Bezpečnostný projekt na ochranu osobných údajov

1. Účel

Bezpečnostný projekt Strednej priemyselnej školy elektrotechnickej je vypracovaný v zmysle zákona č. 122/2013 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. Obsah bezpečnostného projektu zodpovedá požiadavke vyhlášky č. 164/2013 Z.z. Úradu na ochranu osobných údajov Slovenskej republiky z 13. júna 2013 o rozsahu a dokumentácii bezpečnostných opatrení. Obsahom Bezpečnostného projektu sú:

- vysvetlenie základných pojmov,
- názov informačných systémov, na ktoré sa vzťahuje,
- bezpečnostný zámer,
- analýza bezpečnosti informačných systémov,
- bezpečnostná smernica.

Vysvetlenie základných pojmov

Informačný systém osobných údajov – informačný systém, v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe. Informačným systémom je aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracovanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania.
Osobné údaje – údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej, či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.
Dotknutá osoba – každá fyzická osoba, ktorej sa osobné údaje týkajú.
Prevádzkovateľ – každý, kto sám alebo spoločne s inými vymedzí účel spracúvania osobných údajov, určí podmienky spracúvania a spracúva osobné údaje vo vlastnom mene.
Sprostredkovateľ – každý, kto spracúva osobné údaje v mene prevádzkovateľa, v rozsahu a za podmienok dojednaných s prevádzkovateľom v písomnej zmluve.
Oprávnená osoba – každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania alebo v rámci výkonu verejnej funkcie, a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení podľa § 21 zákona.
Tretia strana – každý, kto nie je dotknutou osobou, prevádzkovateľom poskytujúcim osobné údaje, jeho zástupcom, sprostredkovateľom alebo oprávnenou osobou.
Príjemca – každý, komu sú osobné údaje poskytnuté alebo sprístupnené, pričom príjemcom môže byť aj tretia strana: prevádzkovateľ, ktorý spracúva osobné údaje na základe § 3 ods. 1 písm. g) a úrad, ktorý plní úlohy ustanovené týmto zákonom sa nepovažujú za príjemcu.
Adresa – súbor údajov o pobyte fyzickej osoby, do ktorého patria názov ulice, orientačné, prípadne súpisné číslo domu, názov obce, prípadne názov časti obce, poštové smerovacie číslo, názov okresu, názov štátu.
Anonymizovaný údaj – osobný údaj upravený do takej podoby, v ktorej ho nemožno priradiť dotknutej osobe, ktorej sa týka.
Účel spracúvania osobných údajov – vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť.

Súhlas dotknutej osoby – akýkoľvek slobodne daný výslovný a zrozumiteľný prejav vôle, ktorým dotknutá osoba na základe poskytnutých informácií vyjadruje súhlas so spracovaním svojich osobných údajov.
Likvidácia osobných údajov – likvidácia tých osobných údajov, ktorých účel spracúvania sa skončil. Po skončení účelu spracúvania možno osobné údaje ďalej spracúvať len za podmienok ustanovených v odseku 5, § 6 zákona č. 122/2013 Z.z.
Zástupca prevádzkovateľa – každý, kto na území Slovenskej republiky zastupuje prevádzkovateľa so sídlom, organizačnou zložkou, prevádzkarňou alebo trvalým pobytom v tretej krajine.
Tretia krajina – krajina, ktorá nie je členským štátom Európskej únie alebo Dohody o Európskom hospodárskom priestore.
Aktívum – čokoľvek, čo má pre organizáciu hodnotu.
Dostupnosť – schopnosť byť dostupný a použiteľný na požiadanie autorizovanej entity.
Dôvernosť – vlastnosť, na základe ktorej informácie nie sú sprístupňované a odhaľované neautorizovaným osobám, entitám a procesom.
Integrita – vlastnosť zabezpečujúca presnosť a kompletnosť aktív.
Zostatkové riziko – riziko zostávajúce po ošetrenie rizík.
Akceptácia rizika – rozhodnutie prijať určité riziko.
Incident – jedna alebo viaceré neželané a neočakávané udalosti informačnej bezpečnosti, pri ktorých je vysoká pravdepodobnosť kompromitácie aktivít spoločnosti a ohrozenia informačnej bezpečnosti.
Informačná bezpečnosť – zachovanie dôvernosti, integrity a dostupnosti informácií, navyše sa môže týkať aj ďalších vlastností, akými sú autenticita, sledovateľnosť, nemožnosť poprieť zodpovednosť a spoľahlivosť.
Analýza rizík – systematické používanie informácií na identifikovanie zdrojov a odhad rizika.
Dozorný organ – nezávislý orgán verejnej moci zriadený členským štátom podľa článku 41 nariadenia 680/2016.

2. Názov informačných systémov

1. **Informačný systém Vzdelávanie - žiaci**
2. **Informačný systém Personalistika a mzdy**
3. **Informačný systém Knižnica**
4. **Informačný systém Ubytovanie - žiaci**
5. **Informačný systém Ubytovanie - verejnosť**
6. **Informačný systém Právne vzťahy**
7. **Informačný systém Verejné obstarávanie**
8. **Informačný systém Správa registratúry**
9. **Informačný systém Vrátnica**
10. **Informačný systém Oprávnené osoby**
11. **Informačný systém Účtovníctvo**
12. **Informačný systém Evidencia odbornej spôsobilosti elektrotechnikov**
13. **Informačný systém Sťažnosti**
14. **Informačný systém WASET**
15. **Informačný systém Kamerový systém**

3. Bezpečnostný zámer

Bezpečnostný zámer vymedzuje spoločné základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu osobných údajov pred ohrozením ich bezpečnosti v informačných systémoch uvedených v časti 2., v ktorých sa spracúvajú osobné údaje, pričom je potrebné vziať do úvahy spôsob ich spracúvania vzhľadom na mieru automatizáciu jednotlivých činností v jednotlivých informačných systémoch.
Údaje sú spracúvané spôsobom, ktorý zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, likvidáciou alebo

poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení. (Zdroj: nariadenie 679 Kap II, Cl. 4, ods 1., f)
Prostredníctvom bezpečnostného projektu a súvisiacich interných dokumentov a smerníc boli navrhnuté procesné a technologické opatrenia pre:

a) zabránenie neoprávnenému prístupu k zariadeniam na spracúvanie, ktoré sa používajú na spracúvanie (kontrola prístupu k zariadeniam),
b) zabránenie neoprávnenému čítaniu, kopírovaniu, pozmeňovaniu alebo odstráneniu nosičov údajov (kontrola nosičov údajov),
c) zabránenie neoprávnenému vkladaniu osobných údajov a neoprávnenému prehliadaniu, pozmeňovaniu alebo vymazaniu uchovávaných osobných údajov (kontrola uchovávania),
d) zabránenie použitiu systémov automatizovaného spracúvania neoprávnenými osobami pomocou zariadenia na prenos údajov(kontrola užívateľa),
e) zabezpečenie, aby osoby oprávnené používať systém automatizovaného spracúvania mali prístup iba k tým osobným údajom, na ktoré sa vzťahuje ich oprávnenie na prístup (kontrola prístupu k údajom),
f) zabezpečenie, aby bolo možné overiť a zistiť subjekty, ktorým sa preniesli alebo poskytli, alebo môžu preniesť alebo poskytnúť osobné údaje prostredníctvom zariadenia na prenos údajov (kontrola prenosu údajov),
g) zabezpečenie, aby bolo následne možné overiť a zistiť, aké osobné údaje sa vložili do systému automatizovaného spracúvania, a kedy a kto ich tam vložil (kontrola vkladania),
h) zabránenie neoprávnenému čítaniu, kopírovaniu, pozmeňovaniu alebo vymazaniu osobných údajov počas ich prenosu alebo počas prepravy nosiča údajov (kontrola prepravy),
i) zabezpečenie, aby sa inštalované systémy mohli v prípade prerušenia obnoviť (obnova),
j) zabezpečenie, aby funkcie systému fungovali, aby sa výskyt chýb v jeho funkciách hlásil (spoľahlivosť) a aby sa uchovávané osobné údaje nemohli v prípade poruchy systému poškodiť (integrita).

(Zdroj: nariadenie 679 Kap II, Cl. 29.)

3.1 Formulácia základných bezpečnostných cieľov a požadované bezpečnostné opatrenia

3.1.1 Zabrániť neautorizovanému fyzickému prístupu, strate, poškodeniu a ohrozeniu priestorov a informácií prevádzkovateľa.

Požadované bezpečnostné opatrenia v podmienkach prevádzkovateľa:

3.1.1.1 Vstup do priestorov prevádzkovateľa, kde sú spracúvané osobné údaje je riadený, zabezpečený cez vstupné uzamykateľné dvere, oddelený od ostatných častí objektu.
3.1.1.2 Oprávnená osoba vždy uzamyká miestnosť, v ktorej sú uložené osobné údaje, keď z nej odchádza ako posledná.
3.1.1.3 Všetky prvky zariadení obsahujúce úložné média pre dáta musia byť skontrolované, aby sa zabezpečilo, že všetky citlivé dáta a licencovaný softvér boli bezpečne zmazané alebo boli prepísané pred vyradením zariadení, o čom musí byť písomný záznam.
3.1.1.4 Osobné údaje v papierovej podobe musia byť primerane chránené pred stratou, zničením, prezradením, neoprávnenému použitiu, náhodnej zámene.
3.1.1.5 Prevádzkovateľ na ničenie fyzických nosičov osobných údajov používa vhodné zariadenia.

3.1.2 Zabezpečiť autorizovaný prístup používateľov a zabrániť neautorizovanému prístupu do informačných systémov alebo krádeži informácií.

Požadované bezpečnostné opatrenia v podmienkach prevádzkovateľa:

3.1.2.1 Od zamestnancov prevádzkovateľa sa vyžaduje, aby zaisťovali primeranú ochranu nestrážených prostriedkov.
3.1.2.2 Prístup k uloženým údajom v jednotlivých aplikáciách vyžadujú zadanie prístupových údajov – meno a heslo.
3.1.2.3 Používatelia musia mať prístup iba k službám, na ktoré sú autorizovaní.
3.1.2.4 Pri práci s heslom je potrebné dodržiavať:

- 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 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.

3.1.2.5 Prístup tretích strán k informačnému systému je riadený pravidlami.

3.1.3 Chrániť integritu softvéru a informácií

Požadované bezpečnostné opatrenia v podmienkach prevádzkovateľa:

3.1.3.1 Sú implementované opatrenia detekcie prítomnosti škodlivého kódu v prichádzajúcej elektronickej pošte a v iných súboroch prijímaných z verejne prístupnej počítačovej siete.

3.1.3.2 Prevádzkovateľ používa iba legálny softvér.

3.1.3.3 Prevádzkovateľ má zabezpečenú ochranu pred nevyžiadanou elektronickou poštou a sú nastavené obmedzenia pre sťahovanie súborov z verejne prístupnej počítačovej siete.

3.1.4 Udržiavať integritu a dostupnosť informácií a prostriedkov na ich spracúvanie

Požadované bezpečnostné opatrenia v podmienkach prevádzkovateľa:

3.1.4.1 Pravidelná tvorba záložných kópií.

3.1.4.2 Bezpečné uloženie záložných kópií.

3.1.4.3 Testovanie funkčnosti záložných kópií.

3.1.5 Zabrániť neautorizovanému prezradeniu, modifikácii, odstráneniu alebo zničeniu aktív

Požadované bezpečnostné opatrenia v podmienkach prevádzkovateľa:

3.1.5.1 V prípade, že sú na prenosné počítačové média ukladané osobné údaje a iné citlivé informácie je potrebné, aby oprávnená osoba venovala zvýšenú pozornosť ich uloženiu, je zakázané ich nechávať bez dozoru (napr. voľne položený USB kľúč na stole, ponechanie notebooku v kufri auta a pod.).

3.1.5.2 Média, ak už nie sú potrebné musia byť bezpečne zlikvidované.

3.1.5.3 Aktualizáciu operačného systému a aplikačného vybavenie môže vykonávať iba administrátor IT.

3.1.5.4 Prideľovanie prístupových práv a úroveň prístupu je riadená a zdokumentovaná.

3.1.6 Zabezpečiť, že zamestnanci, zmluvní partneri a používatelia v pozícii tretích strán rozumeli svojim zodpovednostiam, a že sú vhodní na výkon rolí, ktoré im boli pridelené.

Požadované bezpečnostné opatrenia v podmienkach prevádzkovateľa:

3.1.6.1 Zamestnanci, zmluvní partneri a používatelia v pozícii tretích strán musia odsúhlasiť a podpísať v pracovnej zmluve alebo inej zmluve ustanovenia, ktoré musia definovať zodpovednosť za informačnú bezpečnosť v rámci prevádzkovateľa.

3.1.6.2 Oboznámenie oprávnených osôb s bezpečnostnými opatreniami.

3.1.6.3 Vzdelávanie oprávnených osôb v oblasti ochrany a bezpečnosti osobných údajov.

3.1.6.4 Prístupové práva všetkých zamestnancov, musia byť po ukončení pracovnoprávneho pomeru alebo dohody odňaté alebo upravené podľa zmeny.

3.1.6.5 Všetci zamestnanci musia vrátiť akékoľvek aktíva patriace organizácii po zrušení ich pracovného pomeru, resp. zmluvy alebo dohody.

3.1.6.6 Poverenie zodpovednej osoby nad dohľadom spracúvania osobných údajov.

3.1.7 Dosiahnuť a udržiavať primeranú ochranu aktív organizácie

Požadované bezpečnostné opatrenia v podmienkach prevádzkovateľa:

3.1.7.1 Všetky aktíva musia byť jednoznačne identifikované a musí byť udržiavaný ich zoznam.

3.1.7.2 Za jednotlivé druhy aktív je jednoznačne pridelená zodpovednosť.

3.1.7.3 Na riadenie prístupu vzdialených používateľov sú použité primerané autentizačné metódy.

3.1.7.4 Sú nastavené pravidlá prístupu do verejne prístupnej počítačovej siete (zamedzenie pripojenia k určitým webovým sídlam).

3.1.7.5 Prístup do verejnej počítačovej siete je chránený prostredníctvom vhodného firewallu.

3.1.8 Zabezpečiť, aby udalosti a incidenty informačnej bezpečnosti boli oznamované spôsobom, ktorý umožní včas poskytnúť potrebné nápravné opatrenia.

Požadované bezpečnostné opatrenia v podmienkach prevádzkovateľa**:**

3.1.8.1 Udalosti informačnej bezpečnosti musia byť nahlásené prostredníctvom primeraných riadiacich kanálov.

3.1.8.2 Od všetkých zamestnancov, zmluvných partnerov a používateľov, ktorí využívajú informačné systémy a služby sa musí vyžadovať zaznamenávanie a ohlasovanie spozorovaných a potenciálnych bezpečnostných slabín v systémoch.

3.1.8.3 Musia byť zavedené zodpovednosti a postupy, s cieľom zaistiť rýchlu, efektívnu a systematickú odozvu na incidenty informačnej bezpečnosti.

3.1.9 Zabrániť závažným zlyhaniam alebo havárii informačného systému a zabezpečiť jeho včasnú obnovu.

Požadované bezpečnostné opatrenia v podmienkach prevádzkovateľa:

3.1.9.1 V rámci organizácie musí byť vyvinutý a udržiavaný riadený proces pre kontinuitu činností, ktorý zohľadňuje požiadavky na informačnú bezpečnosť.

3.1.10 Vyhnúť sa porušeniu zákonných požiadaviek na spracúvanie osobných údajov.

Požadované bezpečnostné opatrenia v podmienkach prevádzkovateľa:

3.1.10.1 Zabezpečiť, aby všetky oprávnené osoby mali dostupnú dokumentáciu prevádzkovateľa k ochrane osobných údajov.

3.1.10.2 Zabezpečiť aktualizáciu dokumentácie o ochrane osobných údajov v prípade legislatívnych zmien.

3.1.10.3 Zabezpečiť, aby všetky oprávnené osoby poznali a dodržiavali podmienky spracúvania osobných údajov ustanovených zákonom č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov.

3.1.10.4 Dodržiavanie lehoty pre časovo nevyhnutné spracovanie osobných údajov je kontrolované každoročne interným auditom. (Zdroj: nariadenie 679 Kap II, Cl. 5, ods 1.)

3.1.10.5 Pro zistení prenosu alebo použitia nesprávnych údajov alebo ich nezákonného prenosu či zverejnenia bude táto situácia bezodkladne oznámená príjemcovi. Bezodkladne sa zaistí oprava, výmaz údajov alebo sa obmedzí ich spracúvanie v súlade s článkom 16 NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679. (Zdroj: nariadenie 679 Kap II, Cl. 7, ods 3.)

3.1.11 Zabezpečenie kontrolnej činnosti v oblasti prijatých bezpečnostných opatrení

Požadované bezpečnostné opatrenia v podmienkach prevádzkovateľa:

3.1.11.1 Výkon kontrolnej činnosti je vykonávaný v rámci interných auditov podľa dokumentovaného postupu o interných auditoch v rámci SMK. Kontrolnú činnosť riadi a vykonáva zodpovedná osoba v zmysle zákona č. 122/2013 Z.z.

3.1.11.2 Súčasťou interného auditu je kontrola integrity a kvality uložených osobných údajov. V prípade zistenia nesprávnosti, neúplnosti alebo neaktuálnosti sa takéto údaje nebudú prenášať a poskytovať. Bude posúdené ich odstránenie prípadne zaistenie opravy a aktualizácie. (Zdroj: nariadenie 679 Kap II, Cl. 7, ods 2.)

3.2 Špecifikácia opatrení na zabezpečenie ochrany osobných údajov v informačných systémoch prevádzkovateľa

3.2.1 Technické opatrenia

Stredná priemyselná škola elektrotechnická je na adrese Plzenská 1, Prešov. Vstup do budovy je cez informátorku. Návštevy sú informátorkou zapísané do knihy jednorazových vstupov fyzických osôb.

3.2.1.1 Technické opatrenia realizované prostriedkami fyzickej povahy

Miestnosti, v ktorej sa spracúvajú osobné údaje sú oddelené priečkami a vstupné dvere oprávnené osoby uzamykajú pri opustení miestnosti, keď odchádzajú ako posledné. Na prvom

poschodí v trakte, kde sú kancelárie riaditeľa školy, zástupcov, hospodárky je inštalovaný elektronický zabezpečovací systém. Papierové dokumenty s osobnými údajmi sú uložené v zásuvkách alebo regáloch. Všetky papierové záznamy, ktoré sa nearchivujú sú skartované v skartovači.

3.2.1.2 Ochrana pred neoprávneným prístupom

Osobné údaje v papierovej podobe sú uložené v zásuvkách. Prístup do počítačov je prostredníctvom mena a hesla. V prípade prenosu osobných údajov prostredníctvom e-mailovej komunikácie je zakázané v tele e-mailu uvádzať osobné údaje. Tieto môžu byť pripojené iba ako prílohy.

3.2.1.3 Riadenie prístupu oprávnených osôb

O zriadení prístupu pre oprávnenú osobu rozhoduje jej nadriadený v zmysle platnej organizačnej štruktúry prevádzkovateľa.

3.2.1.4 Ochrana proti škodlivému kódu

Počítače majú nainštalovaný antivírový program, ktorý je nastavený na automatickú aktualizáciu. Spoločnosť používa iba legálny softvér.

3.2.1.5 Sieťová bezpečnosť a bezpečnosť aplikácie

Prístup na internet je chránený prostredníctvom firewall. Softvérové aplikácie sú aktualizované podľa doporučení výrobcov softvéru. Za aktualizáciu zodpovedá správca IT.

3.2.1.6 Zálohovanie

Prevádzkovateľ zabezpečuje zálohovanie ASC agendy na lokálny disk PC. Zálohované sú PC riaditeľa školy zástupcov a sekretariátu na dátové úložisko.

3.2.1.7 Likvidácia osobných údajov a dátových nosičov

Všetky dokumenty, doklady v papierovej forme sú uložené v zásuvkách alebo policiach s prístupom iba určených oprávnených osôb. Osobné údaje v papierovej forme sú archivované pokiaľ to vyžaduje zákon, inak po splnení účelu spracúvania sú likvidované v skartovacom stroji. V prípade likvidácie elektronických dátových nosičov vedenie školy a zodpovední pracovníci sú si vedomí, že všetky prvky zariadení obsahujúce úložné média pre dáta musia byť skontrolované, aby sa zabezpečilo, že všetky citlivé dáta a licencovaný softvér boli bezpečne zmazané alebo boli prepísané pred vyradením zariadení o čom musí byť písomný záznam.

3.2.1.8 Aktualizácia operačného systému

Operačný systém je na počítačoch nastavený na automatickú aktualizáciu..

3.2.2 Organizačné opatrenia

3.2.2.1 Vedenie zoznamu aktív a jeho aktualizácia

Prevádzkovateľ vedie zoznam informačných aktív, ktoré obsahujú osobné údaje v rámci analýzy bezpečnosti informačného systému. Pracovníci používajú iba aktíva zamestnávateľa.

3.2.2.2 Riadenie prístupu oprávnených osôb k osobným údajom

Prístup pracovníkov prevádzkovateľa do informačných systémov schvaľuje príslušný vedúci pracovník podľa platnej organizačnej štruktúry prevádzkovateľa. K listinnej forme osobných údajov majú prístup iba určené oprávnené osoby.

3.2.2.3Organizácia spracúvania osobných údajov:

<u>Informačný systém Vzdelávanie – žiaci</u>

Informačný systém je prevádzkovaný na softvéri AsC. Zápis žiaka do agendy AsC je na základe dotazníka od žiaka, ktorý zabezpečuje triedny učiteľ. Údaje z dotazníka do systému AsC zadáva administratíva asistentka. Aktualizácia údajov sa vykonáva na začiatku školského roka alebo podľa potreby prostredníctvom informácií od triednych učiteľov. Dotazník po spracovaní je uložený u triedneho učiteľa. Po ukončení štúdia žiaka je dotazník zlikvidovaný. Prístup k AsC agende žiacka knižka majú všetci učitelia podľa ročníkov a predmetov, ktoré vyučujú a vedúci metodických útvarov. Papierová dokumentácia v rámci informačného systému Vzdelávanie – žiaci obsahuje prihlášku na štúdium a zápisný lístok, ktoré sú uložené u triedneho učiteľa, triedne knihy uložené v zborovni, katalógové listy a protokoly o maturitnej skúške sú uložené v trezore. V rámci systému sa spracúvajú údaje o žiakoch v zmysle Zákon č. 245/2008 Z. z. o výchove a vzdelávaní (školský zákon) a o zmene a doplnení niektorých zákonov.

Informačný systém Personalistika a mzdy

Oprávnené osoby strednej priemyselnej školy elektrotechnickej získavajú osobné údaje od dotknutých osôb do informačného systému Mzdy a personalistika len pre účely vedenia personálnej a mzdovej agendy pracovníkov prevádzkovateľa pre účely pracovnoprávne, mzdové a pre účely zdravotného a sociálneho poistenia, starobného dôchodkového sporenia a dane z príjmov zo závislej činnosti zamestnancov prevádzkovateľa v pracovnom pomere, ako aj osôb vykonávajúcich činnosti pre prevádzkovateľa na základe dohôd o vykonaní práce, dohôd o pracovnej činnosti, mandátnych zmlúv mimo pracovného pomeru v zmysle ustanovení Zákonníka práce. Kopírovanie alebo skenovanie úradných dokladov s osobnými údajmi je možné iba na základe písomného súhlasu dotknutej osoby. Osobné údaje získavajú oprávnené osoby do informačného systému Mzdy a personalistika bez súhlasu dotknutej osoby. Oprávnená osoba prevádzkovateľa však zabezpečí preukázateľné poučenie dotknutej osoby.

Dotknutými osobami sú:

- zamestnanci prevádzkovateľov v pracovnoprávnom vzťahu a ich rodinní príslušníci,
- osoby vykonávajúce činnosť pre prevádzkovateľov na základe dohôd o vykonaní práce a dohôd o pracovnej činnosti mimo pracovného pomeru.

Oprávnená osoba, ktorou je pracovníčka miezd a personalistiky, získava osobné údaje do informačného systému od pracovníka prevádzkovateľa písomne. Pravdivosť osobných údajov je potrebné vždy overiť. Osobné údaje v Mzdovom a personálnom systéme sa spracúvajú v softvéri MAGMA, ktorý je prevádzkovaný v sieti VUCnet Prešovského kraja cez vzdialený prístup. Dochádzkový systém je na základe čipových kariet bez osobných údajov v softvéri spoločnosti Tangram. Papierové záznamy sú uložené v miestnosti mzdovej účtovníčky. Po splnení účelu spracúvania sú osobné údaje bezpečne zlikvidované okrem osobných údajov, ktoré je potrebné archivovať v zmysle platnej legislatívy.

Informačný systém Knižnica

Evidujú sa osobné údaje žiakov a učiteľov, ktorí využívajú služby knižnice. Pred zavedením do knižničného informačného systému záujemca vyplní dotazník, ktorý obsahuje: meno a priezvisko, bydlisko, číslo občianskeho preukazu, e-mail a telefónne číslo a triedu u žiakov. Na základe vyplneného dotazníka asistentka centra záujmového vzdelávania zaeviduje záujemcu do softvéru knižničného informačného systému. Papierové dotazníky sú uložené v zásuvke asistentky. Keď žiak ukončí školu osobné údaje v softvéri knižničného informačného systému asistentka vymaže.

Informačný systém Ubytovanie – žiaci

Osobné údaje o žiakoch sú spracúvané v zmysle vyhlášky 236 MŠ z 3. júna 2009 o školskom internáte. Osobné údaje sú v papierovej aj elektronickej forme. Osobné údaje sú získané zo žiadosti o prijatie do školského internátu. Papierové záznamy vyžadované vyhláškou sú uložené v miestnosti vychovávateľov v uzamykateľnej skrini. Osobné údaje v elektronickej forme sú iba vo forme súborov MS Excel alebo MS Word, menných zoznamov, ktoré obsahujú osobné údaje – meno a priezvisko, triedu a bydlisko žiaka. Prístup do počítača je na základe mena a hesla. Prístup majú iba vychovávatelia. Po ukončení školy sú osobné údaje archivované v zmysle platného registratúrneho poriadku a plánu.

Informačný systém Ubytovanie - verejnosť

Informačný systém je vedený iba v papierovej forme v knihe návštev. Ubytovaný sa identifikuje na základe občianskeho preukazu alebo pasu u cudzinca. V knihe návštev koordinátor ubytovania eviduje meno a priezvisko, dátum narodenia, bydlisko a číslo občianskeho preukazu, u cudzincov číslo pasu a štátnu príslušnosť. Kniha návštev je uložená v miestnosti koordinátora ubytovania v uzamykateľnej skrini. Pokladničný doklad za úhradu odovzdáva osobne koordinátor ubytovania v pokladni školy.

Informačný systém Právne vzťahy

Informačný systém predstavuje osobné údaje v zmluvách prevádzkovateľa, ktoré sú uložené miestnosti riaditeľa školy, zástupcu alebo hospodárky. Systém je iba v papierovej forme. Po splnení účelu sú zmluvy archivované v zmysle platného registratúrneho poriadku a plánu.

Informačný systém Verejné obstarávanie

Postup je riadený smernicou „Verejné obstarávanie". Osobné údaje sú iba v papierovej podobe v rozsahu dokumentácie k jednotlivým prípadom verejného obstarávania uložené v trezore na sekretariáte školy.

Informačný systém Správa registratúry

Škola má registratúrne stredisko na prvom a druhom poschodí. Prevádzka je v zmysle vypracovaného registratúrneho plánu a poriadku. Prístup do registratúrneho strediska má hospodárka školy a zástupca riaditeľa. Prijatá pošta sa eviduje na sekretariáte školy v registratúrnom denníku.

Informačný systém Vrátnica

Informačný systém je vedený iba v papierovej forme. Pri jednorazovom vstupe je dotknutá osoba identifikovaná informátorkou, ktorá zapíše do knihy „Jednorazových vstupov fyzických osôb" dátum a čas, meno a priezvisko, číslo predloženého identifikačného dokladu a priezvisko zamestnanca prevádzkovateľa, za ktorým dotknutá osoba ide. Po zapísaní knihy je táto archivovaná podľa platného registratúrneho poriadku a plánu.

Informačný systém Oprávnené osoby

Informačný systém vedený v papierovej a elektronickej forme. V elektronickej forme je to zoznam oprávnených osôb a formuláre poučení. V papierovej forme sú to identické poučenia a zoznam ako v elektronickej forme, ale s podpisom poučených osôb. Dokumentácia je uložená u zodpovednej osoby školy.

Informačný systém Účtovníctvo

Osobné údaje v účtovnom systéme sú v papierovej podobe a v elektronickej podobe v informačnom systéme iSPIN v rámci intranetu VUCnet Prešovského samosprávneho kraja. Papierové záznamy sú uložené v regáloch v miestnosti hospodárky a účtovníčky. Po ročnej uzávierke sú záznamy archivované v zmysle platného registratúrneho poriadku a registratúrneho plánu. Prevádzkovateľ má vypracovanú smernicu „Vedenie účtovníctva", v rámci ktorej je riadený obeh účtovných dokladov. Jednotliví užívatelia majú prístup do informačného systému na základe mena a hesla.

Informačný systém Evidencia odbornej spôsobilosti elektrotechnikov

Osobné údaje v informačnom systéme sú získavané na základe žiadosti o overenie odbornej spôsobilosti. Žiadosť obsahuje osobné údaje: meno a priezvisko, bydlisko, dátum narodenia, telefónne číslo, e-mail a vzdelanie. Osobné údaje sú v papierovej a elektronickej forme. Uložené sú v kancelárii zástupcu riaditeľa školy a na PC na sekretariáte školy.

Informačný systém Sťažnosti

Postup pri riešení sťažností je podľa smernice o vybavovaní sťažností. Sťažnosti a súvisiaca dokumentácia v papierovej forme je uložená u zástupcu riaditeľa školy. V elektronickej forme ako jednotlivé súbory v počítači na sekretariáte riaditeľa školy.

Informačný systém WASET

Osobné údaje v informačnom systéme sú získavané na základe prihlášky uchádzača na ECDL testovanie. Prihláška obsahuje osobné údaje: meno a priezvisko, bydlisko, dátum narodenia, štátna príslušnosť, telefónne číslo, číslo občianskeho preukazu, e-mail, číslo indexu ECDL. Osobné údaje sú v papierovej forme uložené na sekretariáte školy a registratúrnom stredisku školy. Súčasťou papierovej dokumentácie sú aj výsledky testovania vo forme odpoveďových hárkov, vypracovaných zadaní a zoznamu uchádzačov s bodovým hodnotením. V elektronickej podobe sú všetky spomenuté osobné údaje prístupne po prihlásení sa do informačného systému prihlasovacím menom a heslom. Úplný prístup majú v rámci školy len manažér ECDL testovania, asistentka manažéra ECDL testovania a tri komisárky ECDL testovania. Uchádzač o ECDL testovanie získa prístup len k svojim údajom, a to jedine po požiadaní o prístup v prihláške na testovanie.

Informačný systém Kamerový systém

1. Účel kamerového systému

Kamerový systém pozostávajúci z 3 statických kamier plní nasledujúce účely:

- monitorovanie priestorov školy,
- ochranu a prevenciu proti vzniku škôd na majetku školy,
- ochranu pred vandalizmom cudzích osôb,

2. Osoby prichádzajúce do styku s kamerovým systémom

Do styku s kamerovým systémom školy prichádzajú títo pracovníci školy:

- Ing. Slavomír Kožár, MBA – riaditeľ školy
- Ing. Bohuš Popík, MBA – zástupca riaditeľa pre TEČ
- Ing. Martin Vujčík – správca školskej siete
- Jozef Anderko – školník, údržbár
- Ján Pasternák – kurič, údržbár
- Marta Hlavatá – informátorka, vrátnička
- Katarína Mihoková – informátorka, vrátnička

3. Opis kamerového systému

Kamerový systém školy tvoria 3 statické kamery. Obrazový záber kamier je uvedený v prílohe s nákresom budovy. Kamerový systém je prepojený s PC softvérom.

4. Technické údaje kamerového systému

- 3 ks kamery DH-IPC-HFW5421E-Z - rozlíšenie 4MPX, varifocal objektív, záznamník DH- NVR4208-8P-4K, 8 kanálov

3.2.2.4 Bezpečnostné incidenty

Prevádzkovateľ má poučených pracovníkoch, ktorí poznajú postup v prípade bezpečnostných incidentov a sú oboznámení so smernicou pre riadenie postupov v prípade vzniku bezpečnostných incidentov. Smernica pre riadenie bezpečnostných incidentov je v prílohe tohto projektu.

3.2.2.5 Kontrolná činnosť

Prevádzkovateľ má vypracovaný kontrolný plán na dodržiavanie prijatých bezpečnostných opatrení. Kontrolná činnosť je realizovaná v rámci interných auditov ISO9001. Za realizáciu vykonávania kontrolných činnosti je zodpovedná osoba v zmysle zákona č. 122/2013 Z. z.

3.2.3 Personálne opatrenia

3.2.3.1 Písomné poučenie oprávnených osôb

Prevádzkovateľ má preukázateľne poučené všetky oprávnené osoby. V prípade zmeny podmienok spracúvania osobných údajov je ich prevádzkovateľ povinný opätovne poučiť. Za poučenie oprávnených osôb je zodpovedný zamestnanec, ktorého vymenoval prevádzkovateľ za zodpovednú osobu v zmysle zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

3.2.3.2 Oboznámenie oprávnených osôb s bezpečnostnými smernicami

Oprávnené osoby sú oboznámené s bezpečnostným projektom, o čom je vyhotovený záznam. Za oboznámenie zodpovedá prevádzkovateľ.

3.2.3.3 Postup pri ukončení pracovného alebo obdobného pomeru oprávnenej osoby

Pri ukončení pracovného alebo obdobného pracovného pomeru sa oprávnenej osobe zrušia prístupové práva. Osoba odovzdá pridelené aktíva a je poučená o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti. V prípade vlastných pracovníkov sa riadi ustanoveniami zákonníka práce v aktuálnom znení, v prípade externých subjektov podľa vzájomných zmluvných dojednaní.

3.2.3.4 Poverenie zodpovednej osoby

Prevádzkovateľ je povinný písomne poveriť zodpovednú osobu, keď spracúva osobné údaje 20 a viac oprávnenými osobami. Poverenie musí obsahovať náležitosti podľa zákona č. 122/2013 Z. z. § 23 odst. 10. Prílohou poverenia musí byť záznam o poučení. Prevádzkovateľ je povinný o poverení zodpovednej osoby informovať Úrad na ochranu osobných údajov najneskôr do 30 dní. Oznámenie musí obsahovať náležitosti podľa § 25 odst. 2 zákona č. 122/2013 Z .z.

3.3 Vymedzenie okolia informačných systémov a jeho vzťah k možnému narušeniu bezpečnosti informačných systémov

Prevádzkovateľ spracúva osobné údaje v budovách Strednej priemyselnej školy elektrotechnickej na adresách Plzenská 1, Plzenská 4 a Masarykova 12 v Prešove. Okolie informačných systémov predstavuje aj intranetová sieť VUCnet Prešovského samosprávneho kraja, v rámci ktorej je realizované pripojenie do informačných systémov softvér iSPIN účtovného systému a softvér MAGMA mzdového a personálneho systému a sieť SANET, v ktorej je prevádzkovaná AsC agenda.

3.4 Vymedzenie hraníc určujúcich množinu zostatkových rizík

Na základe analýzy rizík prevádzkovateľ rozhodol o nasledujúcich pravidlách pre prijateľnú mieru rizika:

1. S aktívami, kde je výška rizika do 3 vrátane, nie je potrebné sa zaoberať.
2. Aktíva, kde je výška rizika nad 3 do 5 vrátane, vyžadujú pozornosť. Táto výška rizika je ešte pre spoločnosť akceptovateľná.
3. Prevádzkovateľ nebude akceptovať žiadnu hodnotu väčšiu ako 5. Pri hodnote väčšej ako 5 je potrebné prijať opatrenia tak, aby po ich aplikovaní sa výška rizika znížila na akceptovateľnú úroveň.

4. Analýza bezpečnosti informačných systémov

4.1 Identifikácia aktív a ich vlastníkov

Identifikácia aktív a ich vlastníkov je v dokumente Analýza_rizika.

4.2 Identifikácia zraniteľností zneužiteľných hrozbami a ich dopad na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti

Identifikácia zraniteľností zneužiteľných hrozbami a ich dopad na aktíva v dôsledku straty dôvernosti, integrity a dostupnosti je v dokumente Analýza_rizika.

4.3 Ohodnotenie rizík na základe dopadov, ktoré môžu vyplynúť zo zlyhania bezpečnosti

Prevádzkovateľ ohodnocuje výšku rizika ako súčin Hodnoty dopadu * Hodnota pravdepodobnosti. Hodnota dopadu je v rozmedzí od 1 – 3 a je to najväčšia hodnota z dostupnosti, integrity a dôvernosti aktíva.
Hodnoty dôvernosti, integrity a dostupnosti informácií sú definované tak, ako je uvedené nižšie.
Stanovenie hodnoty aktív sa realizuje, ako keby neboli zavedené žiadne opatrenia na zabezpečenie dôvernosti, integrity a dostupnosti aktív.

Dôvernosť
Dôvernosť je vlastnosť, na základe ktorej informácie nie sú sprístupňované a odhaľované neautorizovaným osobám, entitám alebo procesom.
Dôvernosť, čiže dostupnosť aktív sa ohodnocuje nasledovnou stupnicou:
1 - verejné informácie sú k dispozícii pre verejnosť
Príklady: informácie na webe
2 – interné informácie, ktoré nie sú prístupné verejnosti, ale sú prístupné všetkým zamestnancom
Príklady: bezpečnostné smernice, pracovné postupy
3 – dôverné informácie, ktoré nie sú prístupné verejnosti, ani všetkým zamestnancom spoločnosti, a sú prístupné iba vybraným skupinám zamestnancov
Príklady: účtovné informácie, osobné údaje.
Integrita

Integrita: vlastnosť zabezpečujúca presnosť a kompletnosť aktív.
Integrity aktív sa ohodnocuje nasledovnou stupnicou (Dopad narušenia integrity aktív na činnosť spoločnosti):
1 - minimálna požiadavka na integritu aktív; narušenie integrity aktív na podnikanie pri neúplnosti alebo nesprávnosti nemá žiaden významný dopad
2 - nízka požiadavka, narušenie integrity aktíva ovplyvní prácu oddelenia jej obnova je v možnostiach oddelenia
3 - vysoká požiadavka, narušenie integrity aktíva ovplyvní prácu celej spoločnosti, na jej obnovu je potreba špecialistov z oddelenia IT alebo externých.

Dostupnosť
Dostupnosť: schopnosť byť dostupný a použiteľný na požiadanie autorizovanej entity.
Požiadavka na dostupnosť sa ohodnocuje nasledovne:
1 - nízka dostupnosť, ak aktíva sú dostupné až na siedmy deň, tak to nemá vážny dopad na chod oddelenia, spoločnosti
2 - stredná dostupnosť, ak aktíva sú dostupné až na druhý deň, tak nemá dopad na chod oddelenia, spoločnosti
3 - vysoká dostupnosť, aktíva musia byť dostupné okamžite.

Určenie hodnoty pravdepodobnosti
Pravdepodobnosť, že identifikovaná hrozba využije zraniteľnosť a obmedzí dostupnosť, integritu a dôvernosť aktíva.

Hodnoty pravdepodobnosti sú nastavené nasledovne:

Hodnota	Vysvetlenie	Príklad
1	Nikdy nenastane	V posledných troch rokoch nikdy nenastala
2	Zriedkavo	Raz za rok
3	Občas	Raz za štvrťrok
4	Častejšie	Raz za štrnásť dní
5	Veľmi často	Raz za týždeň a častejšie

Výška rizika počítaná ako hodnota dopadu * hodnota pravdepodobnosti môže nadobúdať nasledovné hodnoty:

	Pravdepodobnosť	Výška rizika				
		1	2	3	4	5
Hodnota dopadu	1	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15

4.4 Výber cieľov a opatrení na ošetrenie rizík a vymedzenie súpisu nepokrytých rizík

Výber cieľov a opatrení na ošetrovanie rizík je uvedený v dokumente „Plán ošetrovania rizík".

5. Bezpečnostná smernica

5.1 Popis bezpečnostných opatrení a spôsob ich uplatňovania v podmienkach prevádzkovateľa.

Prevádzkovateľ má PC, na ktorých sú spracúvané osobné údaje zaradené do domény. Overenie užívateľov je pri vstupe do intranetovej siete menom a heslom. Sila hesla nie je stanovená. Doménové

meno a heslo sa preberá do e-mailu. Na PC sú inštalované rôzne operačné systémy. V dokumente „Vnútorný poriadok" sú určené pravidlá pre používanie siete. Administrátorský prístup do PC má iba IT administrátor. Pracovné stanice majú nastavenú automatickú aktualizáciu operačného systému. Ako ochranu proti škodlivému softvéru prevádzkovateľ má inštalovaný na všetkých PC antivírusový systém NOD32. Posledná osoba odchádzajúca z miestnosti, miestnosť vždy uzamyká. Na prvom poschodí, kde sú kancelárie riaditeľa školy, zástupcov riaditeľa školy, hospodárky, účtovníčky a mzdovej účtovníčky je elektronické zabezpečovacie zariadenie

1. Informačný systém Vzdelávanie – žiaci

Informačný systém Vzdelávanie – žiaci je prevádzkovaný na štyroch počítačoch, ktoré sú pripojené do verejnej počítačovej siete. Počítače sú v miestnosti s uzamykateľnými dverami. Prístup je na základe mena a hesla. Prístupy zriaďuje administrátor IT na základe rozhodnutia riaditeľa školy. Prístup do všetkých modulov softvéru AsC majú: technicko-administratívna asistentka, administratívna asistentka, mzdová účtovníčka, zástupkyňa riaditeľa pre odborné predmety a správca siete. Do elektronickej žiackej knižky majú prístup všetci učitelia podľa ročníkov a predmetov. Žiaci majú prístup iba do svojej žiackej knižky.

2. Informačný systém Personalistika a mzdy

Informačný systém je prevádzkovaný v miestnosti mzdovej účtovníčky. Vstup do miestnosti je cez uzamykateľné dvere. Softvér MAGMA, v ktorom sú spracúvané osobné údaje je prevádzkovaný v siete VUCnet Prešovského samosprávneho kraja. Prístup do počítača je na základe mena a hesla. Osobné údaje pedagogických a nepedagogických pracovníkov sú uložené u mzdovej účtovníčky.

3. Informačný systém Knižnica

Prístup do miestnosti, kde je prevádzkovaný knižničný informačný systém je so vstupom cez uzamykateľné dvere a miestnosť je zabezpečená elektronickým zabezpečovacím systémom. Prístup do počítača je chránený heslom. Spôsob získavania, spracúvania a likvidácie osobných údajov v informačnom systéme Knižnica je opísaný v časti 3.2.2.3.

4. Informačný systém Ubytovanie – žiaci

Informačný systém je prevádzkovaný v papierovej aj elektronickej podobe. V elektronickej forme je vo forme lokálnych súborov na PC vychovávateľa. PC je umiestnený v miestnosti vychovávateľa, vstup do PC je chránený heslom. Vstup do miestnosti je cez uzamykateľné dvere. Papierová dokumentácia s osobnými údajmi je uložená v uzamykateľnej skrini. Posledný odchádzajúci z miestnosti vždy miestnosť uzamyká.

5. Informačný systém Ubytovanie - verejnosť

Informačný systém je iba v papierovej forme. Kniha návštev je uložená v miestnosti koordinátora ubytovania v uzamykateľnej zásuvke. Prístup ku knihe má iba koordinátor ubytovania. Prístup do miestnosti je cez uzamykateľné dvere.

6. Informačný systém Právne vzťahy

Záznamy obsahujúce osobné údaje predstavujú zmluvy s dodávateľmi, ktoré sú uložené v kancelárii riaditeľa, zástupcu riaditeľa, hospodárky školy a účtovníčky. Prístup do miestnosti je cez uzamykateľné dvere.

7. Informačný systém Verejné obstarávanie

Záznamy s osobnými údajmi sú uložené v elektronickej podobe na PC na sekretariáte školy. PC sú zaradené do domény s prístupom chráneným heslom. Papierové záznamy sú uložené u zástupcu riaditeľa školy.

8. Informačný systém Správa registratúry

Registratúrne stredisko je umiestnené na prvom a druhom poschodí školskej budovy. Na prvom poschodí je umiestnené v trakte budovy s elektronickým zabezpečovacím systémom. Vstup do

miestností registratúrneho strediska je cez uzamykateľné dvere. Kľúče od miestností majú hospodárka školy a zástupca riaditeľa. Evidencia došlej pošty je na sekretariáte školy. Evidencia je iba v papierovej forme. Organizácia registratúrneho strediska je riadená Registratúrnym poriadkom a plánom.

9. Informačný systém Vrátnica

Informačný systém je iba v papierovej forme. Kniha „Jednorazových vstupov fyzických osôb do priestorov školy" je umiestnená na vrátnici školy. Prístup ku knihe majú iba vrátnici, zastupujúci zamestnanci, riaditeľ a zástupcovia školy. Po zapísaní je kniha uložená do registratúrneho strediska.

10. Informačný systém Oprávnené osoby

Informačný systém v papierovej forme predstavuje záznamy o poučení oprávnených osôb. Záznamy sú uložené u zástupcu riaditeľa školy v zásuvke. Elektronická forma predstavuje samostatné súbory uložené na PC na sekretariáte školy.

11. Informačný systém Účtovníctvo

Informačný systém je prevádzkovaný v miestnosti účtovníčky a hospodárky školy. Informačný systém je v papierovej forme aj v elektronickej forme. Miestnosti sú v trakte zabezpečenom elektronickým zabezpečovacím zariadením. Vstup do miestností je cez uzamykateľné dvere. Oprávnené osoby sa prihlasujú do PC menom a heslom, na vstup do aplikácie iSPIN je potrebné meno a heslo. Pri odchode z miestnosti posledná osoba miestnosť uzamyká. Papierové záznamy sú uložené voľne v policiach. Postup spracovanie je opísaný v časti 3.2.2.3.

12. Informačný systém Evidencia odbornej spôsobilosti elektrotechnikov

V elektronickej forme je v lokálnych súboroch na PC na sekretariáte školy. PC sú v doméne a vstup je chránený heslom. V papierovej forme sú uložené záznamy u zástupcu riaditeľa školy.

13. Informačný systém Sťažnosti

Informačný systém sťažnosti je vedený v papierovej elektronickej forme. V papierovej forme je uložený u zástupcu riaditeľa školy uložený v zásuvke. V elektronickej forme je vedený na PC na sekretariáte školy.

14. Informačný systém WASET

Informačný systém je prístupný z akéhokoľvek PC, ktorý má prístup na internet. V papierovej forme je uložený na sekretariáte školy a v registratúrnom stredisku školy.

15. Informačný systém Kamerový systém

Informačný systém je prevádzkovaný z PC na vrátnici školy. Prístup k PC majú iba riaditeľ školy, určený zástupca riaditeľa školy, správca školskej siete, vrátnici a informátorky.

5.2 Rozsah oprávnení oprávnených osôb

Riaditeľ školy – prístup do informačného systému Právne vzťahy, Projekty, Overenie odbornej spôsobilosti elektrotechnikov, Verejné obstarávanie, Sťažnosti, Vrátnica, Personalistika a mzdy, WASET, Kamerový systém

Zástupcovia riaditeľa školy – prístup do informačného systému Vzdelávanie – žiaci, Sťažnosti, Vrátnica, Verejné obstarávanie, Personalistika a mzdy, Kamerový systém

Technicko-administratívna asistentka – prístup do AsC agendy – všetky prístupové práva, prístup do informačného systému Vzdelávanie – žiaci, Projekty, Overenie odbornej spôsobilosti elektrotechnikov, Verejné obstarávanie, Sťažnosti, správa registratúry, WASET

Administratívna asistentka – prístup do informačného systému Vzdelávanie – žiaci, Projekty, Overenie odbornej spôsobilosti elektrotechnikov, Verejné obstarávanie, Sťažnosti, Správa registratúry

Pedagogickí zamestnanci školy – prístup do AsC agendy modul Elektronická žiacka knižka

Zamestnanci na vrátnici – prístup do informačného systému Vrátnica, Kamerový systém

Mzdová účtovníčka – prístup do informačného systému Mzdy a personalistika, prístup do AsC agendy – všetky prístupové práva, TANGRAM dochádzkový systém, Projekty

Účtovníčka – prístup do informačného systému Účtovníctvo, Ubytovanie – žiaci, Ubytovanie verejnosť, Projekty

Hospodárka – prístup do informačného systému Účtovníctvo, Verejné obstarávanie, Správa registratúry, Projekty

Vychovávatelia – prístup do informačného systému Ubytovanie žiaci

Koordinátor ubytovania – prístup do informačného systému Ubytovanie verejnosť

Komisárky ECDL testovania – prístup do informačného systému WASET

Asistentka centra záujmového vzdelávania – prístup do informačného systému Knižnica

Správca školskej siete – prístup do informačného systému Kamerový systém

5.3 Popis povolených činností oprávnených osôb

Riaditeľ školy – informačné systémy Právne vzťahy, Projekty, Overenie odbornej spôsobilosti elektrotechnikov, Verejné obstarávanie, Sťažnosti – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie
Informačný systém Vrátnica – vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie
Personalistika a mzdy – usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie
WASET – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie
Kamerový systém – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

Zástupcovia riaditeľa školy – informačné systémy Vzdelávanie – žiaci, Sťažnosti, Verejné obstarávanie – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie
Informačné systémy Vrátnica, Personalistika a mzdy - usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie
Kamerový systém – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

Technicko-administratívna asistentka – informačné systémy Vzdelávanie – žiaci, Sťažnosti, Verejné obstarávanie, Správa registratúry. WASET – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

Administratívna asistentka – informačné systémy Vzdelávanie – žiaci, Sťažnosti, Verejné obstarávanie, Správa registratúry – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

Pedagogickí zamestnanci školy – informačný systém Vzdelávanie – žiaci, AsC agenda modul Elektronická žiacka knižka – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie

Zamestnanci na vrátnici – informačný systém Vrátnica – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie
Kamerový systém – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

Mzdová účtovníčka – informačný systém Mzdy a personalistika – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

Účtovníčka – informačný systém Účtovníctvo, Ubytovanie žiaci, Ubytovanie verejnosť – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

Hospodárka – informačný systém Účtovníctvo, Verejné obstarávanie, Správa registratúry – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

Vychovávatelia – informačný systém Ubytovanie žiaci – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

Koordinátor ubytovania – Ubytovanie verejnosť – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

Komisárky ECDL testovania – informačný systém WASET – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

Asistentka centra záujmového vzdelávania – informačný systém Knižnica – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

Správca školskej siete – informačný systém Kamerový systém – zhromažďovanie, usporadúvanie, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, využívanie, uchovávanie

5.4 Spôsob identifikácie a autentizácie oprávnených osôb

Spôsob identifikácie oprávnených osôb je na základe prideleného mena a hesla do domény. Do aplikácie informačného systému Účtovníctvo softvér iSPIN, Mzdy a Personalistika softvér MAGMA sa užívatelia prihlasujú svojím menom a heslom.

5.5 Rozsah zodpovedností oprávnených osôb

Rozsah zodpovedností oprávnených osôb je definovaný vo vzťahu k spracúvaniu osobných údajov. Príslušné zodpovednosti vo vzťahu k príslušnému pracovnému miestu sú určené v pracovnej zmluve a Organizačnom poriadku.

Riaditeľ školy – zodpovednosť za dodržiavanie bezpečnostných opatrení na ochranu osobných údajov v celej škole

Zástupcovia riaditeľa školy – zodpovednosť za dodržiavanie bezpečnostných opatrení v rámci riadených činností v organizácii. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

Technicko-administratívna asistentka – zodpovednosť za dodržiavanie bezpečnostných opatrení na ochranu osobných údajov podľa zaradenia. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

Administratívna asistentka – zodpovednosť za dodržiavanie bezpečnostných opatrení na ochranu osobných údajov podľa zaradenia. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

Pedagogickí zamestnanci školy – zodpovednosť za dodržiavanie bezpečnostných opatrení na ochranu osobných údajov podľa zaradenia. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

Zamestnanci na vrátnici – zodpovednosť za dodržiavanie bezpečnostných opatrení v informačných systémoch Vrátnica, Kamerový systém. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

Mzdová účtovníčka – zodpovednosť za dodržiavanie bezpečnostných opatrení v informačnom systéme Personalistika a mzdy. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

Účtovníčka – zodpovednosť za dodržiavanie bezpečnostných opatrení v informačnom systéme Účtovné doklady. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

Hospodárka – zodpovednosť za dodržiavanie bezpečnostných opatrení v informačnom systéme Verejné obstarávanie, Účtovníctvo, Právne vzťahy v rozsahu oprávnení v jednotlivých informačných systémoch. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

Vychovávatelia – zodpovednosť za dodržiavanie bezpečnostných opatrení v informačnom systéme Ubytovanie – žiaci. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

Koordinátor ubytovania – zodpovednosť za dodržiavanie bezpečnostných opatrení v informačnom systéme Ubytovanie verejnosť. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

Komisárky ECDL testovania – zodpovednosť za dodržiavanie bezpečnostných opatrení v informačnom systéme WASET. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

Asistentka centra záujmového vzdelávania – zodpovednosť za dodržiavanie bezpečnostných opatrení v Knižničnom informačnom systéme. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

Správca školskej siete – zodpovednosť za dodržiavanie bezpečnostných opatrení v Kamerovom systéme. Zodpovednosť za porušenie práv a povinností je špecifikovaná v Zázname o poučení zodpovednej osoby.

5.6 Záznamy o prístupoch (logy)

5.6.1 O prístup k systémom kde sa uchovávajú osobné údaje sú zaznamenávané logy (záznamy o udalostiach), ktoré zachytávajú získavanie, zmena, prehliadanie, poskytovanie vrátane

prenosov, kombinovanie a vymazanie. Log záznamy taktiež obsahujú dôvody, dátum a čas takýchto operácií, a pokiaľ možno aj identifikačné údaje osoby, ktorá k údajom pristupovala. (Zdroj: nariadenie 679 Kap II, Cl. 25 ods 1)

5.6.2 Logy o prístupoch sa využijú výlučne na overovanie zákonnosti spracúvania, vlastné monitorovanie, na zabezpečenie integrity a bezpečnosti osobných údajov a na účely trestného konania. (Zdroj: nariadenie 679 Kap II, Cl. 25 ods 2.)

6. Dotknuté osoby

6.1 Dotknuté osoby majú právu na informácie o spracovávaných osobných údajoch o jej osobe:

a) účely a právny základ spracúvania;
b) kategórie dotknutých osobných údajov;
c) príjemcovia alebo kategórie príjemcov, ktorým boli osobné údaje sprístupnené, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie;
d) ak je to možné, predpokladaná doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;
e) existencia práva požadovať od prevádzkovateľa opravu alebo vymazanie osobných údajov alebo obmedzenie spracúvania osobných údajov týkajúceho sa dotknutej osoby;
f) právo podať sťažnosť dozornému orgánu a kontaktné údaje dozorného orgánu;
g) oznámenie osobných údajov, ktoré sa spracúvajú, a akýchkoľvek dostupných informácií, pokiaľ ide o ich pôvod.
(Zdroj: nariadenie 679 Kap II, Cl. 1.)

6.2 Akékoľvek zamietnutie alebo obmedzenie prístupu k informáciám bude dotknutej osobe oznámené písomne a bude zahŕňať skutkové alebo právne dôvody, na ktorých je rozhodnutie založené. (Zdroj: nariadenie 680, ods 45)

6.3 V prípade zistenia porušená ochrany osobných údajov je potrebné bezodkladne informovať dotknuté osoby, ktorých sa porušenie ochrany osobných údajov priamo dotýka. Informovanie sa realizuje za účelom umožnenia prijať preventívne opatrenia. (Zdroj : nariadenie 680, ods 62)

7. Dozorný orgán

7.1 Na vyžiadanie dozorného orgánu poskytne SPŠE súčinnosť pri výkone úloh dozorného orgánu. (Zdroj: nariadenie 679 Kap II, Cl. 26)

7.2 Pred zavedením nových technológií alebo procesov sa posúdi vplyv a riziká voči osobným údajom, ktoré SPŠE spracováva a bude spracovávať v budúcnosti. Posúdenie sa realizuje minimálne všeobecným popisom:
a) plánovaných operácií,
b) hodnotením rizík,
c) opatrení a mechanizmov pre riešenie rizík.
(Zdroj: nariadenie 679 Kap II, Cl. 27.)

7.3 V prípade, že zavedenie nového informačného systému by predstavovalo vysoké riziko pre spracovanie osobných údajov, SPŠE bude ešte pred zavedením technológie alebo procesu do prevádzky,

konzultovať navrhovaný proces alebo technológie s dozorným orgánom. (Zdroj: nariadenie 679 Kap II, Cl. 28)

8. Mimoriadne situácie

8.1 Postupy pri haváriách, poruchách a iných mimoriadnych situáciách

Postup pri haváriách, poruchách a iných mimoriadnych situáciách je uvedený v smernici pre „SM_02 Smernica pre riadenie postupu pri haváriách, poruchách a iných mimoriadnych situáciách – ochrana osobných údajov".

8.2 Preventívne opatrenia na zníženie rizika vzniku mimoriadnych situácií

Postup podávania a riadenia nápravných a preventívnych opatrení je riadený v zmysle dokumentovaného postupu pre nápravné a preventívne opatrenia SMK prevádzkovateľa podľa ISO 9001.

8.3 Záznamy o bezpečnostných incidentoch

Postup pri vzniku, nahlasovaní a riadení v prípade vzniku bezpečnostných incidentov je uvedený v smernici „SM_03 Smernica pre riadenie incidentov informačnej bezpečnosti – ochrana osobných údajov".

8.4 Pri vzniku mimoriadnej udalosti, pri ktorej dôjde k porušeniu ochrany osobných údajov bude táto situácia bez zbytočného odkladu oznámená dozornému orgánu, najneskôr však do 72 hodín po zistení o vzniku takejto udalosti. (Zdroj: nariadenie 679 Kap II, Cl. 30. ods 1.)

8.4.1 Oznámenie musí obsahovať nasledujúce údaje:

a) opis povahy porušenia ochrany osobných údajov vrátane, podľa možnosti, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch;
b) meno/názov a kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií;
c) opis pravdepodobných následkov porušenia ochrany osobných údajov;
d) opis opatrení prijatých alebo navrhovaných prevádzkovateľom s cieľom napraviť porušenie ochrany osobných údajov vrátane, podľa potreby, opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov. (Zdroj: nariadenie 679 Kap II, Cl. 30. ods 2., nariadenie 679 Kap II, Cl. 30. ods 3. V prípade nedostatku informácií v danej dobe, je možné oznámenie zaslať vo viacerých fázach bez zbytočného odkladu.)

9. Zodpovedná osoba

9.1 Určenie zodpovednej osoby sa vykonáva na základe odborných a osobnostných predpokladov a kvalít a to najmä znalostí z oblasti práva a postupov v oblasti ochrany osobných údajov a spôsobilosti plní úlohy ako:

a) poskytovanie informácií a poradenstva prevádzkovateľovi a zamestnancom, ktorí vykonávajú spracúvanie, o ich povinnostiach podľa tejto smernice a ostatných právnych predpisov Únie alebo členského štátu týkajúcich sa ochrany údajov;
b) monitorovanie súladu s touto smernicou, s ostatnými právnymi predpismi Únie alebo členského štátu týkajúcimi sa ochrany údajov a s pravidlami prevádzkovateľa v súvislosti s ochranou

osobných údajov vrátane rozdelenia povinností, zvyšovania povedomia a odbornej prípravy personálu, ktorý je zapojený do spracovateľských operácií, a súvisiacich auditov;

c) poskytovanie poradenstva na požiadanie, pokiaľ ide o posúdenie vplyvu na ochranu údajov a monitorovanie jeho vykonávania;
d) spolupráca s dozorným orgánom;
e) plnenie úlohy kontaktného miesta pre dozorný orgán v súvislosti s otázkami týkajúcimi sa spracúvania vrátane predchádzajúcej konzultácie a podľa potreby aj konzultácie v akýchkoľvek iných veciach.
(Zdroj nariadenie 679 Kap II, Cl. 32)

9.2 SPŠE poskytne zodpovednej osobe maximálnu podporu a súčinnosť pri vykonávaní jej úloh a povinností**.**

9.3 Kontaktné zodpovednej osoby údaje budú oznámené dozornému orgánu.

10. Interné kontroly

10.1 Realizácia kontrolných činností zameraných na dodržiavanie bezpečnostných opatrení

Kontrolné činnosti zamerané na dodržiavanie bezpečnostných opatrení sa realizujú v rámci interných auditov podľa príslušného dokumentovaného postupu SMK. Kontrolu dodržiavania bezpečnostných opatrení na ochranu osobných údajov vykonáva poverená zodpovedná osoba v zmysle zákona č. 122/2013 Zb. z. Záznamy o vykonaných kontrolách sa riadia dokumentovanými postupmi pre riadenie záznamov a riadenie interných auditov SMK.

Zoznam príloh:
Príloha č. 1 Informačný systém Kamerový systém – obrazový záber kamier

Príloha č. 1 k S-49-3 Bezpečnostný projekt na ochranu osobných údajov

Informačný systém Kamerový systém – obrazový záber kamier

