ZOZNAM BEZPEČNOSTNÝCH OPATRENÍ NA ZABEZPEČENIE OCHRANY OSOBNÝCH ÚDAJOV

1. Technické opatrenia

1. Technické opatrenie realizované prostriedkami fyzickej povahy

1.1. Zabezpečenie objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarna signalizácia).
1.2. Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu (napr. steny, mreže alebo presklenia).
1.3. Umiestnenie dôležitých prostriedkov informačných technológií v chránenom priestore a ochrana informačnej infraštruktúry pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia.

1.4. Bezpečné uloženie fyzických nosičov osobných údajov vrátane bezpečného uloženia listinných dokumentov.

1.5. Opatrenie pre zamedzenie náhodného prečítania osobných údajov zo zobrazovacích jednotiek (napr. vhodné umiestnenie zobrazovacích jednotiek).

2. Ochrana pred neoprávneným prístupom

2.1. Šifrová ochrana uložených a prenášaných údajov, pravidlá pre kryptografické opatrenia.
2.2. Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza.

3. Riadenie prístupu poverených osôb

3.1. Riadenie prístupov a opatrenia na zaručenie platných politík riadenia prístupov (napr. identifikácia, autentizácia a autorizácia osôb v informačnom systéme).
3.2. Riadenie privilegovaných prístupov v informačných systémoch.
3.3. Zaznamenávanie prístupu a aktivít poverených osôb v informačnom systéme.

4. Riadenie zraniteľností

4.1. Opatrenia pre detekciu a odstránenie škodlivého kódu a nápravu následkov škodlivého kódu.
4.2. Ochrana pred nevyžiadanou elektronickou poštou.
4.3. Používanie legálneho a prevádzkovateľom schváleného softvéru.
4.4. Opatrenia pre zaručenie pravidelnej aktualizácie operačných systémov a programového aplikačného vybavenia.
4.5. Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete a spôsob ich overovania. Filtrovanie sieťovej komunikácie.
4.6. Zhromažďovanie informácií o technických zraniteľnostiach informačných systémov, vyhodnocovanie úrovne rizík a implementácia opatrení na potlačenie týchto rizík.

5. Sieťová bezpečnosť

5.1. Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou.
5.2. Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástrojov sieťovej bezpečnosti (napr. firewall), segmentácia počítačovej siete.
5.3. Pravidlá prístupu do verejne prístupnej počítačovej siete, opatrenia pre zamedzenie pripojenia k určitým adresám, pravidlá pre používanie sieťových protokolov.
5.4. Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok).
5.5. Aktualizácia operačného systému a programového aplikačného vybavenia.

6. Zálohovanie

6.1. Test funkčnosti záložných dátových nosičov.
6.2. Vytváranie záloh s vopred zvolenou periodicitou.
6.3. Určenie doby uchovávania záloh a kontrola jej dodržiavania.
6.4. Test obnovy informačného systému zo zálohy.
6.5. Bezpečné ukladanie záloh.

7. Likvidácia osobných údajov a dátových nosičov

7.1. Technické opatrenia pre bezpečné vymazanie osobných údajov z dátových nosičov.
7.2. Zariadenie na mechanické zničenie dátových nosičov osobných údajov (napr. zariadenie na skartovanie listín a dátových médií).

2. Organizačné opatrenia

1. Personálne opatrenia

1.1. Poverenie osoby prevádzkovateľom alebo sprostredkovateľom, ktorá má prístup k osobným údajom.
1.2. Pokyny prevádzkovateľa na spracúvanie osobných údajov, najmä
- 1.2.1. vymedzenie osobných údajov, ku ktorým má mať konkrétna osoba prístup na účel plnenia jej povinností alebo úloh,
- 1.2.2. určenie postupov, ktoré je poverená osoba povinná uplatňovať pri spracúvaní osobných údajov,
- 1.2.3. vymedzenie základných postupov alebo operácií s osobnými údajmi,
- 1.2.4. vymedzenie zodpovednosti za porušenie zákona alebo osobitného predpisu[1)].

1.3. Poučenie poverených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov).
1.4. Určenie zodpovednej osoby.
1.5. Vzdelávanie poverených osôb (napr. právna oblasť, oblasť informačných technológií).
1.6. Postup pri ukončení pracovného alebo obdobného pomeru poverenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti).
1.7. Práca na diaľku a pravidlá mobilného spracovania dát.

2. Riadenie aktív

2.1. Vedenie inventárneho zoznamu aktív a jeho pravidelná aktualizácia.
2.2. Evidencia všetkých miest prepojenia sietí vrátane prepojení s verejne prístupnou počítačovou sieťou.
2.3. Určenie vlastníctva aktív a zodpovednosti za riziká.
2.4. Pravidlá a postupy pre klasifikáciu informácií.
2.5. Pravidlá a postupy na označovanie informácií a zaobchádzanie s nimi v súlade s platnou klasifikačnou schémou.
2.6. Pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií.
2.7. Opatrenia pre vrátenie aktív (napr. prostriedkov spracúvania osobných údajov) patriacich prevádzkovateľovi po ukončení pracovného pomeru, po vypršaní uzatvorenej dohody alebo zmluvy, pri zmene pracovného miesta alebo pracovného zaradenia a pod.

3. Riadenie prístupu osôb k osobným údajom

3.1. Pravidlá fyzického vstupu do objektu a chránených priestorov prevádzkovateľa.
3.2. Správa kľúčov (individuálne prideľovanie kľúčov, bezpečné uloženie rezervných kľúčov).
3.3. Pravidlá pre prideľovanie prístupových práv a úrovní prístupu (rolí) povereným osobám.
3.4. Politika hesiel a pravidlá používania autorizačných a autentizačných prostriedkov.
3.5. Pravidlá pre vzájomné zastupovanie poverených osôb (napr. v prípade nehody, dočasnej pracovnej neschopnosti, ukončenia pracovného alebo obdobného pomeru).
3.6. Pravidlá pre odstránenie alebo zmenu prístupových práv poverených osôb a zariadení na spracúvanie informácií pri ukončení zamestnania, zmluvy alebo dohody, prípadne prispôsobenie zmenám rolí.

4. Organizácia spracúvania osobných údajov

4.1. Pravidlá spracúvania osobných údajov v chránenom priestore.
4.2. Nepretržitá prítomnosť poverenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako poverené osoby.
4.3. Režim údržby a upratovania chránených priestorov.
4.4. Pravidlá spracúvania osobných údajov mimo chráneného priestoru, ak sa také spracúvanie predpokladá
4.4.1. pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, fotografie) mimo chránených priestorov a vymedzenie zodpovedností,
4.4.2. pravidlá používania automatizovaných prostriedkov spracúvania (napr. notebooky) mimo chránených priestorov a vymedzenie zodpovedností,
4.4.3. pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovedností.

5. Likvidácia osobných údajov

5.1. Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých poverených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov).

6. Porušenia ochrany osobných údajov

6.1. Postup pri oznamovaní porušenia ochrany osobných údajov úradu a dotknutej osobe na účel včasného prijatia preventívnych alebo nápravných opatrení.
6.2. Pravidelné preskúmavanie záznamov udalostí, záznamov o aktivitách používateľov, záznamov o výnimkách.
6.3. Evidencia porušení ochrany osobných údajov a použitých riešení.
6.4. Postup pre identifikáciu a riešenie jednotlivých typov porušení ochrany osobných údajov.
6.5. Postup pre odstraňovanie následkov porušení ochrany osobných údajov.
6.6. Postupy zaručenia kontinuity pri haváriách, poruchách a iných mimoriadnych situáciách.
6.7. Postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania.

7. Kontrolná činnosť

7.1. Kontrolná činnosť zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov).
7.2. Informovanie osôb o kontrolnom mechanizme[1], ak je u prevádzkovateľa alebo sprostredkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania).
7.3. Postupy pre monitorovanie súladu spracúvania osobných údajov podľa § 9.

8. Dodávateľské vzťahy

8.1. Postup pre overenie dostatočných záruk.
8.2. Začlenenie požiadaviek na ochranu údajov do požiadaviek pre nové systémy a do pravidiel pre vývoj a nákup systémov.
8.3. Začlenenie požiadaviek na ochranu údajov do zmluvných vzťahov s dodávateľmi a tretími stranami.
8.4. Testovanie bezpečnostných funkcií počas vývoja systémov.
8.5. Monitorovanie a pravidelné preskúmavanie úrovne bezpečnosti služieb poskytovaných dodávateľmi.