:
II. Používateľský prístup bol vytvorený dňa a v hodine:
III. Používateľský prístup do informačného systému je povolený pre:
IV. Účel za akým je používateľský prístup povolený:
V. Názov informačného systému:
VI. Používateľský prístup pridelil:
VII. Používateľský prístup schválil:
VIII. Podpis osoby, ktorej bol používateľský prístup pridelený:

Poučenie: Osoba, ktorej sa používateľský prístup prideľuje sa podpisom v bode VIII. zaväzuje, že pridelené heslo bude využívať len pre svoju činnosť, ktorá jej vyplýva z pracovnej zmluvy a obdobného vzťahu, obchodnej zmluvy, prípadne iného zmluvného vzťahu. Osoba, ktorej bolo heslo pridelené, ho nesmie poskytnúť inej osobe. Pri výzve na zmenu hesla, ho zmení tak, že nové heslo bude mať minimálne osem znakov. Heslo nesmie byť vo vzťahu k osobe používateľa jednoducho uhádnuteľné (je neprípustné používať heslá typu priezvisko, meno používateľa, meno a priezvisko príbuznej osoby, dátum narodenia a pod.). Heslo je používateľ povinný uchovávať v dôvernosti a manipulovať s ním zodpovedne. Heslo nesmie byť zaznamenávané na papieri, pod klávesnicou, do kalendára, v súbore a pod. alebo iným neschváleným spôsobom, kedy by sa s ním mohli oboznámiť neoprávnené osoby. V prípade, ak má podozrenie, že heslo bolo prezradené, je povinný ho v čo najkratšom čase zmeniť. Heslo nesmie byť zahrnuté do automatického prihlasovacieho procesu. Heslo používané v práci nesmie byť využívané aj pre mimopracovné účely. Ak došlo k strate alebo k prezradeniu hesla, je toto povinný ihneď oznámiť určenému pracovníkovi.....

Tab. B
Používateľský prístup z tab. A bol zrušený dňa o hodine:
Používateľský prístup zrušil:
Zrušenie užívateľského prístupu schválil:

List č.: .....

Vzor oznámenia zmeny tretej strane
podľa §25 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej ako zákon)

Názov organizácie:

Právna forma:

Sídlo:

Identifikačné číslo prevádzkovateľa:

Týmto oznamuje tretej strane, ktorou je:

….....

(obchodný názov, sídlo)

že poskytnuté osobné údaje v rozsahu:

….....

….....

Vám boli poskytnuté neaktuálne.

Ako prevádzkovateľ informačného systému s osobnými údajmi sme tieto opravili a implementovali mechanizmus, ktorý zabezpečí ich pravidelnú aktualizáciu.

Týmto Vás preto žiadame o aktualizáciu poskytnutých osobných údajov vo svojom informačnom systéme nasledovne:

….....

….....

….....

V ..... dňa: .....

.....

Za prevádzkovateľa

Preverenie spôsobilosti sprostredkovateľa podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len ako „zákon o ochrane osobných údajov“)

Názov sprostredkovateľa: ….....

Adresa sídla sprostredkovateľa: ….....

Identifikačné číslo sprostredkovateľa: ….....

(ďalej ako sprostredkovateľ)

Podľa § 34 ods. 1 zákona o ochrane osobných údajov, ak sa má spracúvanie osobných údajov uskutočniť v mene prevádzkovateľa, prevádzkovateľ môže poveriť len sprostredkovateľa, ktorý poskytuje dostatočné záruky na prijatie primeraných technických a organizačných opatrení tak, aby spracúvanie osobných údajov spĺňalo požiadavky tohto zákona a aby sa zabezpečila ochrana práv dotknutej osoby. Na poverenie sprostredkovateľa spracúvaním osobných údajov podľa prvej vety sa súhlas dotknutej osoby nevyžaduje.

Sprostredkovateľ je povinný chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania.

Zmluva, alebo iný právny úkon podľa § 34 odsekov 3 a 5 sa musí uzatvoriť v listinnej podobe alebo elektronickej podobe - obsahuje všetky nariadenia podľa § 34 ods.1 zákona o ochrane osobných údajov.

Na tento účel prijal horeuvedený sprostredkovateľ tieto technické, organizačné a personálne opatrenia:

….....

….....

….....

….....

….....

za sprostredkovateľa spracoval

Vzor zmluvy medzi prevádzkovateľom a sprostredkovateľom

ZMLUVA

o spracúvaní osobných údajov

v zmysle zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len ako „zákon o ochrane osobných údajov“)

uzatvorená medzi prevádzkovateľom a sprostredkovateľom

Názov organizácie:

Adresa sídla:

Identifikačné číslo:

Zastúpená:

Zapísaná v Obchodnom registri:

ako prevádzkovateľ informačných systémov (ďalej len ako „prevádzkovateľ“)

a

Názov organizácie:

Adresa sídla:

Identifikačné číslo:

Zastúpená:

Zapísaná v Obchodnom registri:

ako sprostredkovateľ (ďalej len ako „sprostredkovateľ“)

I. Predmet zmluvy

1. Predmetom tejto zmluvy je vymedzenie rozsahu a podmienok spracúvania osobných údajov v zmysle zákona o ochrane osobných údajov a vymedzenie práv a povinností zmluvných strán podľa §34 zákona o ochrane osobných údajov.

II. Okruh dotknutých osôb

1. Prevádzkovateľ odovzdáva sprostredkovateľovi na spracúvanie osobné údaje dotknutých osôb, ktorými sú zamestnanci prevádzkovateľa v pracovnom pomere a osoby vykonávajúce činnosť pre prevádzkovateľa na základe dohôd o vykonaní práce mimo pracovného pomeru v zmysle ustanovení Zákonníka práce v platnom znení a ich rodinní príslušníci.

III. Účel spracúvania osobných údajov

1. Účelom spracúvania osobných údajov ja zabezpečenie vedenia mzdovej a personálnej agendy prevádzkovateľa.

IV. Informovanie dotknutej osoby o spracúvaní osobných údajov a poverenom sprostredkovateľovi

1. Pri získavaní osobných údajov zabezpečuje plnenie požiadaviek zákona zák.č.18/2018 Z.z.o ochrane osobných údajov o ochrane osobných údajov :

2. Ak prevádzkovateľ poveril spracúvaním osobných údajov sprostredkovateľa až po získaní osobných údajov, je povinný zabezpečiť oznámenie tejto skutočnosti dotknutým osobám pri prvom kontakte s nimi, najneskôr však do troch mesiacov odo dňa poverenia sprostredkovateľa. To platí aj vtedy, ak spracúvanie osobných údajov prevezme právny nástupca prevádzkovateľa.

3. Sprostredkovateľ je vždy povinný pri prvom kontakte s dotknutou osobou oznámiť, že spracúva jej osobné údaje v mene prevádzkovateľa na vymedzený alebo ustanovený účel, ak zákon o ochrane osobných údajov neustanovuje inak.

V. Názov informačného systému a zoznam osobných údajov, ktoré sa budú spracúvať

1. Prevádzkovateľ odovzdá sprostredkovateľovi osobné údaje dotknutých osôb, ktoré sú súčasťou informačného systému s názvom „mzdová a personálna agenda“ a to v nasledujúcom rozsahu:
- meno, priezvisko, rodné priezvisko a titul,
- rodné číslo, dátum a miesto narodenia,
- podpis,
- rodinný stav ….. .

VI. Podmienky spracúvania osobných údajov

1. Osobné údaje dotknutých osôb doručí prevádzkovateľ sprostredkovateľovi elektronicky e-mailom, faxom, poštou alebo osobne. Sprostredkovateľ je vždy povinný potvrdiť prijatie e-mailovej správy predmetom, ktorej sú osobné údaje dotknutých osôb.

2. Za správnosť poskytnutých osobných údajov sprostredkovateľovi zodpovedá prevádzkovateľ. Aktuálnosť osobných údajov zabezpečuje prevádzkovateľ a to previerkou aktuálnosti spracúvaných osobných údajov, ktorú vykonáva prevádzkovateľ minimálne jedenkrát ročne alebo zmluvným záväzkom dotknutých osôb, že sú povinné prevádzkovateľa informovať o všetkých zmenách týkajúcich sa ich osobných údajov a to v čo najkratšom čase. Zaktualizované osobné údaje doručí prevádzkovateľ sprostredkovateľovi.

3. Osobné údaje spracúva sprostredkovateľ v listinnej podobe, ako aj použitím automatizovaných prostriedkov spracúvania.

4. Sprostredkovateľ je oprávnený poskytovať osobné údaje príslušnému úradu práce, sociálnych vecí a rodiny, Sociálnej poisťovni, zdravotným poisťovniam, príslušnému daňovému úradu, doplnkovej dôchodkovej sporiteľni, dôchodkovej správcovskej spoločnosti, v osobitných prípadoch aj orgánom štátnej správy a verejnej moci na výkon kontroly a dozoru (napr. inšpektorát práce), súdom, orgánom činným v trestnom konaní, exekútorom a iným oprávneným subjektom v zmysle osobitných zákonov.

5. V nevyhnutnom rozsahu je sprostredkovateľ oprávnený osobné údaje sprístupniť ním určenému poskytovateľovi služby údržby softvéru alebo hardvéru.

6. Spracované osobné údaje doručuje sprostredkovateľ oprávnenej osobe prevádzkovateľa vo forme výplatných pások, prevodných príkazov, mesačných prehľadov e-mailom, poštou alebo osobne. Prevádzkovateľ je vždy povinný potvrdiť prijatie e-mailovej správy predmetom, ktorej sú osobné údaje dotknutých osôb.

7. Spracované osobné údaje vo forme kópií výkazov do príslušnej sociálnej poisťovne, zdravotných poisťovní a hlásení daňovému úradu a pod. sprostredkovateľ uchováva u seba a odovzdáva prevádzkovateľovi osobne vždy jedenkrát ročne, za predchádzajúci kalendárny rok.

8. Po skončení účelu spracúvania je sprostredkovateľ povinný bez zbytočného odkladu zabezpečiť likvidáciu osobných údajov, okrem prípadov kedy sú osobné údaje súčasťou registratúrneho záznamu. Pričom je sprostredkovateľ povinný zabezpečiť likvidáciou osobných údajov spôsobom, kedy dôjde k zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.

VII. Práva a povinnosti zmluvných strán

1. Prevádzkovateľ aj sprostredkovateľ sú povinní pri spracúvaní osobných údajov postupovať podľa §.34 ods.3 zák.č.18/2018 Z.z. o ochrane osobných údajov..Za bezpečnosť osobných údajov zodpovedá prevádzkovateľ aj sprostredkovateľ. Prevádzkovateľ aj sprostredkovateľ sú povinní chrániť spracúvané osobné údaje pred ich poškodením, zničením, stratou, zmenou, neoprávneným prístupom a sprístupnením, poskytnutím alebo zverejnením, ako aj pred akýmikoľvek inými neprípustnými spôsobmi spracúvania. Na tento účel prijímajú primerané technické, organizačné a personálne opatrenia zodpovedajúce spôsobu spracúvania osobných údajov, pričom berú do úvahy najmä použiteľné technické prostriedky, dôvernosť a dôležitosť spracúvaných osobných údajov, ako aj rozsah možných rizík, ktoré sú spôsobilé narušiť bezpečnosť alebo funkčnosť informačného systému.

2. Zodpovedná osoba prevádzkovateľa je oprávnená preverovať u sprostredkovateľa dodržiavanie ustanovení zákona o ochrane osobných údajov pri spracúvaní osobných údajov sprostredkovateľom.

3. Z vykonanej previerky vyhotoví zápis, ktorý podpíše štatutárny orgán sprostredkovateľa a prevádzkovateľa.

4. Sprostredkovateľ sa zaväzuje, že tých svojich pracovníkov, ktorí budú mať prístup k osobným údajom prevádzkovateľa poučí v súlade so zák.č.18/2018 Z.z. o ochrane osobných údajov. O poučení vykoná písomný záznam a v prípade požiadavky ho predloží určenému pracovníkovi prevádzkovateľa.

5. Sprostredkovateľ sa zaväzuje k udržiavaniu bezpečnostného povedomia svojich pracovníkov s ohľadom na informačnú bezpečnosť najmä ich preškoľovaním či odborným vzdelávaním.

6. Sprostredkovateľ sa zaväzuje, že všetci pracovníci, ktorí búdu mať prístup k osobným údajom či iným aktívam prevádzkovateľa, si budú vedomí povinnosti ohlasovať zraniteľnosti a bezpečnostné incidenty, spôsobu oznamovania a budú zaviazaní povinnosťou mlčanlivosti v zmysle zák.č.18/2018 Z.z. §34 ods.3 písm.b) o ochrane osobných údajov.

7. V prípade, ak si dotknutá osoba uplatní svoje právo podľa §21 zákona o ochrane osobných údajov u sprostredkovateľa je tento povinný túto žiadosť alebo zápisnicu odovzdať prevádzkovateľovi bez zbytočného odkladu.

VIII. Spracúvanie osobných údajov subdodávateľom

1. Sprostredkovateľ vykonáva spracúvanie osobných údajov osobne. V prípade, ak by chcel sprostredkovateľ vykonávať spracúvanie osobných údajov prostredníctvom inej osoby tzv. subdodávateľom je povinný o tom najskôr písomne informovať prevádzkovateľa. K spracúvaniu osobných údajov subdodávateľom je nevyhnutný súhlas prevádzkovateľa. Subdodávateľ následne spracúva osobné údaje a zabezpečuje ich ochranu na zodpovednosť sprostredkovateľa.

IX. Záverečné ustanovenia

1. Prevádzkovateľ týmto vyhlasuje, že pri výbere sprostredkovateľa dbal na jeho odbornú, technickú, organizačnú a personálnu spôsobilosť a jeho schopnosť zaručiť bezpečnosť spracúvaných osobných údajov a že došlo k prevereniu spôsobilosti sprostredkovateľa podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov

2. Zmluva nadobúda účinnosť dňom jej podpísania oboma zmluvnými stranami. Sprostredkovateľ je oprávnený začať so spracúvaním osobných údajov v mene prevádzkovateľa odo dňa …..

3. Všetky ustanovenia tejto zmluvy možno meniť len vzájomnou dohodou, písomne, formou dodatku, ktorý bude tvoriť neoddeliteľnú súčasť tejto zmluvy.

4. Zmluvné strany svojim podpisom potvrdzujú, že si zmluvu prečítali, rozumejú jej a uzatvárajú ju slobodne a bez nátlaku

5. Táto zmluva zaniká dňom ukončenia zmluvných prác realizovaných sprostredkovateľom pre prevádzkovateľa.

6. Zmluva sa vyhotovuje v dvoch vyhotoveniach, po jednom pre každú zmluvnú stranu.

7. Zmluva sa uzatvára na dobu…..

V ....., dňa ..... .

....

za prevádzkovateľa za sprostredkovateľa

Evidencia chránených priestorov typu I

Por. číslo: ….....
Umiestnenie (poschodie, č. dv.): ….....

Zoznam pracovníkov oprávnených na vstup do priestoru:

Por. číslo	**Titul, meno, priezvisko** **Pracovná pozícia (pri externých pracovníkoch názov organizácie)**	
1.		
2.		
3.		

Por. číslo: ….....
Umiestnenie (poschodie, č. dv.): ….....

Zoznam pracovníkov oprávnených na vstup do priestoru:

Por. číslo	**Titul, meno, priezvisko**	**Pracovná pozícia (pri externých pracovníkoch názov organizácie)**
1.		
2.		
3.		

Preberací protokol aktíva

Názov a označenie aktíva:

Meno a priezvisko pracovníka, ktorému bude aktívum zverené:

Zoznam povoleného a nainštalovaného softvéru:

Poučenie pracovníka o manipulácii s aktívom:

Dátum: ….....

Podpis pracovníka, ktorému bude aktívum zverené: ….....

Podpis: ….....

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:

Záznam o premiestnení aktíva za účelom údržby alebo opravy

Inventárne označenie aktíva:
Dôvod premiestnenia:
Dátum premiestnenia:
Miesto premiestnenia (názov, adresa, poschodie, prípadne iný podrobný popis):
Predpokladané činnosti:
Predpokladaný dátum vrátenia aktíva:
Aktívum bolo dočasne nahradené (názov, inventárne označenie aktíva):

Evidencia vydaných kľúčov od priestorov prevádzkovateľa

Názov organizácie:

Právna forma:

Sídlo:

Identifikačné číslo prevádzkovateľa:

Ako dolu podpísaný pracovník prevádzkovateľa týmto preberám kľúče a zodpovednosť za manipuláciu s nimi od miestností uvedených nižšie. Som si vedomý, že v prípade ich straty či nefunkčnosti uzamykacieho systému som povinný o tomto bezodkladne informovať:

Titul, meno, priezvisko: .....

Pracovná pozícia: .....

telefonický kontakt: .....

Označenie kľúča	**Označenie/číslo miestnosti**	**Podpis pracovníka**	**Dátum prebratia kľúča**	**Dátum odovzdania kľúča**	**Poznámky:**

Záznam o údržbe technického zariadenia

Por. číslo: **1**
Názov aktíva a inventárne označenie:
Dátum obstarania:
Umiestnenie (adresa, poschodie, kancelária, prípadne iný podrobný popis) :
Interval údržby:
Údržbu vykonáva:
Predpokladané poruchy:
Popis činností, ktoré je potrebné minimálne na zariadení vykonať:

Dátum údržby:	Popis činností:	Záznam o poruche:	Podpis:

List č. …….

ZÁZNAM O INFORMOVANÍ PRACOVNÍKA
O POVINNOSTI MLČANLIVOSTI

v zmysle integrity a dôvernosti podľa §11 zákona č. 18/2018 Z. z. a §34 ods.3 písm b)

o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Názov prevádzkovateľa: .....

Sídlo: .....

Identifikačné číslo prevádzkovateľa: .....

Meno a priezvisko pracovníka: .....
Pracovná pozícia pracovníka: .....

V súvislosti s činnosťou, ktorú pre prevádzkovateľa vykonávate môžete prísť do styku s osobnými údajmi. O všetkých osobných údajoch ste povinný/povinná zachovávať mlčanlivosť.
Znamená to, že bez súhlasu prevádzkovateľa nesmiete osobné údaje zverejniť, nikomu poskytnúť ani sprístupniť. Povinnosť mlčanlivosti ste povinný/povinná zachovávať aj po zániku pracovného pomeru alebo obdobného pracovného vzťahu.
Povinnosť mlčanlivosti neplatí, ak je to nevyhnutné na plnenie úloh súdu a orgánov činných v trestnom konaní podľa osobitného zákona, ako aj vo vzťahu k Úradu na ochranu osobných údajov Slovenskej republiky; tým nie sú dotknuté ustanovenia o mlčanlivosti podľa osobitných predpisov.

V ....., dňa: .....

.....
(titul, meno, priezvisko, podpis pracovníka)

Prehľad používaných bezpečnostných opatrení

Názov opatrení	Číslo aktuálnej verzie a dátum schválenia						
Bezpečnostné opatrenie pre riadenie spracúvania osobných údajov							
Bezpečnostné opatrenie pre manipuláciu s osobnými údajmi							

List č.: ....

EVIDENCIA INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV

I. NÁZOV INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV
Monitoring e-mailovej komunikácie

II. ÚDAJE O PREVÁDZKOVATEĽOVI	
Názov prevádzkovateľa	
Identifikačné číslo organizácie (IČO)	
Obec a PSČ	
Ulica a číslo	
Štát	Slovenská republika
Právna forma	
Štatutárny orgán prevádzkovateľa (alebo osoba oprávnená konať v jeho mene)	
Zástupca prevádzkovateľa	Nie je vymenovaný
Počet oprávnených osôb	

III. ÚDAJE O INFORMAČNOM SYSTÉME OSOBNÝCH ÚDAJOV	
Účel spracúvania osobných údajov	zavedenie kontrolného mechanizmu prevádzkovateľa (zamestnávateľa) z dôvodu kontroly efektivity využívania pracovného času a plnenia povinností zamestnanca
Právny základ spracúvania osobných údajov	čl. 11 a § 13 ods. 4 zákona č. 311/2001 Z. z. Zákonník práce
Okruh dotknutých osôb	zamestnanci prevádzkovateľa
Zoznam osobných údajov (alebo rozsah) meno, priezvisko, titul, adresa elektronickej pošty, údaje týkajúce pracovnej e-mailovej komunikácie	
Označenie bezpečnostných opatrení	

IV. SPRACOVATEĽSKÉ OPERÁCIE S OSOBNÝMI ÚDAJMI	
Poskytovanie osobných údajov	
Tretie strany (prípadne okruh tr. strán)	**Právny základ**
iný oprávnený subjekt	

Sprístupňovanie osobných údajov	
Okruh príjemcov	**Právny základ**
Osobné údaje nie sú sprístupňované	
Zverejňovanie osobných údajov	
Spôsob zverejnenia	**Právny základ**
Osobné údaje nie sú zverejňované	
Cezhraničný prenos osobných údajov	
Tretia krajina	**Právny základ**
Osobné údaje nie sú predmetom cezhraničného prenosu	

V. ZAČIATOK SPRACÚVANIA OSOBNÝCH ÚDAJOV

.....
Odtlačok pečiatky prevádzkovateľa

.....
Dátum, meno a podpis
štatutárneho orgánu prevádzkovateľa

EVIDENCIA INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV

I. NÁZOV INFORMAČNÉHO SYSTÉMU OSOBNÝCH ÚDAJOV

II. ÚDAJE O PREVÁDZKOVATEĽOVI	
Názov prevádzkovateľa	
Identifikačné číslo organizácie (IČO)	
Obec a PSČ	
Ulica a číslo	
Štát	
Právna forma	
Štatutárny orgán prevádzkovateľa (alebo osoba oprávnená konať v jeho mene)	
Zástupca prevádzkovateľa	
Počet oprávnených osôb	

III. ÚDAJE O INFORMAČNOM SYSTÉME OSOBNÝCH ÚDAJOV	
Účel spracúvania osobných údajov	
Právny základ spracúvania osobných údajov	
Okruh dotknutých osôb	
Zoznam osobných údajov (alebo rozsah) meno, priezvisko, titul, adresa elektronickej pošty, údaje týkajúce pracovnej e-mailovej komunikácie	
Označenie bezpečnostných opatrení	

IV. SPRACOVATEĽSKÉ OPERÁCIE S OSOBNÝMI ÚDAJMI	
Poskytovanie osobných údajov	
Tretie strany (prípadne okruh tr. strán)	**Právny základ**
iný oprávnený subjekt	

Sprístupňovanie osobných údajov	
Okruh príjemcov	**Právny základ**
Zverejňovanie osobných údajov	
Spôsob zverejnenia	**Právny základ**
Cezhraničný prenos osobných údajov	
Tretia krajina	**Právny základ**

V. ZAČIATOK SPRACÚVANIA OSOBNÝCH ÚDAJOV

.....
Odtlačok pečiatky prevádzkovateľa

.....
Dátum, meno a podpis
štatutárneho orgánu prevádzkovateľa

Súhlas s poskytnutím osobných údajov
podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Názov prevádzkovateľa:
Sídlo:
Identifikačné číslo:
Týmto ..... *(uviesť meno a priezvisko)*
ako dotknutá osoba súhlasím, aby hore uvedený prevádzkovateľ:

1. Poskytol o mne osobné údaje v rozsahu môjho pracovného posudku.
   - o áno
   - o nie

2. Potvrdil pravdivosť informácií uvedených v mojom pracovnom posudku.
   - o áno
   - o nie

3. Poskytol o mne referenciu v súvislosti s mojim pracovným pomerom u prevádzkovateľa.
   - o áno
   - o nie

Uvedené žiadam poskytnúť tejto organizácii:
.....
.....
(názov, sídlo, IČO)
Platnosť súhlasu zaniká dňom poskytnutia osobných údajov uvedenej organizácii.

V ..... dňa: .....
.....
podpis dotknutej osoby

POSKYTNUTIE INFORMÁCIÍ DOTKNUTEJ OSOBE

podľa §21 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej ako zákon)

Názov prevádzkovateľa: ….....

Sídlo: ….....

Identifikačné číslo prevádzkovateľa: ….....

Dňa …….. sme prijali Vašu písomnú žiadosť, v ktorej si uplatňujete právo podľa §28 ods. 1 písm. a) zákona. Žiadate o potvrdenie, či sú alebo nie sú osobné údaje o Vás v našich informačných systémoch spracúvané.
V zmysle zákona Vás týmto informujeme, že v našich informačných systémoch osobné údaje o Vás spracúvame / nespracúvame.

V …....., dňa …..... .

.....…

Žiadosť vybavil/a

POSKYTNUTIE INFORMÁCIÍ DOTKNUTEJ OSOBE

podľa §21 zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej ako zákon)

Názov prevádzkovateľa: ….....

Sídlo: ….....

Identifikačné číslo prevádzkovateľa: ….....

Dňa ..... sme prijali Vašu písomnú žiadosť, v ktorej žiadate vo všeobecne zrozumiteľnej forme informácie o spracúvaní osobných údajov v informačnom systéme podľa §21 ods. 1 písm. a).b).c).d). zákona.

V zmysle zákona Vás týmto informujeme nasledovne:

Identifikačné údaje prevádzkovateľa sú uvedené vyššie.

Identifikačné údaje sprostredkovateľa:

.....

Účel spracúvania osobných údajov:

.....

Kategória spracúvaných osobných údajov:

.....

Právny základ spracúvania osobných údajov:

.....

Doba uchovávania osobných údajov

Tretie strany, ktorým sú údaje poskytnuté:

.....

Príjemcovia, ktorým sú údaje sprístupňované:

.....

Forma zverejnenia osobných údajov:

.....

Tretie krajiny, do ktorých je uskutočňovaný prenos: .....

V zmysle §21 ods. 3 prevádzkovateľ je povinný poskytnúť dotknutej osobe jej osobné údaje, ktoré spracúva. Za opakované poskytnutie osobných údajov, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Prevádzkovateľ je povinný poskytnúť osobné údaje dotknutej osobe spôsobom podľa jej požiadavky.

V zmysle §21 ods. 4 Právo získať osobné údaje podľa odseku 3 nesmie mať nepriaznivé dôsledky na práva iných fyzických osôb.

V …....., dňa ….....

.....…

Žiadosť vybavil/a

POSKYTNUTIE INFORMÁCIÍ DOTKNUTEJ OSOBE

podľa §20 ods. 2 písm. f) zák. č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej ako zákon)

Názov prevádzkovateľa: ….....

Sídlo: ….....

Identifikačné číslo prevádzkovateľa: ….....

Dňa …….. sme prijali Vašu písomnú žiadosť podľa §20 ods. 2 písm. f), v ktorej žiadate vo všeobecne zrozumiteľnej forme presné informácie o zdroji, z ktorého sme získali Vaše osobné údaje na spracúvanie. V zmysle zákona Vás týmto informujeme nasledovne:

Vaše osobné údaje sme získali z nasledovného zdroja :

……..

……..

……..

Pochádzajú z verejných zdrojov : ano - nie

V …....., dňa ….....

S pozdravom

.....

Žiadosť vybavil/a

Preukázanie príslušnosti oprávnenej osoby
podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

Názov organizácie: ….....

Právna forma: ….....

Sídlo: ….....

Identifikačné číslo: ….....

Nižšie uvedeného pracovníka týmto oprávňujeme k získavaniu osobných údajov do informačných systémov.

Oprávnená osoba:

titul, meno, priezvisko:

Pracovné zaradenie:

V …..... , dňa: ….....

Oprávnenie vydal:

….....
Podpis a pečiatka

Kontrolná činnosť

Kontrolné činnosti sú zamerané na dodržiavanie bezpečnosti IS. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození IS prevádzkovateľa identifikovaných podľa bezpečnostnej politiky prevádzkovateľa s periodicitou najmenej raz ročne. Kontroly spravidla vykonáva zodpovedná osoba prevádzkovateľa, pokiaľ nie je vymenovaná, konateľ prevádzkovateľa s vyhotovením písomných záznamov o zistených skutočnostiach, nedostatkoch a opatreniach prijatých na ich odstránenie. Prevádzkovateľ a sprostredkovateľ IS sú povinní umožniť kontrolu Úradu na ochranu osobných údajov v zmysle ustanovení zákona č. 18/2018 Z. z., vstupom do IS do úrovne správcu systému, v rozsahu potrebnom na vykonanie kontroly

Štandardom pre kontrolný mechanizmus riadenia informačnej bezpečnosti je: - dodržiavanie bezpečnostnej politiky prevádzkovateľa a zabezpečenie a vykonávanie vnútornej kontroly alebo auditu informačnej bezpečnosti, - zabezpečenie archivácie, ochrany a vyhodnocovania auditných správ, - spôsob, forma a periodicita výkonu kontrolných činností.

Kontrola dodržiavania bezpečnostných smerníc
- pred začatím používania IS, osoby zodpovedné za dohľad nad ochranou osobných údajov preveria, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb,
- zistenie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov zodpovedná osoba bezodkladne písomne oznámi prevádzkovateľovi, ak príslušný vedúci pracovník po upozornení bezodkladne nevykoná nápravu, oznámi to zodpovedná osoba úradu na ochranu osobných údajov,
- pri zistení porušenia zákona o ochrane osobných údajov sa okamžite pozastaví zálohovanie dátového záznamu a hľadajú sa postupy, ako dostať situáciu do súladu so zákonom,
- pri zistení nedostatku spracuje zodpovedná osoba zápis o zistenom nedostatku, jeho odstránení a navrhovanom riešení,
- zodpovedná osoba musí vždy vykonať zápis pri zistení systémového nedostatku a pri porušení práv dotknutých osôb,
- pri porušení povinností oprávnených osôb sa postupuje v zmysle ZP,
- kontrolu dodržiavania bezpečnostných smerníc vykonáva zodpovedná osoba a to pravidelne, minimálne raz ročne,
- kontrolujú sa zásady spracúvania osobných údajov a vyhotovuje sa o tom písomný záznam,
- pred začatím kontroly je o kontrole upovedomený príslušný vedúci pracovník zodpovedný za danú agendu,
- zásady spracúvania osobných údajov sa kontrolujú minimálne raz za rok,
- o každej kontrole zodpovedná osoba musí vypracovať zápis do knihy kontrol bezpečnosti IS a musí obsahovať minimálne:

- **dátum a čas kontroly,**
- **rozsah kontroly,**
- **zistené nedostatky pri kontrole,**
- **návrh protiopatrení,**
- **zoznam osôb zodpovedných za vykonanie protiopatrení,**
- **termín kontroly splnenia protiopatrení,**

- záznam z kontroly zodpovedná osoba predloží prevádzkovateľovi IS,
- pri bezpečnostnej udalosti musí zodpovedná osoba vykonať mimoriadnu kontrolu a vypracovať zápis do knihy kontrol bezpečnosti IS,
- kontrola prevádzky automatizovaného IS sa prevádza nepretržite a to technickými a programovými prostriedkami. V pracovnej dobe sa prevádza denne povereným správcom siete,
- kontrola zabezpečenia miestností pred nedovoleným prístupom v pracovnej dobe ale i v mimopracovnom čase, je vykonávaná náhodne vedúcimi pracovníkmi zodpovednými za danú agendu

Záznamy o revíziách

Popis zmeny / poznámky : Vytvorenie, úpravy a schválenie dokumentu , Popis zmeny , Nové vydanie

Záznam č :

Meno, Priezvisko :

Vypracoval :

Preveril:

Schválil :

Dátum:

Ročný harmonogram kontrolnej činnosti pre rok ….....

Por. číslo	Dátum kontrolnej činnosti	Názov kontrolovaného procesu	Meno a priezvisko určeného kontrolóra
1.		Základné pravidlá ochrany osobných údajov prevádzkovateľa	
2.		Riadenie procesu personálnej bezpečnosti	
3.		Riadenie aktív prevádzkovateľa v oblasti spracúvania osobných údajov	
4.		Kontrolná činnosť a preskúmavanie manažmentom prevádzkovateľa	
5.		Riadenie bezpečnostných incidentov	
6.		Riadenie dostupnosti	
7.	Riadenie prevádzky		
8.		Riadenie bezpečnostných rizík	
9.		Bezpečnosť systémov	

Operačný plán kontrolnej činnosti

Označenie a názov kontrolovaného procesu: .....

Cieľ kontrolnej činnosti:

Dôvod kontrolnej činnosti:

Dátum konania kontroly:

Predpokladané trvanie kontroly:

Predpokladané potrebné zdroje:

Určenie vrchného kontrolóra:

Operačný plán kontrolnej činnosti vypracoval: ….....

Dňa: ….....

Podpis pracovníka: ….....

Protokol z kontrolnej činnosti

Označenie a názov kontrolovaného procesu: .....

Kritériá kontrolnej činnosti:

Zistenia kontrolnej činnosti:

Navrhované opatrenia:

Dátum konania kontroly:

Kontrolu vykonal:
Ostatní prítomní pracovníci:

Protokol z kontrolnej činnosti vypracoval: ….....

Dňa: ….....

Podpis pracovníka: ….....

Priebežné zaznamenávanie údajov pri bezpečnostnom incidente (BI)

Časť A:

BI rozpoznal (meno, priezvisko):

Dátum a čas rozpoznania BI:

Dátum a čas vzniku BI (aj predpokladaný):

BI spôsobil nasledovné:

Kde došlo k prejavu BI a ako sa prejavil:

Pravdepodobný dôvod BI:

Ostatné dôležité informácie pre podrobnejší popis BI:

Časť B:

Dátum a čas kedy došlo k obnove prevádzky použitím priebežných opatrení:
Dátum a čas kedy došlo k úplnej obnove:

Vykonané nápravné opatrenia:
Opatrenia pre zamedzenie opakovaného výskytu BI:

Záznam vypracoval: ….....

Dňa: ….....

Podpis pracovníka: ….....

Bezpečnostné incidenty

Postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou. Štandardom pre periodické hodnotenie zraniteľnosti je pravidelné hodnotenie slabých miest a ohrození IS prevádzkovateľa s periodicitou najmenej raz ročne.

1. Narušenie personálnej bezpečnosti

- *strata, vyzradenie, alebo krádež hesiel pre vstup do IS – môže dôjsť k narušeniu integrity, alebo zneužitiu dátového záznamu z IS*
 zmeniť všetky prihlasovacie heslá do IS a to aj administrátorské
 vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS
 vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou - oprávnený vstup neoprávnenej osoby – môže dôjsť k narušeniu integrity alebo zneužitiu osobných údajov
 zmeniť všetky prihlasovacie heslá do IS a to aj administrátorské
 vykonať poučenie osôb o ochrane a utajení hesiel pre vstup do IS
 vykonať disciplinárne opatrenie, ak sa jednoznačne zistí, že išlo o poskytnutie autorizácie pre vstup, neoprávnenej osobe osobou oprávnenou

2. Narušenie fyzickej bezpečnosti

- *Narušenie dverí, okien*
 preventívne opatrenia:
 pravidelne sledovať funkčnosť
 postup pre zabezpečenie stavu obnovy:
 neodkladne zabezpečiť opravu,
 hľadať príčinu a odstrániť.

- *Narušenie monitorovaného objektu*
 preventívne opatrenia:
 pravidelne sledovať funkčnosť,
 postup pre zabezpečenie stavu obnovy:
 hľadať a eliminovať príčinu narušenia.

- *Krádež záznamového zariadenia/počítača– môže dôjsť k zneužitiu osobných údajov*
 zabezpečiť miesto, kde je uložený počítač proti opätovnému odcudzeniu – napr. inštalovaním doplnkových mechanických zábran,
 zakúpiť nový počítač s vyššími bezpečnostnými prvkami, inštalovať systém a obnoviť dáta zo záloh,
 zabezpečiť ukladanie archivovaných údajov v kryptovanom tvare.

- *Krádež, alebo strata kľúčov – môže dôjsť k neoprávnenému vstupu do miestností s aktívami IS a odcudzeniu osobných údajov, prípadne počítačov s osobnými údajmi*
 okamžite vymeniť zámky, prípadne doplniť bezpečnostné ochrany IS – napr. inštalovaním doplnkových mechanických zábran.

- *Strata záložných médií – môže dôjsť k zneužitiu osobných údajov*
 zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.
- Krádež záložných médií – môže dôjsť k zneužitiu osobných údajov
 zabezpečiť miesto, kde sú uložené média, proti opätovnému odcudzeniu – napr. inštalovaním doplnkových mechanických zábran,
 zabezpečiť zálohu údajov v kryptovanom tvare s prístupom cez heslo.

3. Narušenie technicko-softvérovej bezpečnosti

- Havárie IS spôsobené technickou chybou niektorého komponentu centrálneho počítača – serveru
 preventívne opatrenia:
 zabezpečiť záložné zdroje s automatickým vypnutím,
 monitorovať činnosť severov, kontrolovať chybové hlásenia,
 zabezpečiť dostatok finančných prostriedkov na obnovu IS, podľa možnosti obmieňať sever každé tri roky,
 zachovávať pravidlo – novší server sa stáva hlavným a starší záložným

 postup na zabezpečenie stavu obnovy:
 pri zálohovacom zariadení presmerovať prevádzku na záložné zálohovacie zariadenie/PC,
 obnoviť nastavenie zo zálohy,
 presmerovať aplikácie a užívateľov na záložný server,
 odstrániť poruchu na hlavnom serveri,
 po odstránení poruchy presmerovať prevádzku na hlavný server. - Vírusová infiltrácia – môže dôjsť k narušeniu integrity alebo straty a zneužitiu dát s osobnými údajmi

 preventívne opatrenia:
 zabezpečiť antivírovú ochranu,
 inštalovať len autorizované programy oprávnenými zamestnancami,
 preverovať cudzie nosiče (FD, CD, ROM, USB...),
 nepripájať nepreverené PC bez vedomia admin do LAN,
 nepoužívané pasívne rozvody odpojiť od aktívnych prvkov LAN,
 neotvárať nevyžiadané e-mailové prílohy,
 sledovať aktuálne dianie na LAN a v sieti internet,

 postup na zabezpečenie stavu obnovy:
 odpojiť každého užívateľa,
 okamžite skontrolovať aktualizácie antivírového programu, prípadne inštalovať aktualizácie, alebo zakúpiť kvalitnejší (z hľadiska bezpečnosti) antivírový program,
 skontrolovať všetky počítače zapojené do spoločnej LAN siete aktualizovaným antivírovým programom,
 detekovať spôsob narušenia,
 odstrániť príčiny,
 opraviť narušenú funkčnosť, opätovne skontrolovať systém antivírovým programom,
 prekontrolovať všetky PC, nájsť zdroj infiltrácie a zabezpečiť jeho eliminovanie,
 znovu spustiť systém a pripojiť užívateľov,
 inštalovať doplnkové programy uvedené v bode 4.2.4, ktoré eliminujú možnosť napadnutia počítača.

- Neautorizovaný vstup z internetu
– môže dôjsť k narušeniu integrity, odcudzeniu alebo strate a zneužitiu dát s osobnými údajmi
 preventívne opatrenia:
 nespúšťať programy z prostredia internetu nepodpísané certifikačnou autoritou,
 nesťahovať neautorizované programy z prostredia internetu,

 postup na zabezpečenie stavu obnovy.
 skontrolovať log súborov firewallu, routerov, antivírového programu a pod. a vyhodnotiť ich,
 zabezpečiť súborovú integritu OS a obnovu poškodených alebo infiltrovaných údajov zo záloh,
 zvýšiť bezpečnosť firewallov,
 nastaviť kryptované prenosy v LAN sieti, pokiaľ existuje prístup z internetu do lokálnej siete, je nutné, aby bol vytvorený iba kryptovaným prenosom minimálne cez protokol SSH a nepoužívalo sa pre autorizáciu a vstupov meno a heslo, ale privátne a verejné kľúče v minimálnej dĺžke 512 bite, optimálne 1024 bite,
 inštalovať doplnkové programy, ktoré eliminujú možnosť napadnutia počítača z internetu.

- Technické narušenie, alebo zlyhanie bezpečnosti zariadenia v IS
 pamäť počítača – môže dôjsť k narušeniu integrity alebo strate dát (v prípade vykazovania podozrivého správanie je nutná výmena),
 procesor - môže dôjsť k narušeniu integrity alebo strate dát (nutná výmena),
 CD/DVD RW - môže dôjsť k narušeniu integrity zálohovaných dát alebo strate dát (v prípade, že sa zistí na záložnom CD/DVD médiu sú nečitateľné alebo inak znehodnotené informácie nutná výmena zálohovacieho zariadenia),
 hard disk – tvorí najdôležitejšiu časť počítača a preto mu je potrebné venovať náležitú ochranu. Môže dôjsť k narušeniu integrity alebo strate dát (v prípade, že sa zistí, že na disku sú nečitateľné alebo inak znehodnotené údaje je nutná kontrola antivírusovým programom, prípadne výmena za nový a skopírovanie dát, ktoré neboli znehodnotené, alebo použiť dáta zo záloh),
 wifi zariadenie – môže dôjsť k úniku informácií a neautorizovanému vstupu do systému (nutná rekonfigurácia hesiel a v prípade nefunkčnosti celková výmena a konfigurácia). - Porucha napájania, strata dodávky elektrickej energie
 preventívne opatrenia:
 dôležité aktívne prvky siete je nutné chrániť záložnými zdrojmi elektrickej energie so stabilizátorom sieťového napätia,

 postup na zabezpečenie stavu obnovy:
 v čase výpadku sa musí záložný zdroj automaticky aktivovať,
 pri dlhodobejšom výpadku sa server musí automaticky vypnúť (shutdown),
 po nábehu el. energie je nutné server spustiť a skontrolovať.

- Porucha prostriedkov demilitarizovanej zóny
 preventívne opatrenia:
 monitorovať činnosť zariadení,
 monitorovať funkčnosť všetkých zariadení,
 zabezpečiť prístup len pre pracovníkov s oprávnením,
 periodicky meniť administrátorské a užívateľské prístupy s heslami,
 zabezpečiť antivírovú ochranu všetkých PC, ako aj e-mailového prístupu,

 zabezpečiť programovú aktuálnosť,
 zabezpečiť technickú aktuálnosť,
 kontrolovať súbory zaznamenávajúce činnosť systému,
 kontrolovať súbory,

 v prípade narušenia:
 odpojiť LAN od prostriedkov demilitarizovanej zóny
 vyhľadať príčinu nefunkčnosti,
 odstrániť príčinu výmenou častí, inštalovaním aktualizácií, výmenou celku,
 preveriť prostriedky firewallu, prekladu adries (DNS) a proxy,
 po otestovaní funkčnosti pripojiť LAN. - Porucha aktívnych prvkov IS/siete

 preventívne opatrenia:
 monitorovať činnosť,
 zabezpečiť dostatočnú kapacitu,
 pripájať ich prostredníctvom záložného zdroja,
 zabezpečiť dostatočnú ochranu pred nepovolaným prístupom.

 postup na zabezpečenie stavu obnovy:
 vymeniť nefunkčnú časť.

- Porucha pasívnej časti siete
 preventívne opatrenia:
 premerať a kontrolovať kabeláž, zásuvky a konektory, - postup na zabezpečenie stavu obnovy:

 opraviť, prípadne vymeniť chybnú časť. - Havária databáz

 preventívne opatrenia:
 sledovať konfiguračné súbory,
 monitorovať hlásenia programov a včas na ne reagovať,
 denne kontrolovať chybové hlásenia aplikácie a databázy,

 postup na zabezpečenie stavu obnovy:
 po odstránení nedostatkov a kontrole spätne inštalovať databázu zo zálohy.

- Havária aplikácie
 preventívne opatrenia:
 sledovať hlásenia aplikácie a zaznamenávať postrehy užívateľov,
 sledovať konfiguračné súbory,
 monitorovať hlásenia a včas na ne reagovať,
 denne kontrolovať chybové hlásenia aplikácie,

 postup na zabezpečenie stavu obnovy:
 preinštalovať aplikáciu,
 nainštalovať novšiu verziu aplikácie,
 konzultovať chyby s dodávateľom.

- Porucha pracovných staníc
 preventívne opatrenia:
 používať len autorizované programy,
 inštalovať antivírové programy,

 inštalovať nové programy smie len poverený zamestnanec,
 nezasahovať do konfiguračných súborov,
 chybové hlásenia hlásiť správcovi systému,
 zálohovať dáta na určené média,
 za zálohy, prevádzku a bezpečnosť zodpovedá zamestnanec.

 postup pre zabezpečenie stavu obnovy:
 technická chyba – zabezpečiť opravu nefunkčnej časti,
 softvérová chyba – identifikovať príčinu, obnoviť súbory zo zálohy, preinštalovať OS, aktualizovať antivírovú ochranu.

4. Mimoriadne udalosti spôsobené vplyvom zvyškových rizík

 preventívne opatrenia:
 zabezpečiť niekoľkonásobné záložné kópie,
 zhotovenie havarijných plánov na zabezpečenie kontinuity činnosti,
 kontrolovať, či sú splnené protipožiarne opatrenia,
 kontrolovať osoby pri vstupe do budovy,
 vo vybraných priestoroch inštalovať EZS, bezpečnostné mreže, dvere,
 zabezpečiť autentizáciu osôb pri vstupe do chránených priestorov,

 v prípade vyradenia IS z činnosti:
 zvolať krízový štáb,
 koordinovať činnosť podľa havarijných smerníc,
 aktivovať záložné pracovisko,
 skontrolovať úplnosť systému na záložnom pracovisku,
 spustiť záložnú prevádzku,
 odstrániť škody na pôvodnom pracovisku,
 po obnovení funkčnosti vrátiť činnosti na pôvodné pracovisko,

 v prípade napadnutia len časti IS:
 presunúť aktíva do vyhovujúcich priestorov,
 inštalovať záložné databázy a pripojenia ak sú nutné,
 spustiť prevádzku,
 po odstránení dôsledkov vrátiť činnosť do stavu pred udalosťou.

Metóda hodnotenia závažnosti porušenia bezpečnosti OÚ (SE)

Hlavné kritéria :

- Kontext spracúvania OÚ (skratka **DPC**)
Jadro hodnotenia, hodnotí kritickosť súboru údajov
- možnosť identifikácie DO (skratka **EI**)
Korekčný faktor, čím jednoduchšia identifikácia - tým vyššie počiatočné skóre
- Okolnosti porušenia (skratka **CB**)
- **SE = DPC x EI +CB**

Zdroj : Recommendations for methodology of the assessment of severity of personal data breacher.
www.enisa.europe.eu

DPC - OÚ zaradíme do kategórií :

- Jednoduché údaje (napr. meno, priezvisko, e-mail, údaje o vzdelaní, adresa) základné skóre **= 1**
DPC = 1, ak nie sú priťažujúce faktory
DPC = 2, ak je možné profilovať, finančný a sociálny stav
DPC = 3, ak je možné získať údaje o zdravotnom stave
DPC = 4, zraniteľné skupiny, osobná bezpečnosť, fyzická bezpečnosť
- Behaviorálne údaje, základné skóre **= 2**
- Finančné údaje , základné skóre **= 3**
- Citlivé údaje, základné skóre **= 4**

EI - možnosť identifikácie DO

- EI = 0,25 zanedbateľné (e-mail neobsahuje žiadne identifikačné údaje a nevyužíva sa na fórach, soc.sieťach)
- EI = 0,5 obmedzené
- EI = 0,75 významné (e-mail neobsahuje žiadne identifikačné údaje a využíva sa však na fórach, soc.sieťach)
- EI = 1 maximálne (e-mail obsahuje identifikačné údaje a využíva sa na fórach, soc.sieťach)

CB - okolnosti porušenia

- CB = 0, OÚ boli nesprávne aktualizované, údaje však neboli použité, poškodenie DB, je však možné ju ihneď obnoviť z vytvorených záloh.
- CB = 0,25, email s osobnými údajmi bol odoslaný známym príjemcom, niektorí zákazníci získali prístup k účtom iných zákazníkov, poškodenie DB - OÚ musia byť opäť získané od jednotlivca.
- CB = 0,5 , zverejnenie OÚ útočníkom, zamestnanec úmyselne predal OÚ zákazníkov inej spoločnosti - škodlivý zámer.

SE = DPC x EI +CB

- SE < 2 nízka, jednotlivci nebudú ovplyvnení, alebo
sa môžu stretnúť s drobnými nepríjemnosťami
- 2 < = SE < 3 stredná, jednotlivci budú ovplyvnení,
nepríjemnosti je možné prekonať (obmedzenie prístupu k službe, dodatočné náklady, nedostatok porozumenia)
- 3 < = SE < 4 vysoká, významné dôsledky na jednotlivca (finančné straty, strata zamestnania)
- 4 < = SE < veľmi vysoká, nezvratné následky pre jednotlivca, ktoré nemusia prekonať (psychické problémy, finančné ťažkosti)

Príklad :
1. Krádež e-mailových kontaktov :

DPC = 1 (žiadne priťažujúce faktory)
EI = 1 (predpokladáme, že DO je možné identifikovať
CB = 0,5 (škodlivý zámer)

SE = 1 x 1 + 0,5 = 1,5 (nízke riziko)

2. Krádež údajov z vernostného programu lekárne

DPC = 3 (z údajov možno získať informácie o zdravotnom stave)
EI = 1 (DO je možné identifikovať)
CB = 0,5 (škodlivý zámer)

SE = 3 x 1 + 0,5 = 3,5

NÁVRHY NA
VYPRACOVANIE – AKTUALIZÁCIU - ZRUŠENIE
OPATRENÍ

Názov opatrenia:

Text:

….....

….....

….....

….....

Návrh vypracoval		**Návrh schválil**	
Meno a priezvisko:		Meno a priezvisko:	
Pracovná pozícia:		Pracovná pozícia:	
Dátum:		Dátum:	
Podpis:		Podpis:	

List č.: .....

Záznam o vykonanom školení pracovníkov dňa ……...

Poradové číslo	Meno, priezvisko	Pracovná pozícia	Podpis pracovníka

.

.

.

Predmet školenia: Poučenie oprávnenej osoby formou interaktívneho videoškolenia

(otázky-odpovede online)

Téma školenia:

- GDPR , zákon 18/2018 Z.z.

…….

Nad absolvovaním videoškolenia dohliadal

(

m

e

n

o

,