Vnútorný predpis č. 15/2026

Smernica o kybernetickej bezpečnosti a riadení IT Vysokej školy zdravotníctva a sociálnej práce sv. Alžbety, n. o.

a

Vysokej školy zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

Obsah

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

1.Zoznam revízií

Číslo revízie	Typ revízie	Dátum
01	Uvoľnenie dokumentu	28.08.2026.

2.Cieľ

Cieľom tejto smernice je upraviť zabezpečenie bezpečnosti správy a prevádzky informačného systému Vysokej školy zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o. (ďalej len „VŠZaSP sv. Alžbety" alebo „vysoká škola" alebo „škola").

Informačný systém je kľúčovým nástrojom pre efektívne fungovanie každej inštitúcie vrátane VŠZaSP sv. Alžbety. Tento systém zahŕňa hardvér, softvér, dáta, elektronickú komunikáciu a pod. Efektívne a zodpovedné používanie informačného systému prispieva k úspešnému fungovaniu vysokej školy a zvyšuje kvalitu, bezpečnosť a efektivitu práce jej zamestnancov, študentov a ďalších oprávnených používateľov.

Neoddeliteľnou súčasťou jeho správnej prevádzky sú osoby zabezpečujúce správu informačných technológií, vrátane externých dodávateľov a poverených osôb, ako aj používatelia, ktorí informačný systém využívajú pri plnení svojich pracovných alebo študijných povinností.

Cieľom tejto smernice je stanoviť rámec pre bezpečnú a spoľahlivú prevádzku informačného systému školy. Smernica je navrhnutá tak, aby jej dodržiavanie zamestnancami, študentmi, externými používateľmi, dodávateľmi a ďalšími oprávnenými osobami chránilo pred neoprávneným prístupom do dátovej siete a informačných systémov vysokej školy a chránilo dôvernosť, integritu a dostupnosť informačných systémov a údajov vysokej školy.

Táto smernica určuje postupy na ochranu pred počítačovými vírusmi, škodlivým softvérom, neoprávneným prístupom a na prevenciu možnej straty, zmeny alebo zneužitia dát, vrátane ochrany osobných údajov zamestnancov, študentov a ďalších dotknutých osôb.

Táto smernica zároveň definuje pravidlá používania informačného systému, internetu, interných informačných služieb, elektronickej pošty a ďalších informačných technológií zo strany používateľov vysokej školy.

Vzhľadom na to, že IT prostriedky vrátane dát a aplikácií používaných pri činnosti vysokej školy predstavujú aktíva VŠZaSP sv. Alžbety, je táto smernica zameraná na ochranu vysokej školy pred ich možným zneužitím, poškodením alebo odcudzením zo strany používateľov, ako aj pred neoprávneným

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

prístupom, útokmi a inými vonkajšími hrozbami.

VŠZaSP sv. Alžbety ako prevádzkovateľ spracúvania osobných údajov má povinnosť dodržiavať predpisy vyplývajúce z článku 32 Nariadenia Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane osobných údajov a zo zákona č. 18/2018 Z. z. o ochrane osobných údajov. V rámci týchto povinností musí vysoká škola implementovať potrebné technické a organizačno-právne opatrenia na zaistenie bezpečnosti a ochrany prístupu v rámci svojej technickej infraštruktúry.

Tieto opatrenia zahŕňajú najmä používanie aktuálnych verzií operačných systémov, databázových a sieťových programov, antivírusovej ochrany a bezpečnostných prvkov na ochranu informačných systémov, dátovej siete a zariadení používaných pri činnosti vysokej školy, a to v rozsahu primeranom technickému a organizačnému zabezpečeniu vysokej školy.

3. Rozsah

Vysoká škola zdravotníctva a sociálnej práce Sv. Alžbety, n.o., so sídlom Palackého 36/1, 811 02 Bratislava-Staré Mesto, právnou formou nezisková organizácia poskytujúca všeobecne prospešné služby, založená na účely poskytovania všeobecne prospešných služieb v oblasti vzdelávania, výchovy a rozvoja telesnej kultúry formou prevádzkovania vysokej školy, je oprávnená pôsobiť ako súkromná vysoká škola pod názvom: Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o., na základe udelenia štátneho súhlasu vládou Slovenskej republiky na pôsobenie súkromnej vysokej školy uznesením vlády Slovenskej republiky č. 891 z 24. septembra 2003, s účinnosťou od 24. septembra 2003, v súlade s príslušnými právnymi predpismi.

Právne úkony v mene zamestnávateľa s vysokoškolskými učiteľmi a výskumnými pracovníkmi vysokej školy vykonáva rektor, ak zákon alebo vnútorný predpis vysokej školy neustanovuje inak.

Právne úkony v mene zamestnávateľa s ostatnými zamestnancami vykonáva riaditeľ, ak zákon alebo vnútorný predpis zamestnávateľa neustanovuje inak.

Procesy, pravidlá a povinnosti popísané v tejto smernici platia pre:

- všetkých zamestnancov VŠZaSP sv. Alžbety,
- všetkých študentov VŠZaSP sv. Alžbety,
- všetkých používateľov, ktorým bol pridelený prístup do informačného systému, dátovej siete, elektronickej pošty, internetu, interných informačných služieb, aplikácií alebo iných prostriedkov informačných technológií VŠZaSP sv. Alžbety,
- externých zamestnancov, spolupracujúce osoby, lektorov, vyučujúcich, školiteľov, konzultantov a iné osoby, ktoré majú s VŠZaSP sv. Alžbety pracovnoprávny, obdobný alebo iný zmluvný vzťah,
- uchádzačov o štúdium, absolventov, osoby na odbornej praxi, osoby pôsobiace v projektoch vysokej školy, dobrovoľníkov a ďalšie osoby, ktorým bol udelený prístup k informačným systémom, aplikáciám, dátam alebo službám VŠZaSP sv. Alžbety,
- tretie strany, dodávatelia vrátane externých IT dodávateľov zabezpečujúcich správu alebo podporu IT prostredia školy a servisné organizácie v rozsahu, v akom sa podieľajú na správe, prevádzke, údržbe, podpore alebo zabezpečení informačných systémov a služieb VŠZaSP sv. Alžbety.

- organizačné súčasti, detašované, zahraničné, partnerské alebo iné pracoviská VŠZaSP sv. Alžbety v rozsahu, v akom používajú informačné systémy, dátové siete, technické prostriedky, aplikácie, elektronickú poštu, dáta alebo služby vysokej školy,
- osoby, ktoré používajú technické prostriedky, programové vybavenie, dátové siete, aplikácie, elektronickú poštu, internetové služby, interné informačné služby alebo iné IT služby školy na základe oprávnenia udeleného vysokou školou.

Táto smernica sa vzťahuje na správu, prevádzku a používanie informačného systému VŠZaSP sv. Alžbety, najmä na hardvér, softvér, dáta, elektronickú komunikáciu, dátovú sieť, internet, interné informačné služby, elektronickú poštu, Wi-Fi, VPN, vzdialený prístup, používateľské kontá, prístupové práva, heslá, zálohovanie, auditné záznamy, bezpečnostné incidenty, ochranu osobných údajov a ďalšie prostriedky informačných technológií používané pri činnosti vysokej školy.

Táto smernica sa vzťahuje na informačné systémy, technické prostriedky, programové vybavenie, dáta a služby používané pri činnosti vysokej školy bez ohľadu na to, či sú prevádzkované priamo školou, prostredníctvom jej organizačných súčastí, alebo prostredníctvom zmluvných dodávateľov.

Táto smernica sa vzťahuje aj na používanie vlastných zariadení používateľov, ak sú na základe povolenia alebo oprávnenia používané na prístup k informačným systémom, dátovej sieti, elektronickej pošte, aplikáciám alebo dátam VŠZaSP sv. Alžbety.

Ustanovenia tejto smernice sa uplatňujú v rozsahu primeranom postaveniu, oprávneniam a činnostiam jednotlivých používateľov, zamestnancov, študentov a tretích strán.

Akademický informačný systém (AIS) je na účely tejto smernice informačným systémom VŠZaSP sv. Alžbety a ustanovenia tejto smernice sa naň uplatňujú v primeranom rozsahu. Vybrané bezpečnostné a prevádzkové opatrenia vzťahujúce sa na AIS sú bližšie špecifikované v prílohe č. 9.1 „Bezpečnostné a prevádzkové opatrenia akademického informačného systému" tejto smernice.

4. Zodpovednosť

Za prijatie tejto smernice zodpovedá vedenie VŠZaSP sv. Alžbety, resp. štatutárny orgán vysokej školy v súlade s internými pravidlami schvaľovania vnútorných predpisov.

Za vecnú správnosť, kontrolu, priebežné vyhodnocovanie a aktualizáciu tejto smernice zodpovedá osoba poverená štatutárnym orgánom vysokej školy na zabezpečenie oblasti informačnej a kybernetickej bezpečnosti.

Za zabezpečenie bezpečnosti správy, prevádzky a používania informačného systému VŠZaSP sv. Alžbety zodpovedajú v rozsahu svojich právomocí najmä:

- štatutárny orgán vysokej školy
- poverená osoba pre oblasť informačnej a kybernetickej bezpečnosti – manažér kybernetickej bezpečnosti (MKB), ak je určený,
- vedúci zamestnanci na všetkých stupňoch riadenia,
- útvar, interné osoby alebo externí dodávatelia zabezpečujúci správu informačných technológií,
- správcovia informačných systémov, aplikácií, databáz, dátovej siete a technických prostriedkov, bez ohľadu na to, či ide o interné osoby alebo externých dodávateľov,

- zamestnanci, študenti a ostatní oprávnení používatelia informačných systémov vysokej školy,
- tretie strany, dodávatelia a servisné organizácie v rozsahu ich zmluvných povinností a pridelených oprávnení.

Vedúci zamestnanci na všetkých stupňoch riadenia zodpovedajú za zabezpečenie plnenia povinností podľa tejto smernice v rozsahu svojej pôsobnosti.

Útvar, interné osoby alebo externí dodávatelia zabezpečujúci správu informačných technológií vysokej školy zodpovedajú v rozsahu svojich poverení a zmluvných povinností za technické a organizačné zabezpečenie správy a prevádzky informačného systému, dátovej siete, používateľských účtov, prístupových práv, technických prostriedkov, programového vybavenia, bezpečnostných opatrení, zálohovania, riešenia bezpečnostných incidentov a poskytovania odbornej podpory používateľom.

Správcovia informačných systémov, aplikácií, databáz, dátovej siete a technických prostriedkov zodpovedajú v rozsahu svojho poverenia alebo zmluvného záväzku za bezpečnosť prevádzky nimi spravovaných systémov a zariadení, nastavovanie a kontrolu prístupových práv, riešenie bezpečnostných incidentov, vedenie potrebnej dokumentácie a bezodkladné upozorňovanie na zistené nedostatky alebo riziká.

Používatelia informačných systémov VŠZaSP sv. Alžbety zodpovedajú za dodržiavanie tejto smernice, ochranu pridelených prístupových údajov a používanie informačných systémov iba v rozsahu pridelených práv.

Tretie strany, dodávatelia a servisné organizácie zodpovedajú za dodržiavanie tejto smernice v rozsahu ich zmluvných povinností a pridelených oprávnení.

Podrobné vymedzenie práv, povinností a zodpovedností jednotlivých osôb, útvarov, externých dodávateľov a rolí v oblasti správy, prevádzky a používania informačného systému je uvedené v príslušných ustanoveniach tejto smernice, najmä v častiach upravujúcich vymedzenie činností zamestnancov a študentov, pravidlá správy a prevádzky dátovej siete, pravidlá používania prostriedkov IT, autentifikáciu používateľov, auditné záznamy, zálohovanie, bezpečnostné incidenty a kontrola.

Prijatie tejto smernice vyjadruje záväzok vedenia VŠZaSP sv. Alžbety zabezpečovať primeranú úroveň informačnej a kybernetickej bezpečnosti a napĺňať pravidlá a povinnosti ustanovené touto smernicou.

5. Použitá literatúra

[1] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
[2] Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
[3] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES, všeobecné nariadenie o ochrane údajov (ďalej len „GDPR")
[4] Autorský zákon č. 185/2015 Z. z. v znení neskorších predpisov.

6. Definície a skratky

Aktívum – akýkoľvek prvok informačného systému, ktorý má hodnotu pre organizáciu a je nevyhnutný na zabezpečenie služieb, procesov a funkcií organizácie, najmä hardvér, softvér, dáta, know-how, dokumentácia, informačné systémy, sieťová infraštruktúra a ľudské zdroje.

Auditný záznam - záznam o činnosti používateľa, administrátora, systému alebo aplikácie, ktorý slúži na spätné overenie vykonaných úkonov, kontrolu oprávnenosti prístupu, riešenie bezpečnostných incidentov a ochranu informačného systému.

Autentifikácia (identifikácia) – bezpečnostný mechanizmus na overenie identity používateľa, ktorý chce získať prístup k chráneným aktívam.

Autorizácia (overenie oprávnenia) – bezpečnostný mechanizmus na určenie úrovne prístupu alebo oprávnení udelených autentifikovanému používateľovi na základe jeho identity, funkcie alebo privilégií na interakciu s konkrétnymi aktívami**.**

Bezpečnostná brána (Firewall) – bezpečnostné zariadenie alebo softvérový nástroj, ktorý slúži na kontrolu a filtrovanie sieťovej komunikácie medzi rôznymi časťami informačného systému alebo medzi vnútornou sieťou a externými sieťami, ako je Internet. Firewall umožňuje alebo blokuje prenos dát na základe vopred definovaných bezpečnostných pravidiel, čím chráni systém pred neoprávneným prístupom, kybernetickými útokmi a ďalšími bezpečnostnými hrozbami.

Bezpečnostná hrozba – potenciálna udalosť, činnosť, entita alebo okolnosť, ktorá môže využiť bezpečnostnú slabinu v informačnom systéme a spôsobiť narušenie dôvernosti, integrity alebo dostupnosti údajov a služieb. Bezpečnostné hrozby môžu byť úmyselné (napr. kybernetické útoky, malware, phishing) alebo neúmyselné (napr. ľudské chyby, zlyhanie hardvéru, prírodné katastrofy).

Bezpečnostné opatrenie – akcia, mechanizmus, proces, technológia alebo postup implementovaný s cieľom chrániť informačné systémy, údaje a služby pred bezpečnostnými hrozbami a zraniteľnosťami. Príklady bezpečnostných opatrení zahŕňajú šifrovanie dát, firewally, antivírusový softvér, autentifikačné systémy, bezpečnostné školenia pre zamestnancov, pravidelné zálohovanie dát, pravidelné aktualizácie softvéru a fyzickú ochranu zariadení.

Bezpečnostné riziko – pravdepodobnosť a potenciálny dopad hrozby, ktorá môže narušiť bezpečnosť informačného systému. Riziko sa vyjadruje ako miera možnej škody spôsobenej hrozbou využívajúcou slabinu v systéme, pričom závisí od pravdepodobnosti zneužitia zraniteľnosti a závažnosti vzniknutej škody (dôsledku).

Bezpečnostný incident – udalosť alebo séria udalostí, ktoré vedú k porušeniu bezpečnostných politík, štandardov alebo postupov, pričom majú negatívny vplyv na dôvernosť, integritu alebo dostupnosť informačných systémov, údajov alebo služieb. Bezpečnostný incident môže zahŕňať neoprávnený prístup k systémom, narušenie dát, útoky typu malware, phishing, výpadky služieb, krádež údajov alebo akékoľvek iné aktivity, ktoré ohrozujú bezpečnosť organizácie.

Dátová sieť – súbor technických a programových prostriedkov, ktoré slúžia na prepojenie počítačov, serverov, sieťových zariadení, tlačiarní a ďalších zariadení a umožňujú prístup k informačným systémom, službám, údajom a internetu.

Dodávateľ – externá osoba alebo organizácia, ktorá na základe zmluvy, objednávky alebo iného právneho vzťahu dodáva, spravuje, udržiava alebo podporuje informačné systémy, technické prostriedky, programové vybavenie, služby alebo dátovú sieť VŠZaSP sv. Alžbety.

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

Dostupnosť – vlastnosť IS, ktorá zaisťuje, že autorizovaní používatelia majú nepretržitý a spoľahlivý prístup k potrebným informáciám, údajom a zdrojom vtedy, keď ich potrebujú. Dostupnosť zahŕňa ochranu systémov a služieb pred výpadkami, útokmi a inými udalosťami, ktoré by mohli znemožniť alebo obmedziť prístup k týmto zdrojom.

Dôvernosť – vlastnosť IS, ktorá zabezpečuje, že informácie a údaje sú prístupné iba oprávneným osobám alebo systémom, a sú chránené pred neautorizovaným prístupom alebo zverejnením. Pod prístupom sa rozumie zobrazenie, skopírovanie, vytlačenie údajov, i samotné zistenie faktu, že došlo k prenosu (uloženiu) údajov.

Informačné technológie (IT) – súbor technológií a infraštruktúry používaných na spracovanie informácií. IT zahŕňa technológie potrebné na prevádzku a údržbu informačných systémov, dátových sietí a aplikácií.

Informačný systém (IS) – integrovaný súbor komponentov – zahŕňajúci hardvér, softvér, dáta a procedúry – ktoré sú navrhnuté na zber, ukladanie, spracovanie a distribúciu informácií. Tieto systémy môžu byť použité na správu, analýzu a organizáciu údajov, vrátane osobných údajov, a slúžia na podporu činností a rozhodovacích procesov vysokej školy. Informačný systém zahŕňa všetky procesy a technológie potrebné na efektívne spracovanie a ochranu osobných údajov, vrátane zabezpečenia ich dôvernosti, integrity a dostupnosti.

Integrita – vlastnosť IS, ktorá zabezpečuje ochranu údajov pred neautorizovanou modifikáciou, neúmyselnými chybami a poškodením, a ktorá zaručuje, že údaje zostávajú verné svojmu pôvodnému stavu počas ich spracovania, ukladania a prenosu.

Komunikačná infraštruktúra – technické a programové prostriedky zabezpečujúce prenos dát a komunikáciu v rámci dátovej siete, najmä sieťové zariadenia, prístupové body, smerovače, prepínače, bezpečnostné prvky a súvisiace služby.

MFA (Viacfaktorové overovanie) – viacfaktorová autentifikácia – bezpečnostný spôsob overenia identity používateľa pomocou najmenej dvoch nezávislých faktorov, napríklad hesla a jednorazového kódu, mobilnej aplikácie, hardvérového kľúča alebo iného schváleného overovacieho prostriedku.“

Osobné údaje – údaje týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby podľa právnych predpisov na ochranu osobných údajov.

Používateľ – autorizovaná osoba, ktorá používa informačné technológie a systémy na vykonávanie svojich študijných, pracovných alebo osobných úloh ako koncový používateľ.

Používateľské konto – účet pridelený používateľovi na prístup do informačného systému, aplikácie, dátovej siete, elektronickej pošty alebo inej služby VŠZaSP sv. Alžbety.

Poverená osoba pre informačnú a kybernetickú bezpečnosť / Bezpečnostný manažér IT (CISO) – osoba určená vedením alebo štatutárnym orgánom vysokej školy na koordináciu, kontrolu a rozvoj opatrení v oblasti informačnej a kybernetickej bezpečnosti. Ak takáto osoba nie je určená, úlohy v tejto oblasti vykonáva vedenie vysokej školy v spolupráci s osobami zabezpečujúcimi správu informačných technológií.

Prístupové práva – oprávnenia pridelené používateľovi, administrátorovi alebo inej oprávnenej osobe, ktoré určujú, ku ktorým systémom, údajom, aplikáciám alebo službám má prístup a aké činnosti v nich môže vykonávať.

Privilegovaný prístup – prístup s rozšírenými oprávneniami, najmä administrátorský alebo správcovský prístup, ktorý umožňuje správu systému, zmenu nastavení, prideľovanie práv alebo prístup k väčšiemu rozsahu údajov.

Programové vybavenie (softvér) – súbor programov, aplikácií a systémových nástrojov, ktoré riadia a koordinujú činnosť hardvéru, umožňujú prácu s údajmi a poskytujú rôzne služby a funkcie informačného systému, vrátane operačných systémov, firmvéru, databázového softvéru, bezpečnostných aplikácií a používateľských programov.

Retenčná lehota – doba, počas ktorej sa uchovávajú údaje, záznamy, dokumenty alebo iné informácie; po jej uplynutí sa údaje vymažú, zlikvidujú alebo archivujú podľa príslušných pravidiel.

Riadenie prístupu – proces a súbor postupov na kontrolu, kto má oprávnenie pristupovať k jednotlivým aktívam informačného systému, a to na základe stanovených pravidiel a politiky organizácie. Cieľom riadenia prístupu je zabezpečiť, aby iba autorizovaní používatelia mali prístup k citlivým informáciám, systémom a zdrojom, čím sa minimalizuje riziko neoprávneného prístupu, zneužitia alebo úniku dát. To zahŕňa autentifikáciu, autorizáciu, prideľovanie a revíziu prístupových práv.

RPO (Recovery Point Objective) - maximálna prípustná strata dát, ktorá môže nastať v prípade incidentu alebo výpadku systému. RPO určuje, ako staré môžu byť dáta, ktoré sa použijú na obnovu, alebo aký časový interval je prijateľný medzi poslednou zálohou a časom incidentu.

RTO (Recovery Time Objective) – maximálny čas, ktorý je prípustný na obnovu systému alebo dát po výpadku alebo incidente, aby sa minimalizoval dopad na prevádzku. RTO stanovuje, ako rýchlo musí byť systém alebo dáta obnovené, aby sa splnili požiadavky na prevádzkovú kontinuitu a minimalizovali sa škody spôsobené výpadkom.

Server – obslužný počítač alebo program, ktorý poskytuje presne stanovené služby alebo prostriedky používateľom.

Sieťová aplikácia – program, ktorý pracuje pre používateľa a ktorý používateľovi poskytuje vopred stanovené sieťové služby.

Sieťová služba – služba na zabezpečenie stanovených požiadaviek alebo potrieb používateľov.

Správca dátovej siete – interná alebo externá osoba zodpovedná za prevádzku konkrétnej dátovej siete, jej časti alebo sieťovej aplikácie.

Šifrovanie – proces konverzie čitateľných údajov (plaintext) do nečitateľnej formy (ciphertext) pomocou kryptografického algoritmu a šifrovacieho kľúča, aby boli chránené pred neoprávneným prístupom. Šifrovanie zabezpečuje, že len oprávnené strany, ktoré majú správny dešifrovací kľúč, môžu údaje prečítať a pochopiť ich obsah. Používa sa na ochranu citlivých informácií pri prenose po sieti, ako aj pri ich ukladaní, čím zvyšuje dôvernosť a integritu údajov.

Technické prostriedky (hardvér) – fyzické komponenty informačného systému, vrátane zariadení, ako sú servery, počítače, sieťové zariadenia, úložiská, periférie a iné elektronické vybavenie, ktoré zabezpečujú funkčnosť systému a umožňujú spracovanie, ukladanie a prenos dát.

Vlastník aktíva – organizačný útvar, ktorý zodpovedá za funkčnosť, ochranu, správu a riadenie prístupu ku konkrétnemu aktívu. Vlastník aktíva má zodpovednosť za určenie požiadaviek na ochranu, zabezpečenie primeraných bezpečnostných opatrení, a monitorovanie ich účinnosti, aby sa zabezpečila bezpečnosť a dostupnosť aktíva. V podmienkach VŠZaSP sv. Alžbety je vlastníkom aktíva ten organizačný útvar, ktorý v zmysle pracovných povinností zhromažďuje, spracúva a archivuje príslušné dáta (údaje, informácie), napr. vlastníkom dát o štúdiu a študentoch je študijné oddelenie.

Záloha – kópia údajov, systému, databázy, aplikácie alebo konfigurácie vytvorená na účely obnovy v prípade straty, poškodenia, výpadku, bezpečnostného incidentu alebo inej mimoriadnej udalosti.

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

Skratka	Popis skratky
AIS	Akademický informačný systém
DPO	Data Protection Officer– osoba určená podľa právnych predpisov na ochranu osobných údajov, ktorá dohliada na dodržiavanie pravidiel ochrany osobných údajov a poskytuje súčinnosť pri otázkach týkajúcich sa spracúvania osobných údajov.
GDPR	Nariadenie Európskeho parlamentu a Rady EÚ 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
IDM	Identity Management; správa používateľských identít a účtov.
IT	Informačné technológie
MKB	Manažér kybernetickej bezpečnosti
RPO	Recovery Point Objective – maximálna prípustná strata dát, ktorá môže nastať v prípade incidentu alebo výpadku systému. RPO určuje, ako staré môžu byť dáta, ktoré sa použijú na obnovu, alebo aký časový interval je prijateľný medzi poslednou zálohou a časom incidentu.
RTO	Recovery Time Objective – maximálny čas prípustný na obnovu systému, služby alebo dát po výpadku, havárii alebo bezpečnostnom incidente tak, aby sa minimalizoval dopad na prevádzku. RTO určuje, ako rýchlo musí byť systém, služba alebo dáta obnovené, aby boli splnené požiadavky na kontinuitu činnosti.
SIF	Systémový integrátor fakulty / pracoviska - rola zodpovedná za správu oprávnení v rozsahu príslušného pracoviska.
SIU	Systémový integrátor univerzity - rola zodpovedná za správu a prideľovanie oprávnení na úrovni celej školy.
SLA	Service Level Agreement; dohoda o úrovni poskytovanej služby, najmä o jej dostupnosti a podmienkach podpory.
UIS	Univerzitný informačný systém; akademický informačný systém používaný VŠZaSP.
VPN	Virtual Private Network; zabezpečené sieťové spojenie umožňujúce komunikáciu medzi systémami alebo sieťami.
VŠZaSP	Vysoká škola zdravotníctva a sociálnej práce

7.Súvisiace dokumenty

[1] Organizačný poriadok Vysokej školy zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
[2] Disciplinárny poriadok Vysokej školy zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
[3] Pracovný poriadok (Vysokej školy zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.)
[4] Smernica o práci, spracovávaní, oznamovaní a nakladaní s osobnými údajmi študentov a učiteľov a ich ochrane na Vysokej školy zdravotníctva a sociálnej práce sv. Alžbety, n. o. v Bratislave
[5] Zásady spracúvania osobných údajov - GDPR predpis dostupný na www.vssvalzbety.sk/gdpr/

8. Smernica o kybernetickej bezpečnosti a riadení IT Vysokej školy zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.

8.1. Základné ustanovenia

Táto smernica je záväzná pre všetky osoby uvedené v kapitole 3 Rozsah tejto smernice.

Informačný systém VŠZaSP sv. Alžbety sa používa na účely súvisiace s činnosťou vysokej školy, najmä na zabezpečenie vzdelávacej, vedeckej, výskumnej, administratívnej, riadiacej a prevádzkovej činnosti vysokej školy.

Používatelia sú oprávnení používať informačný systém, technické prostriedky, programové vybavenie, dátovú sieť, aplikácie, elektronickú poštu a údaje VŠZaSP sv. Alžbety len v rozsahu pridelených práv a oprávnení.

Každý používateľ je povinný bezodkladne hlásiť bezpečnostné incidenty, technické poruchy, podozrenie na neoprávnený prístup alebo zneužitie informačného systému spôsobom uvedeným v časti 8.10 tejto smernice.

Podrobné pravidlá správy, prevádzky, používania a ochrany informačného systému sú uvedené v nasledujúcich častiach tejto smernice.

Zmeny a doplnenia tejto smernice sa vykonávajú formou revízie dokumentu a zaznamenávajú sa v časti Zoznam revízií, ktorá tvorí súčasť tejto smernice.

Dňom nadobudnutia účinnosti tejto smernice sa zrušujú predchádzajúce interné predpisy alebo ich časti, ktoré upravujú rovnakú oblasť a sú v rozpore s touto smernicou, ak VŠZaSP sv. Alžbety nerozhodne inak.

Táto smernica nadobúda platnosť dňom jej podpisu štatutárnym orgánom VŠZaSP sv. Alžbety a účinnosť dňom uvedeným v tejto smernici. Zmeny a doplnenia smernice sa vykonávajú formou revízie dokumentu.

8.2. Vymedzenie rolí a činností pri správe a používaní informačného systému

V tejto časti sú špecifikované činnosti súvisiace s bezpečnou a spoľahlivou prevádzkou a používaním informačného systému pre jednotlivé skupiny používateľov VŠZaSP sv. Alžbety.

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

IT rolou podľa tejto smernice sa rozumie osoba, útvar alebo zmluvný dodávateľ, ktorý vykonáva príslušnú činnosť na základe poverenia, prideleného oprávnenia alebo zmluvného vzťahu s VŠZaSP sv. Alžbety.

Roly uvedené v tejto časti slúžia na vecné rozdelenie činností pri správe a používaní informačného systému a nemusia zodpovedať samostatným pracovným pozíciám VŠZaSP sv. Alžbety.

VŠZaSP sv. Alžbety vedie internú evidenciu informačných systémov, ich správcov, technickej infraštruktúry a zodpovedných IT rolí.

8.2.1 Systémový administrátor IT

- inštaluje, nastavuje a udržiava systémové programy, najmä operačné systémy,
- zabezpečuje prevádzkyschopnosť systémových prostriedkov, serverov a nástrojov,
- podieľa sa na zriaďovaní, zmene, preverovaní a rušení používateľských kont a prístupových práv,
- podieľa sa na zálohovaní, obnove údajov a riešení havarijných stavov,
- monitoruje stav systémov a technických súčastí informačného systému,
- vykonáva ďalšie činnosti určené VŠZaSP sv. Alžbety.

8.2.2 Správca siete IT

- Podľa pravidiel VŠZaSP sv. Alžbety nastavuje prístupové práva na aktívnych sieťových prvkoch a komunikačných zariadeniach.
- Pravidelne monitoruje stav siete pomocou programových nástrojov pre riadenie siete.
- Udržuje v aktuálnom stave informácie o topológii siete, aktívnych a pasívnych prvkoch, o ich parametroch a nastaveniach. Rieši havarijné stavy.
- Podrobný popis práv a povinností správcov dátovej siete VŠZaSP sv. Alžbety je uvedený najmä v časti 8.3.4 Práva a povinnosti správcov dátovej siete a v súvisiacich ustanoveniach časti 8.3 Pravidlá správy a prevádzky dátovej siete a komunikačnej infraštruktúry.

8.2.3 Databázový administrátor IT / privilegovaný používateľ

- spravuje databázy, databázové účty a prístupové oprávnenia,
- vykonáva údržbu, monitorovanie, zálohovanie a obnovu databáz,
- rieši havarijné a neštandardné stavy databáz,
- testuje a nasadzuje aktualizácie alebo nové databázové riešenia,
- kontroluje auditné a logovacie záznamy súvisiace s databázami

8.2.4 Technik IT

- Odstraňuje technické poruchy a závady na zariadeniach IT, a to buď svojpomocne, napríklad výmenou súčiastky, časti dielu alebo celého dielu za nový v rámci záručných podmienok, alebo formou doručenia chybného zariadenia do príslušného servisného strediska alebo dohovoru o oprave cez dodávateľa daného zariadenia.
- Realizuje technické prepojenia lokálnych počítačových sietí na pracoviskách VŠZaSP sv. Alžbety.

- Pripája zariadenia IT do elektrickej siete napájania a do dátovej siete VŠZaSP sv. Alžbety.
- Prepája jednotlivé zariadenia IT medzi sebou.
- Na základe poverenia vykonáva kontrolu nainštalovaného softvéru na PC a o výsledku vyhotoví záznam.
- Vykonáva previerku zariadení IT, ktoré podliehajú pravidelnému technickému auditu s tým, že pripravuje inováciu zariadení IT tak, aby na nich bolo možné inštalovať najnovšie verzie operačných, systémových a aplikačných programových produktov.
- Dôsledne aplikuje opravy, patche, odporúčané výrobcom pre operačné systémy a systémové programy na všetkých inštalovaných zariadeniach IT na VŠZaSP sv. Alžbety v okruhu svojej pôsobnosti.

8.2.5 Používateľ IT

- Používa PC, operačný systém na ňom nainštalovaný, ako aj všetky aplikácie, na ktoré dostal oprávnenie.
- Prihlasuje sa do dátovej siete VŠZaSP sv. Alžbety a používa zdieľané súbory, databázy, aplikácie, tlačiarne či iné zariadenia podľa pridelených práv.
- Je preukázateľne poučený o povinnosti dodržiavať túto smernicu a riadiť sa ňou pri svojej práci.
- Riadi sa pokynmi príslušnej IT roly a obracia sa na ňu v prípade závad, porúch a mimoriadnych situácií.
- Dbá na ochranu spracovávaných dát.

Používateľov informačného systému VŠZaSP sv. Alžbety členíme pre účely tejto smernice podľa spôsobu a rozsahu používania informačných systémov, služieb a prostriedkov informačných technológií na **tieto kategórie:**

8.2.5.1 Používateľ internetu

Používateľom internetu je zamestnanec, študent alebo iná oprávnená osoba, ktorej bolo pridelené používateľské konto alebo iné oprávnenie a na základe toho jej bol umožnený prístup do celosvetovej počítačovej siete Internet prostredníctvom technických prostriedkov alebo dátovej siete vysokej školy.

8.2.5.2 Používateľ interných informačných služieb

Používateľom interných informačných služieb je používateľ, ktorému bolo pridelené oprávnenie na prístup k interným informačným systémom, aplikáciám, službám alebo dátam školy.

8.2.5.3 Používateľ elektronickej pošty

Používateľom elektronickej pošty je zamestnanec, študent alebo iná oprávnená osoba, ktorej bolo pridelené používateľské konto elektronickej pošty a na základe toho jej bolo umožnené používanie elektronickej pošty, e-mailu.

8.2.5.4 Zamestnanec

Pre účely tejto smernice sa za zamestnanca považujú všetci zamestnanci VŠZaSP sv. Alžbety v pracovnom pomere, ako aj osoby vykonávajúce činnosť pre vysokú školu na základe dohody, obdobného pracovnoprávneho vzťahu alebo iného zmluvného vzťahu, ak používajú informačné

systémy, technické prostriedky, aplikácie, elektronickú poštu, dátovú sieť alebo dáta vysokej školy.

8.2.5.5 Študent

Pre účely tejto smernice sa za študenta považujú študenti všetkých stupňov – bakalárskeho, magisterského, doktorandského, a foriem, a to tak dennej ako aj externej formy štúdia.

8.2.5.6 Iný oprávnený používateľ

Za iného oprávneného používateľa sa pre účely tejto smernice považuje osoba, ktorá nie je zamestnancom ani študentom školy, ale ktorej bol na základe oprávnenia udeleného vysokou školou umožnený prístup k informačnému systému, dátovej sieti, elektronickej pošte, aplikáciám, technickým prostriedkom, programovému vybaveniu, interným informačným službám alebo dátam.

8.3. Pravidlá správy a prevádzky dátovej siete a komunikačnej infraštruktúry

V tejto časti sú špecifikované činnosti súvisiace s bezpečnou a spoľahlivou prevádzkou a používaním informačného systému pre jednotlivé skupiny zamestnancov a študentov školy.

8.3.1 Vymedzenie dátovej siete a komunikačnej infraštruktúry

Dátová sieť VŠZaSP sv. Alžbety je súčasťou technickej infraštruktúry vysokej školy a slúži na zabezpečenie výučby, výskumu, administratívnej, riadiacej, prevádzkovej a ďalšej činnosti vysokej školy.

Pod pojmom dátová sieť VŠZaSP sv. Alžbety sa na účely tejto smernice rozumejú všetky technické a programové prostriedky slúžiace na prepojenie počítačov, serverov, sieťových zariadení, tlačiarní a ďalších zariadení, ako aj prostriedky na využitie tohto pripojenia.

Poslaním dátovej siete VŠZaSP sv. Alžbety je vzájomné prepojenie objektov, pracovísk, organizačných súčastí, detašovaných pracovísk alebo iných pracovísk VŠZaSP sv. Alžbety a zabezpečenie ich pripojenia k informačným systémom, aplikáciám, dátam, interným službám a internetu na účely činnosti vysokej školy.

Pre účely tejto smernice sa dátová sieť a komunikačná infraštruktúra môže členiť najmä na:

a) centrálnu, chrbticovú alebo inú hlavnú sieťovú infraštruktúru VŠZaSP sv. Alžbety, ak je v príslušnej lokalite zriadená,
b) lokálne siete pracovísk, organizačných súčastí, detašovaných pracovísk alebo iných pracovísk VŠZaSP sv. Alžbety,
c) sieťové aplikácie a služby,
d) pripojenia do internetu,
e) bezdrôtové siete vrátane Wi-FI,
f) vzdialené prístupy,
g) aktívne prvky komunikačnej infraštruktúry, najmä smerovače, prepínače, prístupové body a bezpečnostné brány.

Pravidlá uvedené v tejto kapitole sú záväzné pre správcov dátovej siete a pre používateľov technických prostriedkov pripojených k dátovej sieti školy.

8.3.2 Prístupové práva a identifikácia používateľov

Dátovú sieť VŠZaSP sv. Alžbety môžu využívať len oprávnení používatelia. Oprávnenými používateľmi sú používatelia, ktorým bolo pridelené príslušné oprávnenie na prístup k dátovej sieti, informačnému systému alebo službám a ktorí boli preukázateľne oboznámení s touto smernicou.

Evidenciu používateľov dátovej siete, IP adries zariadení a využívania doménového priestoru vedie správca dátovej siete v rozsahu potrebnom na plnenie úloh a povinností vyplývajúcich z tejto smernice a všeobecne záväzných právnych predpisov.

Oprávnenie používať prostriedky dátovej siete majú oprávnení používatelia VŠZaSP sv. Alžbety.

Používanie dátovej siete osobami mimo VŠZaSP sv. Alžbety je možné len na základe schválenia podľa pravidiel vysokej školy. Výnimku tvorí používanie hosťovského prístupu (najmä WiFi), ktorý je na tento účel zriadený.

Pokiaľ je pre prístup k dátovej sieti VŠZaSP sv. Alžbety požadovaná identifikácia používateľa, používateľ je povinný používať meno pridelené správcom dátovej siete alebo príslušného informačného systému.

Používateľ je povinný používať na overenie identity heslo vytvorené na základe pravidiel ustanovených touto smernicou, udržiavať toto heslo v tajnosti a chrániť ho tak, aby bolo zabránené jeho zneužitiu.

Používateľ nesmie poskytnúť pridelené prihlasovacie meno, heslo alebo iný autentifikačný prostriedok inej osobe. Za hrubé porušenie pravidiel sa považuje poskytnutie prihlasovacieho mena, hesla alebo iného autentifikačného prostriedku osobe, ktorá nemá nárok na prístup do dátovej siete alebo ktorej bol prístup odopretý alebo zablokovaný.

Používateľ nesmie zneužiť nedbanlivé správanie iného používateľa, najmä náhodné zistenie prihlasovacieho mena a hesla, zabudnuté odhlásenie alebo obdobnú situáciu, na to, aby pracoval pod cudzím menom, heslom alebo iným prístupovým oprávnením.

Prístupové práva používateľa sa prideľujú podľa schváleného procesu školy.

Používateľ sa nesmie žiadnymi prostriedkami pokúsiť získať prístupové práva, ktoré mu neboli pridelené. Pokiaľ používateľ získa prístupové práva neoprávnene bez vlastného pričinenia, je povinný túto skutočnosť bezodkladne ohlásiť určeným spôsobom a tieto práva nesmie použiť.

Používateľ sa dopustí hrubého porušenia pravidiel, pokiaľ sa pokúsi zneužiť dátovú sieť školy na získanie neautorizovaných prístupových práv k akýmkoľvek informačným zdrojom dostupným prostredníctvom dátovej siete, alebo pokiaľ podnikne cez dátovú sieť softvérové útoky na počítače a iné zariadenia kdekoľvek v sieti Internet.

8.3.3 Organizačné zabezpečenie správy dátovej siete

Správa dátovej siete VŠZaSP sv. Alžbety sa zabezpečuje podľa technického a organizačného

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

usporiadania vysokej školy prostredníctvom príslušných IT rolí.

Správa dátovej siete môže zahŕňať správu lokálnych sietí pracovísk VŠZaSP sv. Alžbety, správu sieťových aplikácií a služieb, správu pripojenia do internetu, správu bezdrôtových sietí, správu vzdialeného prístupu a správu aktívnych prvkov komunikačnej infraštruktúry.

Správu lokálnych sietí pracovísk zabezpečujú príslušné IT roly podľa pridelených oprávnení a zodpovedností. Správa sieťových aplikácií a služieb sa vykonáva v rozsahu potrebnom na zabezpečenie ich dostupnosti, funkčnosti, bezpečnosti a oprávneného používania používateľmi školy.

Prevádzku centrálnych informačných systémov, aplikácií, serverov, dátových úložísk a iných technických prostriedkov zabezpečujú príslušné IT roly.

Správcovia dátovej siete, informačných systémov a sieťových služieb spolupracujú s určenými osobami v oblasti informačnej a kybernetickej bezpečnosti, ochrany osobných údajov, správy aktív a riadenia prístupových práv.

Zoznam IT rolí s administrátorskými alebo privilegovanými oprávneniami vedie VŠZaSP sv. Alžbety v rozsahu určenom vysokou školou.

Rozsah oprávnení, povinností a zodpovedností IT rolí musí byť určený poverením, prideleným oprávnením, zmluvou alebo iným preukázateľným spôsobom.

8.3.4 Práva a povinnosti správcov dátovej siete

Správca lokálnej sieťovej aplikácie a lokálnych serverov najmä:

- zabezpečuje prevádzku sieťovej aplikácie, najmä jej inštaláciu, úpravy, konfiguráciu a zálohovanie dát,
- vytvára a spravuje používateľské kontá a prístupové práva podľa schváleného procesu,
- zodpovedá za bezpečné uloženie záložných dát a rieši havarijné stavy.

Správca lokálnej siete pracoviska VŠZaSP sv. Alžbety najmä:

- zabezpečuje prevádzku lokálnej siete od prípojného miesta siete až ku koncovým používateľským pracovným staniciam,
- zabezpečuje správnu funkciu lokálnych serverov,
- vytvára a spravuje používateľské kontá a prístupové práva podľa schváleného procesu,
- udržuje konfiguráciu systémov pre počítače, ktorých systém je spúšťaný zo servera,
- zabezpečuje prideľovanie IP adries podľa technického nastavenia siete,
- vedie evidenciu MAC a IP adries v rozsahu určenom VŠZaSP sv. Alžbety,
- spravuje príslušný doménový priestor pracoviska alebo VŠZaSP sv. Alžbety,
- informuje používateľov o pravidlách práce v sieti,
- zodpovedá za bezpečné uloženie záložných dát a rieši havarijné stavy.

Správca dátovej siete VŠZaSP sv. Alžbety najmä:

- zabezpečuje prevádzku dátovej siete v rozsahu svojej pôsobnosti,

- zabezpečuje konektivitu pripojených dátových sietí a sieťových služieb,
- monitoruje dátovú sieť podľa nastavených pravidiel,
- zabezpečuje prevádzku centrálnych serverov,
- poskytuje odborné konzultácie vedeniu vysokej školy,
- sleduje vývojové trendy v oblasti dátových sietí a navrhuje spôsob ich implementácie do dátovej siete VŠZaSP sv. Alžbety,
- organizuje zavádzanie nových sieťových služieb,
- poskytuje odborné konzultácie správcom lokálnych sietí, pracovísk alebo súvisiacich systémov,
- riadi správu doménového priestoru VŠZaSP sv. Alžbety.

Správca siete na všetkých úrovniach najmä:

- zabezpečuje prevádzku siete, servera alebo sieťovej aplikácie,
- kontroluje dodržiavanie pravidiel prevádzky siete,
- monitoruje prevádzku siete a rieši prípadné kolízie,
- zabezpečuje zálohovanie a archiváciu dát podľa pravidiel VŠZaSP sv. Alžbety.

8.3.5 Používanie dátovej siete

Používateľ môže používať výpočtové prostriedky a dátovú sieť VŠZaSP sv. Alžbety výlučne na vzdelávacie, vedecké, výskumné, vývojové, odborné, administratívne, prevádzkové a riadiace účely súvisiace s činnosťou vysokej školy.

Za porušenie pravidiel sa považuje najmä používanie dátovej siete na účely nesúvisiace s činnosťou školy, najmä na komerčnú činnosť bez súvisu s činnosťou vysokej školy, neoprávnené šírenie reklamného, politického, ideologického, diskriminačného, protiprávneho, škodlivého alebo inak nevhodného obsahu.

Používateľ má právo používať výlučne legálne nadobudnuté programové vybavenie. Kopírovať programy je možné pri dodržaní platných autorských zákonov.

Voľne dostupné programové produkty a informačné materiály získané pomocou dátovej siete VŠZaSP sv. Alžbety smie používateľ používať výlučne na účely uvedené v tejto smernici.

Za hrubé porušenie pravidiel sa považuje použitie dátovej siete školy na ponuku, šírenie alebo sprístupňovanie nelegálne získaného softvéru, dát, informácií alebo autorsky chráneného obsahu.

Používateľ nesmie zasahovať do žiadnych programových produktov, dát, systémového a technického prostredia dátovej siete bez výslovného súhlasu správcu siete.

Zvlášť prísne zakázané sú neautorizované zmeny konfigurácie počítačov alebo iných prostriedkov, ktoré by mohli mať vplyv na správnu prevádzku dátovej siete.

Používatelia nie sú oprávnení inštalovať programové vybavenie bez schválenia príslušnej IT roly.

Používateľ používa vyčlenený diskový priestor, výpočtové prostriedky a dátovú sieť vysokej školy primerane a s ohľadom na ich dostupnosť a zaťaženie.

Používateľ nesmie vedome:

- narušiť činnosť výpočtových prostriedkov,
- obmedziť prácu ďalších používateľov,
- obmedziť chod alebo výkonnosť siete.

Používateľ je povinný bezodkladne vykonať pokyny príslušnej IT roly na zníženie záťaže siete.

Veľkosť odosielaných správ, príloh a využívaného úložiska môže byť obmedzená technickými limitmi používaných služieb.

Pri prekročení používateľských limitov môže dôjsť k obmedzeniu alebo zablokovaniu príslušnej služby.

VŠZaSP sv. Alžbety nezodpovedá za stratu používateľských dát uložených mimo určených alebo schválených úložísk, ak osobitné pravidlá, zmluvné podmienky alebo rozhodnutie vysokej školy neurčujú inak.

Používatelia sú povinní ukladať pracovné dokumenty a osobné údaje do úložísk určených alebo schválených vysokou školou.

Používateľ nesmie ďalej používať zariadenie, pri ktorom je dôvodné podozrenie na napadnutie škodlivým kódom, a je povinný bezodkladne vykonať primerané opatrenia, najmä odpojiť zariadenie od siete a kontaktovať príslušnú IT rolu.

8.3.6 Pravidlá pripojenia k dátovej sieti

Používateľ dátovej siete je povinný požiadať príslušnú IT rolu o súhlas pred pripojením nového zariadenia k dátovej sieti, pred zmenou konfigurácie zariadenia, ktorá môže mať vplyv na prevádzku siete, alebo pred trvalým odpojením zariadenia od dátovej siete.

Pripojené zariadenia sa registrujú prostredníctvom protokolu DHCP a sieťová adresa sa prideľuje podľa pravidiel školy.

Za správnu inštaláciu operačného systému a sieťového programového vybavenia zariadení pripojených k dátovej sieti zodpovedá príslušná IT rola.

Používateľ nesmie používať inú sieťovú adresu než tú, ktorá mu bola pridelená.

8.3.7 Riadenie prístupu k aktívnym prvkom komunikačnej infraštruktúry

Prístup k aktívnym prvkom komunikačnej infraštruktúry majú výhradne určené IT roly. Prístup IT rolí k aktívnym prvkom musí byť obmedzený na nevyhnutný rozsah a preukázateľne určený.

Aktívnymi prvkami komunikačnej infraštruktúry sú najmä smerovače, prepínače, prístupové body bezdrôtovej siete, bezpečnostné brány, firewally a iné zariadenia zabezpečujúce prenos, smerovanie, filtrovanie alebo ochranu sieťovej komunikácie..

Prístupové práva k aktívnym prvkom komunikačnej infraštruktúry sa prideľujú len v rozsahu nevyhnutnom na výkon správy, údržby, monitorovania, konfigurácie alebo riešenia bezpečnostných a

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

prevádzkových udalostí.

Prístupové údaje k aktívnym prvkom komunikačnej infraštruktúry musia byť chránené pred neoprávneným prístupom, sprístupnením, stratou alebo zneužitím.

Konfiguráciu aktívnych prvkov môžu vykonávať len oprávnené IT roly tak, aby nebola ohrozená bezpečnosť, dostupnosť ani prevádzka dátovej siete.

Prístup a zmeny konfigurácie aktívnych prvkov sa evidujú v rozsahu určenom VŠZaSP sv. Alžbety. Konfigurácia aktívnych prvkov sa zálohuje podľa pravidiel školy.

8.3.8 Dokumentácia a evidencia dátovej siete

VŠZaSP sv. Alžbety vedie dokumentáciu dátovej siete v rozsahu určenom vysokou školou. Dokumentácia môže obsahovať najmä základnú topológiu siete, evidenciu sieťových prvkov, prístupov, konfigurácií, sieťových adries, zodpovedných IT rolí a významných zmien siete.

Dokumentácia dátovej siete sa priebežne aktualizuje a je dostupná iba oprávneným osobám.

8.4. Pravidlá používania technických a programových prostriedkov IT

V tejto časti sú upravené pravidlá používania technických prostriedkov, programového vybavenia, internetu, elektronickej pošty, interných informačných služieb a ďalších prostriedkov informačných technológií VŠZaSP sv. Alžbety.

8.4.1 Používanie hardvéru

Na pracoviskách VŠZaSP sv. Alžbety sa používa iba hardvér schválený a evidovaný podľa interných pravidiel vysokej školy. Iný hardvér možno používať len na základe predchádzajúceho schválenia.

Zakazuje sa neoprávnený zásah do hardvéru alebo jeho konfigurácie, ako aj jeho svojvoľné premiestňovanie či výmena. Tieto činnosti vykonáva príslušná IT rola na základe schváleného procesu.

Presun, sťahovanie alebo výmena hardvéru sa vykonáva a eviduje podľa interných pravidiel školy.

Používatelia IT, ktorým boli zverené alebo zapožičané prenosné notebooky alebo akékoľvek iné zariadenia IT, sú povinní používať ich tak, aby nedošlo k ich strate, zneužitiu alebo krádeži.

Používateľ nesmie zverené alebo zapožičané zariadenie prenechať tretej osobe, zaťažiť ho právom tretej osoby ani používať v rozpore s účelom jeho pridelenia.

Zverené IT zariadenie možno prenechať inej osobe len na základe predchádzajúceho schválenia

Dôverné údaje uložené na disku notebooku alebo inom prenosnom zariadení musia byť chránené

primeranými bezpečnostnými opatreniami, najmä šifrovaním, ak to technické možnosti a povaha údajov vyžadujú.

Poruchu hardvéru je používateľ povinný nahlásiť zodpovednej IT osobe.

Príslušná IT rola zabezpečí odstránenie poruchy, opravu alebo výmenu hardvéru podľa dohodnutého postupu.

8.4.2 Používanie vlastných zariadení používateľov

Používanie vlastných zariadení na prístup k informačným systémom, aplikáciám, dátam, elektronickej pošte alebo dátovej sieti VŠZaSP sv. Alžbety je možné len na základe povolenia vysokej školy.

Vlastné zariadenie možno používať len pri dodržaní bezpečnostných pravidiel tejto smernice a podmienok určených školou.

Používateľ vlastného zariadenia je povinný zabezpečiť zariadenie najmä:

- silným heslom alebo iným bezpečným spôsobom autentifikácie,
- pravidelnými aktualizáciami operačného systému a aplikácií,
- antivírusovou ochranou alebo inou bezpečnostnou ochranou, ak je pre daný typ zariadenia dostupná a vyžadovaná,
- ochranou pred neoprávneným prístupom,

Používateľ je povinný umožniť overenie splnenia bezpečnostných požiadaviek na vlastnom zariadení v rozsahu primeranom účelu, oprávneniam používateľa a pravidlám školy.

Prístup vlastných zariadení k interným informačným systémom, službám alebo dátam je možný len zabezpečeným spôsobom určeným školou.

Na vlastnom zariadení používateľa je zakázané uchovávať osobné údaje alebo dôverné údaje vysokej školy bez primeranej ochrany, najmä bez šifrovania alebo iného schváleného bezpečnostného opatrenia.

Stratu, krádež, podozrenie na napadnutie alebo zneužitie vlastného zariadenia je používateľ povinný bezodkladne oznámiť určeným spôsobom.

8.4.3 Používanie softvéru

Na technických prostriedkoch VŠZaSP sv. Alžbety je povolené používať len softvér schválený školou.

Používateľ IT používa len ten softvér, na ktorého používanie má podľa schválenej požiadavky, prideleného oprávnenia alebo rozhodnutia školy právo. Zmeny v používaní softvéru sa vykonávajú podľa schváleného procesu.

Inštaláciu a evidenciu softvéru zabezpečuje príslušná IT rola podľa interných pravidiel.

Poruchu softvéru je používateľ povinný nahlásiť určeným spôsobom. Príslušná IT rola zabezpečí odstránenie softvérovej poruchy podľa dohodnutého postupu.

Zakazuje sa používať, uchovávať alebo distribuovať akýkoľvek pirátsky softvér a neoprávnene nadobudnuté údaje na hardvérovom vybavení školy.

Aktuálnosť softvéru a bezpečnostných opráv sa kontroluje a zabezpečuje podľa pravidiel školy.

8.4.4 Používanie internetu, interných informačných služieb a elektronickej pošty

Na elektronickú poštu zamestnanca alebo iného oprávneného používateľa VŠZaSP sv. Alžbety je potrebné nahliadať ako na neverejnú komunikáciu medzi jednotlivými subjektmi, na ktorú sa vzťahuje ochrana súkromia a príslušné právne predpisy.

Pre zaistenie bezpečnosti a kontinuity prevádzky informačného systému a dátovej siete, ako aj v prípade požiadavky na súčinnosť orgánom činným v trestnom konaní, môže VŠZaSP sv. Alžbety v súlade s právnymi predpismi a internými pravidlami pristupovať k dostupným záznamom súvisiacim s elektronickou poštou, prístupom na internet alebo prístupom do informačných systémov.

Zakazuje sa zobrazovanie, uchovávanie, šírenie alebo spracúvanie obsahu, ktorý je protiprávny, nevhodný alebo nesúvisí s činnosťou vysokej školy.

Prístup na internet a elektronickú poštu sa nesmie použiť v rozpore s právnymi predpismi, internými pravidlami alebo právami tretích osôb.

Akýkoľvek softvér, súbory alebo dokumenty získané prostredníctvom internetu a uložené na počítači alebo inom zariadení vysokej školy sa môžu používať výhradne spôsobom, ktorý je v súlade s ich licenciami, autorskými právami a účelom súvisiacim s pracovnými, študijnými alebo inými oprávnenými povinnosťami používateľa IT.

Zakazuje sa používať technické prostriedky, dátovú sieť alebo informačné systémy školy na zábavný obsah, hry alebo súbory nesúvisiace s oprávneným účelom ich použitia.

Zakazuje sa rozširovanie akéhokoľvek softvéru alebo údajov, ktoré sú majetkom, aktívom alebo chráneným obsahom VŠZaSP sv. Alžbety, bez oprávnenia.

Používateľom sa zakazuje využívať internet alebo elektronickú poštu na šírenie škodlivého softvéru alebo iného škodlivého obsahu.

Používateľ nesmie využiť internet alebo elektronickú poštu na narušenie bezpečnosti, dostupnosti, súkromia alebo riadnej prevádzky systémov, sietí, používateľov alebo tretích osôb.

Každý používateľ internetu a elektronickej pošty sa identifikuje svojim menom, prípadne pracovným zaradením, študijným zaradením alebo iným údajom, ak sa to pri danej komunikácii vyžaduje.

Hovoriť, písať alebo prispievať v mene VŠZaSP sv. Alžbety do diskusných skupín, fór, médií alebo iných verejných komunikačných priestorov môžu len osoby, ktoré sú na to riadne poverené.

Používatelia sa môžu zapájať do verejných diskusií a fór len spôsobom, ktorý nesmie vytvárať dojem, že vystupujú v mene VŠZaSP sv. Alžbety, ak na to neboli poverení.

Pri verejnej elektronickej komunikácii je používateľ povinný zdržať sa prejavov, ktoré sú protiprávne, diskriminačné, urážlivé, neoprávnené alebo poškodzujú dobré meno VŠZaSP sv. Alžbety, ako aj neoprávneného zverejňovania údajov alebo interných informácií.

Používatelia internetu a elektronickej pošty môžu využívať prístup na internet a elektronickú poštu na prieskum alebo prezeranie informačných zdrojov nesúvisiacich s pracovnou alebo študijnou náplňou počas prestávky alebo mimo pracovnej doby, ak sú dodržané všetky ustanovenia tejto smernice.

VŠZaSP sv. Alžbety poskytne orgánom činným v trestnom konaní dostupné záznamy týkajúce sa prístupu na internet alebo elektronickú poštu príslušného používateľa, ak jej taká povinnosť vyplýva z príslušných právnych predpisov.

Používateľ internetu a elektronickej pošty je povinný riadiť sa právnymi predpismi, autorským právom, právami k ochranným známkam a inými právami tretích osôb.

Komerčné používanie internetu mimo činnosti VŠZaSP sv. Alžbety je možné len na základe povolenia vysokej školy.

8.4.5 Používanie hlasovej, faxovej a obrazovej komunikácie pri posielaní osobných údajov alebo iných citlivých informácií

Používanie hlasovej, faxovej a obrazovej komunikácie pri posielaní osobných údajov alebo iných citlivých informácií sa riadi touto smernicou, internými pravidlami a príslušnými právnymi predpismi v oblasti ochrany osobných údajov.

Pri používaní hlasovej, faxovej a obrazovej komunikácie je potrebné dodržiavať pravidlá ochrany osobných údajov, dôverných a iných citlivých informácií.

Porušenie pravidiel pri používaní hlasovej, faxovej alebo obrazovej komunikácie môže byť posudzované ako porušenie pracovnej disciplíny, porušenie študijných povinností alebo porušenie zmluvných povinností podľa postavenia konkrétnej osoby.

Osobné údaje a citlivé informácie môžu prostredníctvom hlasovej, faxovej alebo obrazovej komunikácie posielať len poverené osoby podľa pravidiel vysokej školy.

Všetky zariadenia slúžiace na zber, archivovanie a posielanie osobných údajov alebo iných citlivých informácií sa musia využívať v súlade s pridelenými oprávneniami a pravidlami ustanovenými touto smernicou.

Používatelia sú povinní určeným spôsobom oznámiť zmeny funkcionalít, poruchy zariadení, podozrenia na bezpečnostný incident alebo incidenty súvisiace s posielaním osobných údajov alebo citlivých informácií.

Vstupné zaškolenie používateľov na používanie informačného systému a bezpečnosť prístupu sa zabezpečuje podľa pravidiel VŠZaSP sv. Alžbety.

Pravidelné preškolenie používateľov v oblasti používania informačného systému, ochrany osobných údajov a bezpečnosti prístupu sa zabezpečuje podľa pravidiel VŠZaSP sv. Alžbety.

8.4.6 Kamerové systémy

VŠZaSP sv. Alžbety môže používať kamerové systémy na monitorovanie svojich vnútorných priestorov, vonkajších priestorov alebo prístupových komunikácií z dôvodu ochrany majetku, bezpečnosti osôb a ochrany priestorov vysokej školy.

Všetky priestory, ktoré sú monitorované kamerovým systémom, musia byť označené na viditeľnom mieste informáciou o monitorovaní, ktorú určuje osobitný predpis pre kamerové systémy.

Záznamy z kamerového systému sa ukladajú na určené pamäťové médium alebo do určeného systému a uchovávajú sa len počas nevyhnutnej doby v súlade s právnymi predpismi.

Záznamy z kamerového systému sa uchovávajú počas retenčnej lehoty určenej VŠZaSP sv. Alžbety; po jej uplynutí sa priebežne mažú, v zmysle osobitného interného predpisu pre kamerové systémy.

Prístup k živému náhľadu a archívnym záznamom kamerového systému majú len oprávnené osoby.

Kamerové systémy nesmú byť používané na neoprávnené monitorovanie osôb pri pracovnej činnosti, príchode a odchode do práce alebo pri ostatných bežných činnostiach na pracovisku, ak na to neexistuje osobitný právny dôvod a splnené zákonné podmienky.

8.4.7 Bezpečnostné opatrenia pri používaní technických a programových prostriedkov IT

Na ochranu technických a programových prostriedkov IT sa používajú bezpečnostné opatrenia a systémy podľa technických možností a potrieb vysokej školy.

Zamestnancom, študentom a iným používateľom sa zakazuje vyraďovať z činnosti, narúšať, prekonávať alebo obchádzať ktorékoľvek bezpečnostné zariadenie alebo bezpečnostný systém.

Súbory, ktoré obsahujú dôverné údaje, osobné údaje alebo iné citlivé informácie, musia byť pri prenose prostredníctvom internetu chránené primeraným bezpečnostným opatrením, najmä šifrovaním, ak to povaha údajov a technické možnosti vyžadujú.

Pri opustení pracoviska, aj krátkodobom, je používateľ povinný vylúčiť akúkoľvek možnosť neoprávneného prístupu tretích osôb k údajom a manipulácie s nimi.

Pokus o narušenie bezpečnosti IT alebo ochrany dát je používateľ povinný bezodkladne oznámiť určeným spôsobom.

8.5. Pravidlá autentifikácie, hesiel a prístupových práv

V tejto časti sú upravené pravidlá autentifikácie používateľov, používania prihlasovacích mien, hesiel, viacfaktorového overovania, prideľovania prístupových údajov a zmeny, zrušenia alebo blokovania prístupových práv k informačným systémom a službám VŠZaSP sv. Alžbety.

Každý používateľ IT má pridelené svoje prihlasovacie meno a heslo, ktoré musí zachovať v tajnosti. Tieto prihlasovacie údaje, pomáhajú stanoviť osobnú zodpovednosť používateľa za činnosti vykonané v informačných systémoch vysokej školy.

Zakazuje sa spoločné používanie prihlasovacích mien a hesiel viacerými používateľmi IT.

Používateľ IT je plne zodpovedný za svoje heslo. Heslo nesmie byť ľahko uhádnuteľné alebo odvoditeľné. V prípade zabudnutia hesla sa nové heslo nastaví určeným spôsobom po overení totožnosti používateľa.

V prípade podozrenia na prezradenie hesla je používateľ povinný heslo bezodkladne zmeniť a postupovať určeným spôsobom.

Je zakázané poskytovať tretím osobám informácie o používateľoch, ich oprávneniach, heslách alebo autentifikačných prostriedkoch, ak by mohli byť zneužité na neoprávnený prístup.

8.5.1 Heslá administrátorov

Administrátorské heslo musí spĺňať požiadavky na zložitosť a bezpečnosť určené pre daný systém, v dĺžke minimálne 16 znakov, ak to systém umožňuje.

Pravidlá zmeny administrátorských hesiel sa určujú podľa technických možností príslušného systému. Opätovné používanie administrátorských hesiel sa obmedzuje podľa technických možností príslušného systému.

Administrátorský účet sa pri opakovanom nesprávnom zadaní hesla blokuje podľa bezpečnostných pravidiel a technických možností príslušného systému.

Bezpečnostná kópia aktuálneho hesla administrátora musí byť uložená určeným spôsobom, ktorý zabezpečí ochranu pred neoprávneným prístupom a zároveň umožní núdzový prístup v odôvodnených prípadoch. Môže byť uložená v obálkovom režime, v elektronickom trezore hesiel alebo v inom schválenom systéme správy privilegovaných prístupov. Konkrétny spôsob uloženia bezpečnostnej kópie hesla administrátora určí škola podľa svojich technických a organizačných možností.

- Obálkový režim znamená uloženie bezpečnostnej kópie aktuálneho hesla administrátora v zalepenej a zapečatenej obálke u osoby určenej školou.
- Elektronický trezor hesiel znamená systém alebo aplikáciu určenú na bezpečné uloženie a správu hesiel, prístupových údajov alebo privilegovaných prístupov.
- Iný schválený systém správy privilegovaných prístupov znamená technické alebo organizačné riešenie určené VŠZaSP sv. Alžbety na bezpečné uchovávanie, kontrolu, používanie alebo núdzové sprístupnenie administrátorských hesiel.

8.5.2 Heslá používateľov s privilegovaným prístupom

Používateľmi s privilegovaným prístupom sú IT roly alebo iné osoby, ktoré majú administrátorské alebo rozšírené oprávnenia k informačným systémom, technickým alebo programovým prostriedkom vysokej školy. Privilegovaný prístup sa prideľuje iba v rozsahu nevyhnutnom na plnenie pracovných, zmluvných alebo poverených úloh používateľa.

Používateľ s privilegovaným prístupom nesmie používať privilegovaný účet na bežnú používateľskú činnosť, ak má na tento účel pridelený samostatný bežný účet.

Heslá používateľov s privilegovaným prístupom sa menia podľa požiadaviek určených pre príslušný systém. Administrátorské heslo musí spĺňať požiadavky na zložitosť a bezpečnosť určené pre daný systém, v dĺžke minimálne 16 znakov, ak to systém umožňuje.

Opätovné používanie hesiel používateľov s privilegovaným prístupom sa obmedzuje podľa technických možností príslušného systému.

Účet používateľa s privilegovaným prístupom sa pri opakovanom nesprávnom zadaní hesla blokuje podľa pravidiel a technických možností príslušného systému.

8.5.3 Heslá ostatných používateľov

Heslo ostatného používateľa musí mať najmenej 12 znakov, veľké písmeno, malé písmeno, číslo a špeciálny znak, ak príslušný systém nevyžaduje prísnejšie pravidlá. Musí byť nastavené tak, aby nebolo ľahko uhádnuteľné alebo odvoditeľné.

Používateľ je povinný zachovávať heslo v tajnosti a nesmie ho zapisovať, ukladať alebo sprístupňovať spôsobom, ktorý by umožnil jeho zneužitie.

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

Používateľ nesmie používať rovnaké heslo do informačných systémov VŠZaSP sv. Alžbety a do súkromných alebo externých služieb, ak by tým mohlo dôjsť k ohrozeniu bezpečnosti informačných systémov vysokej školy.

V prípade podozrenia na zneužitie, prezradenie alebo neoprávnené použitie hesla je používateľ povinný heslo bezodkladne zmeniť a oznámiť túto skutočnosť určeným spôsobom.

8.5.4 Prideľovanie adries elektronickej pošty

E-mailové adresy zamestnancov sa prideľujú pri vzniku pracovného, obdobného pracovnoprávneho, zmluvného alebo iného oprávneného vzťahu k VŠZaSP sv. Alžbety na základe schválenej požiadavky oprávnenej osoby. Oprávnenou osobou na podanie alebo schválenie požiadavky je najmä priamy nadriadený používateľa, vedúci príslušného pracoviska, personálne pracovisko alebo iná osoba určená školou.

E-mailové adresy študentov sa prideľujú pri zápise na štúdium alebo inom určenom úkone súvisiacom so vznikom študijného vzťahu podľa pravidiel školy.

E-mailové adresy VŠZaSP sv. Alžbety sa prideľujú v doméne „vssvalzbety.sk" Štandardný formát e-mailovej adresy je:

a) priezvisko@vssvalzbety.sk
b) v prípade zhodného priezviska viacerých používateľov meno.priezvisko@vssvalzbety.sk

Pri prideľovaní adries elektronickej pošty sa rozlišujú najmä osobné, funkčné, skupinové, projektové a dočasné e-mailové adresy.

Používateľ je povinný používať pridelenú e-mailovú adresu v súlade s touto smernicou, internými pravidlami VŠZaSP sv. Alžbety a účelom, na ktorý mu bola pridelená.

Po skončení oprávneného dôvodu používania elektronickej pošty sa e-mailová adresa alebo schránka spracuje podľa pravidiel vysokej školy. Požiadavka na zmenu, zablokovanie alebo zrušenie e-mailovej adresy sa oznamuje určeným spôsobom.

8.5.5 Prideľovanie prístupových údajov do informačných systémov

Prístupové údaje do informačných systémov VŠZaSP sv. Alžbety sa prideľujú používateľom na základe ich pracovného, študijného, zmluvného alebo iného oprávneného vzťahu k VŠZaSP sv. Alžbety podľa schváleného procesu a v rozsahu potrebnom na plnenie ich pracovných, študijných, zmluvných alebo iných oprávnených úloh.

Prístup do dátovej siete, informačných systémov, programov, internetu alebo elektronickej pošty sa zriaďuje určeným spôsobom. Požiadavka na zriadenie, zmenu alebo zrušenie prístupu musí byť schválená podľa pravidiel vysokej školy.

Pri zmene alebo skončení oprávneného dôvodu používania prístupu sa prístupové práva zmenia alebo zrušia podľa pravidiel vysokej školy.

Osoba zodpovedná za schválenie prístupu je priamy nadriadený zamestnanca, resp. osoba poverená dohľadom nad činnosťou konkrétnej tretej strany. V prípade študentov sadu prístupov určuje študijné oddelenie a vyučujúci v rámci rozsahu informačných aktív, ktoré študenti potrebujú na splnenie stanovených cieľov vzdelávania a výskumu.

8.5.6 Prideľovanie prístupov do Wi-Fi a VPN

Prístup do Wi-Fi siete VŠZaSP sv. Alžbety sa prideľuje zamestnancom, študentom a iným oprávneným používateľom podľa určených pravidiel.

Prístup do VPN alebo iného vzdialeného prístupu sa prideľuje len oprávneným používateľom, ktorým je takýto prístup potrebný na plnenie pracovných, študijných, zmluvných alebo iných oprávnených úloh.

Heslá alebo prístupové údaje pre vzdialený VPN prístup a Wi-Fi sieť nesmú byť zhodné s heslami na prístup do hlavných informačných systémov, ak to technické možnosti a bezpečnostné pravidlá VŠZaSP sv. Alžbety umožňujú.

Po skončení oprávneného dôvodu používania sa prístup do Wi-Fi, VPN alebo iného vzdialeného prístupu zablokuje alebo zruší podľa pravidiel školy.

8.5.7 Používanie viacfaktorového overovania (MFA)

Administrátori a používatelia s privilegovaným prístupom používajú viacfaktorové overovanie v systémoch určených školou. VŠZaSP sv. Alžbety môže určiť systémy, pri ktorých je MFA povinné aj pre ostatných používateľov.

Ako MFA metódy sa môžu používať metódy schválené školou, najmä autentifikačná aplikácia, bezpečnostný kľúč, certifikát alebo iný schválený overovací prostriedok.

Záložné MFA kódy alebo náhradné MFA zariadenie sa používajú podľa pravidiel príslušného systému.

O odobratie, resetovanie alebo zmenu MFA metódy môže používateľ požiadať iba vo vlastnom mene a jeho požiadavka musí byť hodnoverne autentifikovaná.

Zakazuje sa ukladanie MFA záložných kódov, QR kódov, seedov na nechránených úložiskách.

8.5.8 Zmena, zrušenie a blokovanie prístupových práv

Zmena, zrušenie alebo blokovanie prístupových práv sa vykonáva pri zmene alebo skončení oprávneného dôvodu používania prístupu, napríklad pracovného zaradenia, zmene študijného statusu, zmene zmluvného vzťahu, zmene rozsahu oprávnení, pri skončení pracovného pomeru, skončení štúdia,

skončení zmluvného vzťahu alebo pri inom dôvode, pre ktorý používateľ už nepotrebuje pôvodne pridelený prístup.

Potreba zmeny, zrušenia alebo blokovania prístupových práv sa oznamuje bezodkladne príslušnej IT role a vykonáva a eviduje sa určeným spôsobom.

Prístupové práva môžu byť dočasne zablokované najmä pri podozrení na zneužitie účtu, prezradenie hesla, bezpečnostný incident, porušenie tejto smernice, skončenie alebo prerušenie oprávneného dôvodu používania prístupu alebo pri nečinnosti účtu.

Po zrušení prístupových práv musí byť používateľovi znemožnený prístup k informačným systémom, údajom a službám VŠZaSP sv. Alžbety v rozsahu, v akom na tento prístup zanikol dôvod.

8.6. Ochrana osobných údajov, súkromia, zverejňovanie a manipulácia s informáciami

V tejto časti sú upravené pravidlá ochrany osobných údajov, ochrany súkromia používateľov, zverejňovania, klasifikácie, označovania, manipulácie, prenosu, zdieľania a uchovávania dokumentov a informácií spracúvaných alebo používaných v rámci systémov a služieb VŠZaSP sv. Alžbety.

VŠZaSP sv. Alžbety pri spracúvaní osobných údajov postupuje v súlade s právnymi predpismi na ochranu osobných údajov, najmä s GDPR a zákonom č. 18/2018 Z. z. o ochrane osobných údajov, ako aj s internými pravidlami školy.

8.6.1 Ochrana súkromia používateľov

VŠZaSP sv. Alžbety pri správe a používaní informačných systémov, technických prostriedkov, dátovej siete, elektronickej pošty, internetu a ďalších služieb rešpektuje právo používateľov na ochranu súkromia v rozsahu ustanovenom právnymi predpismi a internými pravidlami vysokej školy.

Používatelia berú na vedomie, že používanie systémov a služieb školy môže byť v nevyhnutnom rozsahu monitorované alebo zaznamenávané na bezpečnostné, prevádzkové, kontrolné, zákonné alebo zmluvné účely.

Monitorovanie alebo kontrola používania informačných systémov a služieb sa vykonáva len v rozsahu potrebnom na dosiahnutie určeného účelu a spôsobom, ktorý je primeraný, odôvodnený a v súlade s právnymi predpismi.

Prístup k údajom alebo záznamom, ktoré môžu súvisieť so súkromím používateľa, majú len oprávnené osoby v rozsahu potrebnom na plnenie ich pracovných, zmluvných alebo zákonných povinností.

Používateľ nesmie bez oprávnenia pristupovať k údajom, komunikácii, súborom, priečinkom, e-mailovým schránkam alebo iným informáciám iných používateľov.

8.6.2 Zverejňovanie informácií

Informácie, dokumenty, osobné údaje alebo iné údaje spracúvané alebo používané v rámci VŠZaSP sv. Alžbety sa môžu zverejňovať iba vtedy, ak na to existuje právny základ, oprávnený účel, interné oprávnenie alebo súhlas osoby oprávnenej rozhodnúť o ich zverejnení.

Zverejňovanie informácií vo verejne dostupných alebo interných komunikačných priestoroch školy sa vykonáva iba v rozsahu primeranom účelu zverejnenia.

Pri zverejňovaní osobných údajov je potrebné posúdiť najmä účel a právny základ zverejnenia, rozsah údajov, dobu zverejnenia, okruh príjemcov a riziká pre dotknuté osoby.

Zamestnanci, študenti a iní používatelia nesmú bez oprávnenia zverejňovať interné, dôverné, osobné alebo iné citlivé informácie vysokej školy.

Kontaktné údaje zamestnancov, údaje o pracoviskách, študijné informácie, rozvrhy, výsledky, fotografie, videozáznamy alebo iné informácie týkajúce sa fyzických osôb sa môžu zverejňovať iba v súlade s právnymi predpismi a internými pravidlami.

8.6.3 Spracúvanie osobných údajov v informačných systémoch

Osobné údaje sa v informačných systémoch VŠZaSP sv. Alžbety spracúvajú iba na určené, výslovne vymedzené a oprávnené účely súvisiace s činnosťou vysokej školy.

Spracúvanie osobných údajov v informačných systémoch školy môže zahŕňať najmä údaje osôb, ktoré majú alebo mali k vysokej škole študijný, pracovný, zmluvný, projektový, odborný alebo iný oprávnený vzťah.

Prístup k osobným údajom v informačných systémoch sa prideľuje iba oprávneným osobám a len v rozsahu potrebnom na plnenie ich pracovných, študijných, zmluvných alebo iných oprávnených úloh.

Používatelia, ktorí spracúvajú osobné údaje v informačných systémoch, sú povinní chrániť ich pred neoprávneným prístupom, sprístupnením, zmenou, stratou, zničením, poškodením alebo zneužitím.

Osobné údaje sa môžu kopírovať, exportovať, prenášať, ukladať mimo informačného systému alebo poskytovať ďalším osobám iba v rozsahu povolenom právnymi predpismi, internými pravidlami alebo rozhodnutím oprávnenej osoby VŠZaSP sv. Alžbety.

Ak informačný systém umožňuje vedenie auditných záznamov o prístupe k osobným údajom, tieto záznamy sa uchovávajú a vyhodnocujú určeným spôsobom.

8.6.4 Klasifikácia, označovanie a manipulácia s dokumentmi a informáciami

Dokumenty a informácie používané alebo spracúvané v rámci VŠZaSP sv. Alžbety sa chránia podľa ich obsahu, významu a možných následkov ich neoprávneného sprístupnenia, zmeny, straty alebo zneužitia.

Klasifikácia informácií musí byť vykonaná na základe významnosti, funkcie a účelu informácií s ohľadom na dôvernosť, integritu, dostupnosť. Informácia sa klasifikuje bez ohľadu na jej formát, spôsob uloženia, systémy, aplikácie alebo nástroje, v ktorých sa nachádza alebo prostredníctvom ktorých sa informácia spracúva alebo prostredníctvom ktorých je prenášaná.

Z hľadiska:

- **dôvernosti** sú klasifikačné stupne informačných aktív definované ako verejné, interné, chránené, prísne chránené, pričom platí pravidlo, ak nie je informačné aktívum explicitne klasifikované je považované za interné,
- **integrity** sú klasifikačné stupne informačných aktív definované ako nízka, stredná, vysoká,
- **dostupnosti** sú klasifikačné stupne informačných aktív definované ako nízka, stredná, vysoká.

Každá klasifikovaná informácia musí mať pridelený jeden klasifikačný stupeň dôvernosti, jeden klasifikačný stupeň integrity a jeden klasifikačný stupeň dostupnosti.

Informácie, nastavenia, postupy, smernice a ostatné úkony ohľadom riadenia aktív sa klasifikujú rovnakým alebo vyšším klasifikačným stupňom, akým sú označené informačné aktíva, ktorých riadenie opisujú.

Pre každú kategóriu citlivosti informácií musia byť definované zodpovedajúce bezpečnostné opatrenia na ich ochranu.

Používatelia sú povinní s dokumentmi a informáciami zaobchádzať tak, aby nedošlo k ich neoprávnenému sprístupneniu, strate, poškodeniu alebo zneužitiu.

Klasifikované informácie sa ukladajú, prenášajú, zdieľajú, archivujú a likvidujú iba spôsobom určeným VŠZaSP sv. Alžbety alebo v súlade s právnymi predpismi.

8.6.5 Prenos, zdieľanie a uchovávanie klasifikovaných informácií

Klasifikované informácie sa môžu prenášať, zdieľať alebo uchovávať iba spôsobom zodpovedajúcim ich povahe, účelu spracúvania a požiadavkám na ich ochranu.

Pri prenose alebo zdieľaní informácií je používateľ povinný použiť primerané bezpečnostné opatrenia, najmä overenie príjemcu, zabezpečený prenos, chránený prístup alebo šifrovanie, ak to povaha údajov vyžaduje.

Používateľ nesmie odosielať klasifikované informácie prostredníctvom neschválených alebo nezabezpečených kanálov a pred odoslaním je povinný overiť správnosť adresáta a primeranosť rozsahu poskytovaných informácií.

8.6.6 Poskytovanie údajov tretím stranám

Údaje, dokumenty, osobné údaje, dôverné informácie alebo iné citlivé informácie VŠZaSP sv. Alžbety sa môžu poskytovať tretím stranám iba vtedy, ak na to existuje právny základ, zmluvný základ,

oprávnený účel, súhlas oprávnenej osoby alebo iný dôvod ustanovený právnymi predpismi alebo internými pravidlami školy.

Za tretie strany sa na účely tejto smernice považujú osoby alebo organizácie mimo VŠZaSP sv. Alžbety, najmä dodávatelia, servisné organizácie, zmluvní partneri, orgány verejnej moci, partnerské pracoviská a externí spolupracovníci.

Pred poskytnutím údajov tretej strane je potrebné posúdiť najmä účel, právny alebo zmluvný základ, rozsah údajov, oprávnenosť príjemcu, bezpečnostné opatrenia pri prenose, povinnosť mlčanlivosti, zmluvnú ochranu údajov a potrebu sprostredkovateľskej zmluvy.

Ak tretia strana spracúva osobné údaje v mene VŠZaSP sv. Alžbety, musí byť právny vzťah s touto treťou stranou upravený v súlade s právnymi predpismi na ochranu osobných údajov.

Tretím stranám možno poskytnúť iba také údaje a v takom rozsahu, ktorý je nevyhnutný na splnenie určeného účelu.

Poskytnutie údajov tretej strane sa podľa povahy údajov a interných pravidiel školy eviduje alebo dokumentuje.

Používateľ nesmie bez oprávnenia poskytovať tretím stranám údaje o informačných systémoch, technickej infraštruktúre, bezpečnostných opatreniach, prístupových právach, používateľoch alebo iných interných skutočnostiach VŠZaSP sv. Alžbety.

8.7. Účtovateľnosť, monitorovanie a auditné záznamy

V tejto časti sú upravené pravidlá účtovateľnosti činností používateľov, monitorovania používania systémov a služieb VŠZaSP sv. Alžbety, ako aj pravidlá vytvárania, uchovávania, vyhodnocovania a sprístupňovania auditných záznamov.

Účelom účtovateľnosti, monitorovania a auditných záznamov je zabezpečiť možnosť spätne preukázať činnosti používateľov, správcov a systémov, chrániť informačné systémy a údaje VŠZaSP sv. Alžbety, zisťovať a riešiť bezpečnostné incidenty, predchádzať neoprávnenému prístupu a zabezpečiť riadnu prevádzku informačného systému.

8.7.1 Účtovateľnosť činností používateľov

Každý používateľ informačného systému VŠZaSP sv. Alžbety musí používať pridelené prihlasovacie meno, heslo alebo iný autentifikačný prostriedok tak, aby bolo možné jeho činnosť v informačnom systéme primerane identifikovať a spätne priradiť ku konkrétnemu používateľovi.

Používateľ nesmie používať prihlasovacie meno, heslo, účet alebo iný autentifikačný prostriedok iného používateľa.

Používateľ nesmie umožniť inej osobe používanie svojho prihlasovacieho mena, hesla, účtu alebo iného autentifikačného prostriedku.

Používanie spoločných alebo zdieľaných používateľských účtov je zakázané, ak ich použitie nie je výslovne schválené VŠZaSP sv. Alžbety a technicky alebo organizačne zabezpečené tak, aby bolo možné určiť zodpovednosť za vykonané činnosti.

Činnosti používateľov v systémoch a službách školy môžu byť zaznamenávané v rozsahu potrebnom na zabezpečenie bezpečnosti, prevádzky, kontroly oprávnenosti prístupu a riešenia bezpečnostných incidentov.

8.7.2 Auditné záznamy

Auditné záznamy sú záznamy vytvárané informačnými systémami, technickými prostriedkami, aplikáciami, sieťovými zariadeniami alebo bezpečnostnými nástrojmi, ktoré zachytávajú vybrané činnosti používateľov, správcov, systémov alebo zariadení.

Auditné záznamy môžu obsahovať najmä identifikáciu používateľa, systému alebo zariadenia, dátum a čas udalosti, druh a výsledok činnosti, technickú identifikáciu zariadenia, záznamy o prihlásení, zmenách účtov a prístupových práv, administrátorských zásahoch, bezpečnostných udalostiach alebo podozreniach na incident.

Auditné záznamy sa vytvárajú pri systémoch a službách školy v rozsahu ich technických možností a nastavených pravidiel a musia byť chránené pred neoprávneným prístupom, zmenou, zmazaním, stratou alebo zneužitím.

8.7.2.1 Uchovávanie a vyhodnocovanie auditných záznamov

Auditné záznamy sa uchovávajú počas doby určenej školou, právnymi predpismi, bezpečnostnými požiadavkami alebo technickými možnosťami príslušného informačného systému.

Doba uchovávania auditných záznamov musí byť primeraná účelu ich spracúvania, najmä potrebe zabezpečenia bezpečnosti informačných systémov, riešenia bezpečnostných incidentov, kontroly oprávnenosti prístupu a ochrany práv a oprávnených záujmov VŠZaSP sv. Alžbety.

Auditné záznamy sa vyhodnocujú najmä pri podozrení na neoprávnený prístup, zneužitie účtu, porušenie tejto smernice, bezpečnostný incident, technickú poruchu alebo výpadok systému, kontrole činnosti administrátora alebo privilegovaného používateľa, alebo na základe požiadavky oprávneného orgánu alebo vedenia vysokej školy. Záznamy monitorujú a vyhodnocujú určené IT roly alebo iné oprávnené osoby v rozsahu svojej pôsobnosti.

Ak auditné záznamy obsahujú osobné údaje alebo údaje súvisiace so súkromím používateľov, ich uchovávanie a vyhodnocovanie sa vykonáva v súlade s právnymi predpismi na ochranu osobných údajov a internými pravidlami.

8.7.2.2 Prístup k auditným záznamom

Prístup k auditným záznamom majú len oprávnené osoby určené VŠZaSP sv. Alžbety, a to iba v rozsahu potrebnom na výkon ich pracovných, zmluvných alebo zákonných povinností.

Auditné záznamy sa nesmú sprístupňovať neoprávneným osobám ani používať na iný účel, než na ktorý boli vytvorené alebo spracúvané; musia byť chránené pred neoprávneným prístupom, zmenou alebo vymazaním.

Ak sa auditné záznamy poskytujú tretej strane, poskytujú sa len v nevyhnutnom rozsahu a za podmienok ustanovených právnymi predpismi, zmluvou alebo internými pravidlami.

8.8. Zálohovanie, obnova a kontinuita činnosti informačného systému

V tejto časti sú upravené pravidlá zálohovania údajov, obnovy údajov zo záloh, uchovávania záložných médií, likvidácie archívnych médií a zabezpečenia kontinuity činnosti informačného systému VŠZaSP sv. Alžbety.

Cieľom zálohovania je zabezpečiť dostupnosť, obnoviteľnosť a ochranu údajov spracúvaných v informačných systémoch VŠZaSP sv. Alžbety v prípade technickej poruchy, havárie, bezpečnostného incidentu, ľudskej chyby, straty, poškodenia alebo neoprávnenej zmeny údajov.

8.8.1 Zálohovanie údajov serverov a informačných systémov

Údaje serverov, informačných systémov, databáz, aplikácií, konfiguračných súborov a ďalších dôležitých technických alebo programových prostriedkov VŠZaSP sv. Alžbety sa zálohujú v rozsahu určenom vysokou školou. Zálohovanie sa vykonáva podľa významu, klasifikácie a dôležitosti údajov, technických možností príslušného systému a pravidiel školy.

Za vykonávanie zálohovania zodpovedá príslušná IT rola podľa rozsahu pridelených oprávnení a zodpovedností. O zálohovaní sa vedie evidencia v rozsahu určenom školou.

Zálohovanie sa vykonáva v intervaloch určených podľa povahy systému, významu údajov a požiadaviek na obnovu prevádzky.

Zálohovanie sa vykonáva v rozsahu potrebnom na obnovu prevádzky informačných systémov a ochranu údajov, najmä podľa významu systému, citlivosti údajov a požiadaviek na obnovu.

Zálohy musia byť chránené pred neoprávneným prístupom, stratou, poškodením, zničením, neoprávnenou zmenou alebo zneužitím.

Ak zálohy obsahujú osobné údaje, dôverné údaje alebo iné klasifikované informácie, musia byť chránené primeranými bezpečnostnými opatreniami, najmä obmedzením prístupu, šifrovaním alebo uložením v zabezpečenom prostredí podľa technických možností a povahy údajov.

8.8.2 Operatívna záloha

Operatívna záloha je záloha vytváraná na účely rýchlej obnovy údajov alebo systému v prípade bežnej poruchy, neúmyselného vymazania, poškodenia údajov alebo inej prevádzkovej udalosti.

Operatívne zálohy sa vytvárajú v pravidelných intervaloch podľa dôležitosti systému a údajov, ktoré sú predmetom zálohovania. Operatívna záloha môže byť vytváraná v pravidelnom intervale, pri významnej zmene alebo pred aktualizáciou, zásahom alebo údržbou systému.

Operatívne zálohy sa uchovávajú počas doby určenej VŠZaSP sv. Alžbety podľa technických možností, významu údajov a potreby obnovy.

Prístup k operatívnym zálohám majú len osoby oprávnené vykonávať zálohovanie, obnovu údajov alebo správu príslušného informačného systému.

Použiteľnosť operatívnych záloh sa primerane overuje, najmä testovaním obnovy alebo kontrolou úspešnosti zálohovania.

8.8.3 Bezpečnostná záloha

Bezpečnostná záloha je záloha vytváraná na účely ochrany údajov a obnovy prevádzky v prípade závažnej poruchy, havárie, bezpečnostného incidentu, útoku, poškodenia systému alebo inej mimoriadnej udalosti. Prístup k bezpečnostným zálohám je obmedzený na oprávnené osoby a musí byť evidovaný alebo inak kontrolovateľný podľa technických možností školy.

Bezpečnostná záloha sa uchováva oddelene od prevádzkového prostredia alebo spôsobom, ktorý primerane znižuje riziko jej poškodenia, zničenia, neoprávnenej zmeny alebo zneužitia.

Bezpečnostná záloha môže byť uložená najmä na záložnom serveri, externom médiu, zabezpečenom úložisku, v oddelenej lokalite, cloudovej službe alebo inom technicky a bezpečnostne vhodnom prostredí.

Bezpečnostné zálohy obsahujúce osobné údaje, dôverné údaje alebo iné citlivé informácie musia byť chránené primeranými technickými a organizačnými opatreniami.

Bezpečnostné zálohy sa uchovávajú počas doby určenej podľa významu systému, požiadaviek na obnovu prevádzky, právnych požiadaviek a interných pravidiel.

8.8.4 Obnova údajov zo záloh

Obnova údajov zo záloh sa vykonáva v odôvodnených prípadoch, najmä pri strate, poškodení, neúmyselnom vymazaní údajov, technickej poruche, bezpečnostnom incidente alebo havarijnom stave.

Obnovu údajov zo záloh vykonáva príslušná IT rola podľa rozsahu pridelených oprávnení.

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

Ak sa obnova údajov vykonáva v súvislosti s bezpečnostným incidentom, musí sa postupovať tak, aby nedošlo k zmareniu vyšetrovania incidentu alebo strate dôležitých auditných záznamov.

O obnove údajov zo záloh sa vedie záznam v rozsahu určenom VŠZaSP sv. Alžbety, najmä o dátume a čase obnovy, dôvode obnovy, rozsahu obnovovaných údajov, použitej zálohe, osobe vykonávajúcej obnovu, osobe požadujúcej alebo schvaľujúcej obnovu a výsledku obnovy.

Funkčnosť obnovených údajov alebo systému sa po obnove primerane overí.

8.8.5 Likvidácia archívnych médií

Archívne, záložné, pamäťové a iné nosiče údajov, ktoré sa už nepoužívajú alebo ktorým uplynula určená doba uchovávania, sa likvidujú spôsobom, ktorý zabráni neoprávnenému prístupu k údajom, ich obnoveniu alebo zneužitiu.

Likvidácia médií obsahujúcich osobné údaje, dôverné údaje alebo iné citlivé informácie sa vykonáva spôsobom, ktorý znemožní obnovu údajov, najmä bezpečným vymazaním, kryptografickým znehodnotením, fyzickým zničením alebo odovzdaním oprávnenej servisnej alebo likvidačnej spoločnosti.

Pred vyradením alebo odovzdaním zariadenia na servis, opravu, reklamáciu, likvidáciu alebo iné použitie je potrebné zabezpečiť odstránenie alebo primeranú ochranu údajov uložených na médiu.

O likvidácii archívnych alebo záložných médií obsahujúcich osobné, dôverné alebo iné klasifikované údaje sa vedie záznam. Záznam môže obsahovať najmä identifikáciu a typ média, dátum a spôsob likvidácie, osobu vykonávajúcu alebo schvaľujúcu likvidáciu a potvrdenie dodávateľa alebo likvidačnej spoločnosti, ak bola likvidácia vykonaná externe.

8.8.6 Plán kontinuity činnosti informačného systému

VŠZaSP sv. Alžbety zabezpečuje primeranú kontinuitu činnosti informačného systému tak, aby v prípade poruchy, havárie, bezpečnostného incidentu, výpadku služby alebo inej mimoriadnej udalosti bolo možné obnoviť činnosť dôležitých informačných systémov a služieb v primeranom čase.

Pre kritické informačné systémy sa osobitným procesom za účasti garantu procesu, IT role a iných určených pracovných rolí určujú hodnoty RPO a RTO, teda maximálna prípustná strata údajov a maximálny prípustný čas obnovy systému alebo služby.

Plán kontinuity činnosti informačného systému sa preskúmava a aktualizuje podľa zmien informačných systémov, technickej infraštruktúry, organizačnej štruktúry, dodávateľov alebo bezpečnostných požiadaviek. Použiteľnosť plánu, záloh a postupov obnovy sa primerane testuje, najmä pri kritických informačných systémoch alebo po významných zmenách technickej infraštruktúry.

Ak plán kontinuity činnosti informačného systému nie je vypracovaný ako samostatný dokument, základné postupy obnovy a zodpovednosti sa určia v prevádzkovej dokumentácii informačných systémov alebo v dokumentácii správcov systémov.

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

8.9. Ochrana údajov pri dodávke, inštalácii, údržbe a servise IT

V tejto časti sú upravené pravidlá ochrany údajov pri dodávke, inštalácii, údržbe, oprave a servise technických a programových prostriedkov VŠZaSP sv. Alžbety, ako aj pravidlá prístupu dodávateľov, servisných organizácií a iných tretích strán k systémom, službám a údajom vysokej školy.

Cieľom týchto pravidiel je zabezpečiť, aby pri dodávateľských, servisných alebo údržbových činnostiach nedošlo k neoprávnenému prístupu k údajom, strate údajov, poškodeniu údajov, zneužitiu prístupových oprávnení alebo narušeniu bezpečnosti informačného systému vysokej školy.

8.9.1 Dodávka, inštalácia, údržba a servis technických a programových prostriedkov

Dodávka, inštalácia, údržba, oprava alebo servis technických a programových prostriedkov VŠZaSP sv. Alžbety sa vykonáva iba na základe schváleného alebo inak preukázateľného postupu. Tieto činnosti môže vykonávať iba oprávnená IT rola alebo iná poverená osoba.

Pred servisom, opravou, reklamáciou alebo odovzdaním zariadenia tretej strane sa podľa technických možností odstránia alebo zabezpečia osobné údaje, dôverné údaje, prístupové údaje a iné citlivé informácie.

Ak pri dodávke, inštalácii, údržbe, oprave alebo servise vzniká dodávateľovi prístup k systémom, zariadeniam, údajom alebo priestorom školy, zásah sa vykonáva za podmienok určených vysokou školou, najmä v nevyhnutnom rozsahu, na nevyhnutný čas a podľa potreby pod dohľadom oprávnenej osoby.

O vykonanom zásahu sa podľa povahy zásahu vedie primeraný záznam.

8.9.2 Prístup dodávateľov k informačným systémom a údajom

Dodávateľom a iným tretím stranám možno poskytnúť prístup k systémom, zariadeniam, službám alebo údajom vysokej školy iba vtedy, ak je takýto prístup nevyhnutný na plnenie zmluvných, servisných, prevádzkových alebo iných oprávnených úloh. Prístup dodávateľa k systémom a údajom môže byť umožnený najmä fyzicky na pracovisku, vzdialeným prístupom, servisným alebo administrátorským účtom, dočasným prístupovým oprávnením alebo iným spôsobom určeným VŠZaSP sv. Alžbety. Pri vzdialenom prístupe dodávateľa sa používajú primerané bezpečnostné opatrenia, najmä autentifikácia, obmedzenie prístupu, časové obmedzenie, monitorovanie alebo záznam prístupu, ak to technické možnosti umožňujú.

Prístup dodávateľa sa poskytuje iba v rozsahu nevyhnutnom na splnenie konkrétneho účelu a na dobu nevyhnutnú na vykonanie príslušnej činnosti.

Prístup dodávateľa musí byť schválený oprávnenou osobou a podľa povahy prístupu evidovaný alebo inak preukázateľne doložený.

Ak je to technicky možné a primerané, dodávateľovi sa prideľuje samostatný používateľský alebo administrátorský účet; používanie spoločných účtov sa nepripúšťa, ak VŠZaSP sv. Alžbety neurčí výnimočný a kontrolovaný postup.

Po skončení činnosti dodávateľa alebo po zániku dôvodu prístupu sa prístupové oprávnenia dodávateľa zrušia, zablokujú alebo primerane obmedzia.

Dodávateľ nesmie bez výslovného oprávnenia VŠZaSP sv. Alžbety kopírovať alebo prenášať údaje mimo určeného prostredia, poskytovať údaje ďalším osobám, vytvárať používateľské alebo administrátorské účty, meniť bezpečnostné nastavenia, pripájať ďalšie zariadenia alebo systémy ani používať údaje na iný účel, než na ktorý mu bol prístup udelený.

Prístup dodávateľa sa podľa povahy systému, rozsahu oprávnení a technických možností monitoruje alebo spätne kontroluje.

8.9.3 Mlčanlivosť a zmluvné povinnosti dodávateľov

Dodávatelia a iné tretie strany, ktoré majú alebo môžu mať prístup k systémom, zariadeniam, službám, osobným údajom, dôverným údajom alebo iným citlivým informáciám VŠZaSP sv. Alžbety, sú povinní zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvedia pri plnení svojich činností.

Povinnosť mlčanlivosti trvá počas trvania zmluvného alebo iného právneho vzťahu s VŠZaSP sv. Alžbety aj po jeho skončení.

Povinnosti dodávateľa v oblasti ochrany údajov a informačnej bezpečnosti musia byť primerane upravené v zmluve, objednávke, poverení, dohode o mlčanlivosti, sprostredkovateľskej zmluve alebo inom právnom dokumente.

Ak dodávateľ spracúva osobné údaje v mene VŠZaSP sv. Alžbety, musí byť s ním uzatvorená sprostredkovateľská zmluva, poverenie alebo iný právny akt podľa právnych predpisov na ochranu osobných údajov.

Zmluvné povinnosti dodávateľa môžu zahŕňať najmä mlčanlivosť, ochranu údajov pred neoprávneným prístupom, používanie prístupu iba na dohodnutý účel, zákaz využívania údajov na vlastné účely, zákaz neoprávneného odovzdávania údajov ďalším osobám, hlásenie bezpečnostných incidentov, spoluprácu pri ich riešení, vrátenie alebo likvidáciu údajov po skončení zmluvy, umožnenie kontroly alebo auditu v primeranom rozsahu a dodržiavanie tejto smernice alebo relevantných bezpečnostných pravidiel vysokej školy.

Dodávateľ je povinný bezodkladne oznámiť VŠZaSP sv. Alžbety akékoľvek podozrenie na neoprávnený prístup, únik údajov, stratu údajov, bezpečnostný incident alebo inú udalosť, ktorá môže ohroziť bezpečnosť informačných systémov alebo údajov VŠZaSP sv. Alžbety.

VŠZaSP sv. Alžbety môže obmedziť, pozastaviť alebo zrušiť prístup dodávateľa k systémom, zariadeniam, službám alebo údajom, ak pominul dôvod prístupu alebo ak dodávateľ poruší bezpečnostné, zmluvné alebo zákonné povinnosti.

8.10. Bezpečnostné incidenty, zodpovednosť za porušenie smernice a postihy

V tejto časti sú upravené pravidlá oznamovania, evidencie, riešenia a vyhodnocovania bezpečnostných incidentov, mimoriadnych udalostí a porušení tejto smernice, ako aj pravidlá zodpovednosti používateľov a tretích strán za porušenie pravidiel bezpečnosti informačného systému.

Za bezpečnostný incident sa na účely tejto smernice považuje najmä udalosť alebo podozrenie na udalosť, ktorá môže ohroziť dôvernosť, integritu alebo dostupnosť informačného systému, údajov alebo služieb vysokej školy. Môže ním byť najmä neoprávnený prístup, zneužitie prihlasovacích údajov, strata, krádež alebo zneužitie zariadenia IT, výskyt škodlivého softvéru, phishingový alebo iný podvodný útok, neoprávnené sprístupnenie, zmena, strata alebo zničenie údajov, výpadok alebo narušenie dostupnosti systému alebo služby, porušenie pravidiel používania IT prostriedkov, porušenie ochrany osobných údajov alebo iná udalosť ohrozujúca bezpečnosť informačného systému školy.

8.10.1 Technické prostriedky a nástroje pre predchádzanie kybernetickým bezpečnostným incidentom

VŠZaSP sv. Alžbety v primeranom rozsahu využíva alebo postupne zavádza technické a organizačné opatrenia na monitorovanie, vyhodnocovanie a riešenie bezpečnostných udalostí a incidentov v informačných systémoch a dátových sieťach školy.

Tieto opatrenia slúžia na monitorovanie a vyhodnocovanie relevantných udalostí v sieťach a informačných systémoch, ako aj na včasnú identifikáciu podozrivých alebo neštandardných aktivít, ktoré môžu nasvedčovať bezpečnostnému incidentu. Zároveň umožňujú získavanie a uchovávanie primeraných informácií potrebných na posúdenie a riešenie bezpečnostných incidentov. Poznatky získané z bezpečnostných udalostí a incidentov sa vyhodnocujú s cieľom prijať primerané nápravné alebo preventívne opatrenia.

Proces detekcie bezpečnostných incidentov je v podmienkach VŠZaSP sv. Alžbety podporovaný bezpečnostným a prevádzkovým monitoringom v rozsahu dostupných technických možností, používaných informačných systémov, sieťovej infraštruktúry a zmluvne zabezpečených služieb.

Monitoring môže zahŕňať najmä sledovanie dostupnosti a funkčnosti vybraných informačných systémov, serverov, sieťových prvkov, koncových zariadení, bezpečnostných prvkov, elektronickej pošty, prístupov používateľov a auditných alebo prevádzkových záznamov. Získané udalosti a záznamy sa primerane analyzujú a vyhodnocujú s cieľom identifikovať neštandardné správanie, technické poruchy, zraniteľnosti, podozrivé aktivity alebo bezpečnostné incidenty.

Ak sa pri monitoringu alebo vyhodnocovaní udalostí zistí bezpečnostný incident alebo dôvodné podozrenie na bezpečnostný incident, postupuje sa podľa pravidiel oznamovania, evidencie, prešetrovania a riešenia bezpečnostných incidentov uvedených v časti 8.10 tejto smernice.

VŠZaSP sv. Alžbety môže na účely prevencie, detekcie a riešenia bezpečnostných incidentov využívať najmä tieto technické alebo organizačné opatrenia:

- antivírusovú alebo antimalvérovú ochranu koncových zariadení a serverov,
- bezpečnostné prvky dátovej siete, najmä firewall, smerovače, prepínače, prístupové body a ich konfiguračné pravidlá,
- zaznamenávanie a uchovávanie vybraných prevádzkových a bezpečnostných udalostí v rozsahu primeranom technickým možnostiam školy,
- monitorovanie dostupnosti a funkčnosti vybraných informačných systémov, serverov, sieťových prvkov alebo služieb,
- nástroje na správu, aktualizáciu a kontrolu technických a programových prostriedkov,
- nástroje alebo služby externých dodávateľov, ak sú využívané pri správe, prevádzke alebo ochrane informačných systémov školy.

Ak sú na vybraných systémoch alebo službách dostupné pokročilé bezpečnostné funkcionality, napríklad centrálne logovanie, rozšírená detekcia hrozieb, korelácia udalostí alebo automatizované upozornenia, VŠZaSP sv. Alžbety ich využíva v rozsahu primeranom významu daného systému, dostupným technickým možnostiam a rizikám spojeným s jeho prevádzkou.

Technické a organizačné opatrenia v oblasti monitorovania, detekcie a riešenia bezpečnostných incidentov sa priebežne rozvíjajú podľa potrieb školy, dostupných zdrojov, technického stavu infraštruktúry a vyhodnotených bezpečnostných rizík.

8.10.2 Oznamovanie bezpečnostných incidentov

Používateľ vrátane zamestnanca, študenta, externej osoby, dodávateľa alebo tretej strany v rozsahu podľa tejto smernice, ktorý zistí bezpečnostný incident alebo má podozrenie na bezpečnostný incident týkajúci sa systémov, zariadení, údajov alebo služieb školy, je povinný ho bezodkladne oznámiť.

Za dôvod na oznámenie sa považuje aj podozrenie na bezpečnostný incident, detegovaný pokus o narušenie bezpečnosti, zistená bezpečnostná slabina, neštandardné správanie informačného systému alebo porucha IKT prostriedku, ktorá môže mať vplyv na bezpečnosť, dostupnosť, integritu alebo dôvernosť informačných systémov, údajov alebo služieb VŠZaSP sv. Alžbety.

VŠZaSP sv. Alžbety určuje jednotné kontaktné miesto alebo kontaktné osoby na prijímanie hlásení bezpečnostných incidentov, podozrení, bezpečnostných slabín a porúch IKT prostriedkov. Bezpečnostný incident sa oznamuje zodpovednej IT roli, poverenej osobe pre informačnú a kybernetickú bezpečnosť alebo priamemu nadriadenému. Kontaktné údaje a dostupné komunikačné kanály na hlásenie bezpečnostných incidentov sú uvedené v prílohe č. 9.2 tejto smernice.

Používateľ nie je povinný sám posudzovať, či ide o potvrdený bezpečnostný incident; oznamuje sa aj podozrenie na incident. Príklady udalostí, ktoré môžu predstavovať bezpečnostný incident alebo dôvodné podozrenie na bezpečnostný incident, sú uvedené v prílohe č. 9.3 tejto smernice.

Oznamovateľ bezpečnostného incidentu uvedie najmä svoje identifikačné a kontaktné údaje, čas zistenia, dotknutý systém alebo miesto, stručný opis incidentu, informáciu o možnom dotknutí osobných alebo dôverných údajov, vykonané bezprostredné opatrenia a dostupné podklady.

Používateľ je povinný podľa svojich možností vykonať také primerané kroky, aby zabránil ďalšiemu šíreniu incidentu, zhoršeniu stavu alebo vzniku ďalšej škody, avšak iba v rozsahu, v ktorom tým nespôsobí väčšiu škodu alebo neznehodnotí dôkazy potrebné na posúdenie incidentu.

Používateľ nesmie bezpečnostný incident zamlčať, zatajiť, oneskorene oznámiť alebo vykonať neodborný zásah, ktorý by mohol sťažiť jeho vyšetrenie, odstránenie alebo zdokumentovanie. Používateľ najmä nemaže podozrivé e-maily, súbory, správy, logy alebo iné relevantné podklady a nevykonáva svojvoľné zásahy do zariadenia alebo systému, ak na to nebol vyzvaný oprávnenou osobou.

Ak bezpečnostný incident vyžaduje okamžitý zásah, príslušná IT rola alebo iná oprávnená osoba môže prijať nevyhnutné technické alebo organizačné opatrenia na ochranu informačného systému, údajov alebo používateľov.

Ak bezpečnostný incident môže mať závažný dopad na dostupnosť informačného systému, ochranu údajov, prevádzku školy alebo jej organizačnej súčasti, príslušná IT rola alebo kontaktná osoba bezodkladne informuje poverenú osobu pre informačnú a kybernetickú bezpečnosť a podľa povahy incidentu aj štatutárny orgán VŠZaSP sv. Alžbety.

Ak incident môže zahŕňať porušenie ochrany osobných údajov, bezodkladne sa informuje aj osoba zodpovedná za oblasť ochrany osobných údajov.

VŠZaSP sv. Alžbety nie je v čase prijatia tejto smernice určená ako prevádzkovateľ základnej služby podľa zákona o kybernetickej bezpečnosti. Z tohto dôvodu sa na ňu nevzťahuje povinnosť hlásenia kybernetických bezpečnostných incidentov prostredníctvom Jednotného informačného systému kybernetickej bezpečnosti ani povinnosť hlásenia incidentov príslušným štátnym orgánom v rozsahu ustanovenom pre prevádzkovateľov základnej služby.

V prípade potreby je možné obrátiť sa na príslušné orgány, vrátane SK-CERT (www.sk-cert.sk, e-mail: incident@nbu.gov.sk), so žiadosťou o súčinnosť alebo odbornú pomoc. Poskytnutie takejto pomoci však nie je automatické ani garantované a závisí od aktuálnych kapacít a priorít týchto orgánov.

Tým nie je dotknutá povinnosť riešiť bezpečnostné incidenty interne, viesť o nich primeranú evidenciu a v prípade potreby informovať príslušné osoby, zmluvných partnerov, dozorné orgány alebo iné príslušné orgány podľa osobitných právnych predpisov, najmä v oblasti ochrany osobných údajov.

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

8.10.3 *Evidencia, prešetrovanie a riešenie bezpečnostných incidentov*

Ohlásené bezpečnostné incidenty, dôvodné podozrenia na bezpečnostné incidenty a bezpečnostné udalosti sa evidujú v rozsahu určenom VŠZaSP sv. Alžbety. Evidencia bezpečnostného incidentu môže obsahovať najmä dátum a čas zistenia incidentu, dátum a čas jeho oznámenia, osobu, ktorá incident oznámila, dotknutý informačný systém, službu, zariadenie, používateľské konto alebo miesto, stručný opis incidentu, predbežné posúdenie jeho závažnosti, informáciu o možnom dotknutí osobných, dôverných alebo iných citlivých údajov, prijaté opatrenia, použité riešenia osoby alebo dodávateľov zapojených do riešenia incidentu, priebeh riešenia a spôsob jeho uzavretia.

Evidencia bezpečnostných incidentov sa priebežne aktualizuje podľa stavu ich riešenia a podľa dostupných nových informácií. VŠZaSP sv. Alžbety zabezpečuje primeranú ochranu, uchovávanie a archiváciu záznamov o bezpečnostných incidentoch tak, aby bola zachovaná dôvernosť informácií a ochrana osobných údajov podľa platných právnych predpisov a interných pravidiel vysokej školy.

Riešenie incidentu zabezpečuje podľa jeho povahy príslušná IT rola, poverená osoba pre informačnú a kybernetickú bezpečnosť, správca dotknutého systému, dodávateľ alebo iná oprávnená osoba.

Osoba alebo útvar prešetrujúci podozrenie na bezpečnostný incident najskôr posúdi, či oznámená udalosť predstavuje bezpečnostný incident, technickú poruchu, prevádzkovú udalosť, zraniteľnosť alebo iný typ požiadavky. V prípade potreby si vyžiada súčinnosť od príslušných IT rolí, vlastníkov alebo správcov systémov, vedúcich zamestnancov, používateľov alebo dodávateľov. Tieto osoby poskytujú súčinnosť v rozsahu svojich možností, oprávnení a zmluvných povinností.

Ak sa na základe dostupných poznatkov vyhodnotí, že ide o bezpečnostný incident alebo dôvodné podozrenie na bezpečnostný incident, príslušná IT rola alebo kontaktná osoba bez zbytočného odkladu informuje poverenú osobu pre informačnú a kybernetickú bezpečnosť, ak je určená, a osobu alebo útvar zodpovedný za prevádzku dotknutého informačného systému, služby, zariadenia alebo technického prostriedku.

Pri prešetrovaní incidentu sa podľa dostupnosti a povahy incidentu zhromažďujú najmä informácie o charaktere incidentu, dotknutých aktívach, systémoch, zariadeniach, používateľoch, zúčastnených osobách, pracoviskách alebo lokalitách, službách, prípadne technické identifikátory, ako sú IP adresa alebo identifikačné údaje zariadenia, ako aj dostupné podklady potrebné na posúdenie incidentu. Môže ísť napríklad o auditné alebo prevádzkové záznamy, záznamy o prihlásení, kópiu alebo hlavičku podozrivej e-mailovej komunikácie, snímku obrazovky, informáciu o čase a priebehu incidentu alebo informáciu o už vykonaných bezprostredných opatreniach.

Ak je dotknutý informačný systém, služba, zariadenie alebo technický prostriedok spravovaný dodávateľom, VŠZaSP sv. Alžbety si od príslušného dodávateľa vyžiada súčinnosť pri posúdení, riešení a zdokumentovaní incidentu v rozsahu vyplývajúcom zo zmluvy alebo z povahy poskytovanej služby.

Pri riešení incidentu sa prijímajú primerané technické a organizačné opatrenia na obmedzenie jeho dopadu, zabránenie ďalšiemu šíreniu, ochranu údajov a systémov, zachovanie dostupných dôkazov, obnovu bezpečnej prevádzky, zdokumentovanie priebehu a prijatie nápravných alebo preventívnych

opatrení. Podľa povahy incidentu môže ísť najmä o obmedzenie alebo zablokovanie prístupových práv, reset hesiel, izolovanie alebo odpojenie dotknutého zariadenia alebo služby, preverenie auditných a systémových záznamov, obnovu údajov zo záloh, kontrolu zariadenia alebo softvéru, vyžiadanie súčinnosti dodávateľa alebo informovanie príslušných osôb.

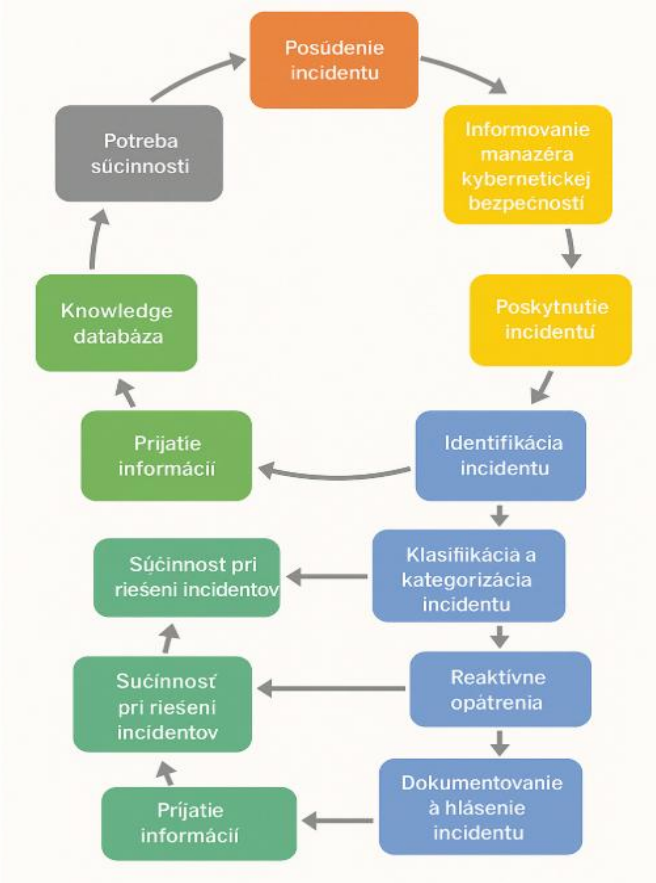
Ako súčasť prešetrovania incidentu sa podľa jeho povahy vykoná identifikácia incidentu, posúdenie jeho závažnosti, prípadná klasifikácia a kategorizácia, prijatie reaktívnych opatrení, zaistenie dostupných stôp a dôkazov, priebežné dokumentovanie a uzavretie incidentu.

Pri klasifikácii a kategorizácii bezpečnostného incidentu sa primerane posudzuje najmä jeho typ, závažnosť, rozsah a dopad na informačné systémy, údaje, služby, používateľov alebo prevádzku VŠZaSP sv. Alžbety, pričom sa vychádza z kategórií, typov a príkladov bezpečnostných incidentov uvedených v prílohe č. 9.3 tejto smernice.

Ak incident môže mať závažný dopad na dostupnosť informačného systému, ochranu údajov, prevádzku školy alebo jej organizačnej súčasti, postup riešenia koordinuje poverená osoba pre informačnú a kybernetickú bezpečnosť v spolupráci s príslušnou IT rolou, správcom dotknutého systému, dodávateľom a podľa potreby aj štatutárnym orgánom VŠZaSP sv. Alžbety alebo ním poverenou osobou.

Ak incident môže zahŕňať porušenie ochrany osobných údajov, bezodkladne sa informuje osoba zodpovedná za oblasť ochrany osobných údajov, najmä DPO. Ďalší postup sa posúdi podľa právnych predpisov na ochranu osobných údajov a interných pravidiel VŠZaSP sv. Alžbety.

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk



Proces riešenia bezpečnostného incidentu je cyklický a zahŕňa najmä potrebu súčinnosti, posúdenie incidentu, informovanie príslušných osôb, poskytnutie informácií, identifikáciu a prípadnú klasifikáciu incidentu, prijatie reaktívnych opatrení, dokumentovanie incidentu, priebežné dopĺňanie informácií, súčinnosť pri riešení a využitie získaných poznatkov pri ďalšom zlepšovaní bezpečnostných opatrení.

Diagram riešenia bezpečnostného incidentu znázorňuje, že riešenie incidentu nie je jednorazový úkon, ale opakujúci sa proces. Po prijatí informácie o incidente sa incident posúdi, identifikuje, rieši, dokumentuje a následne sa z neho vyvodia poznatky pre ďalšie zlepšenie bezpečnosti informačných systémov VŠZaSP sv. Alžbety.

8.10.4 Poučenie sa z bezpečnostných incidentov

Po vyriešení bezpečnostného incidentu sa podľa jeho povahy vyhodnotia jeho príčiny, spôsob zistenia, časový priebeh, dotknuté systémy, služby, zariadenia alebo údaje, dopad na prevádzku vysokej školy, dopad na používateľov alebo dotknuté osoby a účinnosť prijatých opatrení.

V prípade závažnejšieho bezpečnostného incidentu alebo incidentu s významným dopadom na prevádzku školy, používateľov, údaje alebo informačné systémy sa po jeho vyriešení vypracuje primerané záverečné vyhodnotenie incidentu. Záverečné vyhodnotenie obsahuje najmä stručný opis incidentu, jeho príčiny, priebeh, dopad, prijaté opatrenia a odporúčania na zníženie rizika opakovania podobného incidentu.

Na základe vyhodnotenia sa podľa potreby prijmú nápravné alebo preventívne opatrenia zamerané na odstránenie príčin incidentu, zníženie pravdepodobnosti jeho opakovania alebo zmiernenie jeho možných dôsledkov, napríklad úprava prístupových práv, autentifikácie, bezpečnostných nastavení, monitorovania, dokumentácie, interných pravidiel, zmluvných podmienok dodávateľov alebo poučenie používateľov. Plnenie prijatých opatrení sa primerane sleduje.

Návrh nápravných a preventívnych opatrení pripravuje osoba alebo útvar prešetrujúci bezpečnostný incident v súčinnosti s príslušnou IT rolou, poverenou osobou pre informačnú a kybernetickú bezpečnosť, ak je určená, správcom dotknutého systému, príslušným dodávateľom alebo vlastníkom dotknutého aktíva.

Ak si navrhované opatrenia vyžadujú významné finančné, personálne alebo organizačné zabezpečenie, ich realizáciu schvaľuje štatutárny orgán VŠZaSP sv. Alžbety alebo ním poverená osoba.

Poznatky získané pri riešení bezpečnostných incidentov sa primerane využívajú pri aktualizácii interných pravidiel, bezpečnostných opatrení, zmluvných podmienok dodávateľov, školení a materiálov určených na zvyšovanie bezpečnostného povedomia používateľov. Ak z incidentu vyplynie potreba poučenia používateľov alebo tretích strán, prijaté odporúčania sa môžu zapracovať do školiacich alebo informačných materiálov.

Dokumentácia z evidovaných bezpečnostných incidentov a bezpečnostných udalostí sa môže využívať aj na tvorbu interných prehľadov a štatistík, najmä na sledovanie typov incidentov, ich rozsahu, opakujúcich sa príčin, prijatých opatrení a dopadov na prevádzku školy. Tieto informácie slúžia na rozhodovanie o oblastiach, ktoré je potrebné ďalej pokryť bezpečnostnými opatreniami, technickými zmenami alebo interným vzdelávaním, pričom sa primerane prihliada aj na povahu činností VŠZaSP sv. Alžbety, prevádzkované informačné systémy a aktuálnu bezpečnostnú situáciu v Slovenskej republike a Európskej únii.

Ak bezpečnostný incident zakladá podozrenie na porušenie pracovných, študijných, zmluvných alebo právnych povinností, ďalší postup sa rieši podľa príslušných interných predpisov, zmluvných podmienok a právnych predpisov. V odôvodnených prípadoch môže VŠZaSP sv. Alžbety posúdiť aj potrebu spolupráce s príslušnými orgánmi verejnej moci alebo orgánmi činnými v trestnom konaní.

8.10.5 Incidenty týkajúce sa osobných údajov

Ak bezpečnostný incident môže mať za následok neoprávnený prístup k osobným údajom, ich neoprávnené sprístupnenie, stratu, zničenie, zmenu, poškodenie alebo iné porušenie ich bezpečnosti, považuje sa za incident týkajúci sa osobných údajov.

Incident týkajúci sa osobných údajov je potrebné bezodkladne oznámiť osobe určenej VŠZaSP sv. Alžbety na riešenie ochrany osobných údajov.

Pri incidente týkajúcom sa osobných údajov sa posudzuje najmä druh a rozsah dotknutých osobných údajov, kategórie a počet dotknutých osôb, príčina incidentu, možný dopad na práva a slobody dotknutých osôb, prijaté alebo navrhované opatrenia a potreba oznámenia incidentu dozornému orgánu alebo dotknutým osobám.

Ak z posúdenia vyplynie povinnosť oznámiť porušenie ochrany osobných údajov dozornému orgánu alebo dotknutým osobám, VŠZaSP sv. Alžbety postupuje podľa právnych predpisov na ochranu osobných údajov a interných pravidiel.

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

O incidente týkajúcom sa osobných údajov sa vedie dokumentácia v rozsahu potrebnom na preukázanie splnenia povinností VŠZaSP sv. Alžbety podľa právnych predpisov na ochranu osobných údajov.

Ak incident týkajúci sa osobných údajov vznikol u dodávateľa alebo sprostredkovateľa, dodávateľ alebo sprostredkovateľ je povinný poskytnúť VŠZaSP sv. Alžbety bezodkladnú súčinnosť v rozsahu určenom zmluvou, sprostredkovateľskou zmluvou alebo právnymi predpismi.

8.10.6 Porušenie pravidiel študentmi

Porušenie pravidiel tejto smernice študentom VŠZaSP sv. Alžbety sa môže riešiť podľa príslušných vnútorných predpisov vysokej školy.

Pri menej závažnom porušení pravidiel môže byť študent upozornený na porušenie pravidiel a poučený o povinnosti zdržať sa ďalšieho porušovania tejto smernice.

Pri závažnejšom, opakovanom alebo zvlášť závažnom porušení pravidiel môže škola dočasne obmedziť alebo zablokovať prístup študenta k dotknutým IT službám, zdokumentovať porušenie, postúpiť vec na riešenie podľa príslušných vnútorných predpisov a prijať technické alebo organizačné opatrenia na ochranu bezpečnosti alebo prevádzky informačného systému.

Za zvlášť závažné porušenie pravidiel sa môže považovať najmä pokus o neoprávnený prístup, zneužitie cudzieho účtu alebo hesla, šírenie škodlivého softvéru, neoprávnené získavanie alebo poskytovanie informačných zdrojov, neoprávnené sprístupnenie alebo zneužitie osobných údajov, úmyselné narušenie prevádzky dátovej siete alebo informačného systému alebo opakované porušovanie tejto smernice..

Prípadná trestnoprávna, priestupková, občianskoprávna alebo iná právna zodpovednosť študenta nie je postupom podľa tejto smernice dotknutá.

8.10.7 Porušenie pravidiel zamestnancami

Porušenie pravidiel tejto smernice zamestnancom VŠZaSP sv. Alžbety sa môže považovať za porušenie pracovnej disciplíny alebo porušenie základných povinností zamestnanca podľa pracovnoprávnych predpisov, pracovného poriadku alebo iného príslušného interného predpisu.

Pri zistení porušenia pravidiel oprávnená osoba upozorní zamestnanca, ktorý pravidlá porušil, na túto skutočnosť.

Pri opakovanom, hrubom alebo závažnom porušení pravidiel môže vysoká škola prijať opatrenia najmä upozornenie zamestnanca, dočasné obmedzenie alebo zablokovanie prístupu k IT službám, odobratie alebo zmenu prístupových práv, technické alebo organizačné opatrenia na ochranu informačného systému, pracovnoprávne opatrenia alebo postúpenie veci príslušnému orgánu, ak to vyžaduje povaha porušenia.

Pri opakovanom porušení pravidiel sa prípad spolu s dokumentáciou postúpi osobe alebo orgánu určenému na rozhodnutie o ďalšom postupe.

Prípadná trestnoprávna, priestupková, občianskoprávna, pracovnoprávna alebo iná právna zodpovednosť zamestnanca nie je postupom podľa tejto smernice dotknutá.

8.10.8 Porušenie pravidiel externými používateľmi, dodávateľmi a tretími stranami

Porušenie pravidiel tejto smernice externým používateľom, dodávateľom, servisnou organizáciou alebo inou treťou stranou sa posudzuje podľa tejto smernice, zmluvných podmienok, poverenia, dohody o mlčanlivosti, sprostredkovateľskej zmluvy alebo iného právneho vzťahu s VŠZaSP sv. Alžbety.

Pri porušení pravidiel externou osobou môže vysoká škola prijať opatrenia najmä upozornenie, dočasné obmedzenie alebo zablokovanie prístupu, zrušenie prístupových práv, ukončenie alebo obmedzenie servisného zásahu, požiadavku na nápravné opatrenia, uplatnenie zmluvnej zodpovednosti alebo náhrady škody, ukončenie zmluvného vzťahu alebo oznámenie veci príslušnému orgánu, ak to vyžaduje povaha porušenia..

Ak externá osoba alebo dodávateľ poruší pravidlá ochrany osobných údajov, dôverných informácií alebo bezpečnosti informačného systému, VŠZaSP sv. Alžbety posúdi aj potrebu prijatia opatrení podľa právnych predpisov na ochranu osobných údajov a podľa zmluvnej dokumentácie.

Dodávateľ alebo externá osoba je povinná poskytnúť VŠZaSP sv. Alžbety súčinnosť pri objasnení porušenia pravidiel, riešení bezpečnostného incidentu, obnove prevádzky a prijímaní nápravných opatrení.

Prípadná trestnoprávna, občianskoprávna, zmluvná alebo iná právna zodpovednosť externej osoby, dodávateľa alebo tretej strany nie je postupom podľa tejto smernice dotknutá.

8.10.9 Nácvik incidentov

Nácvik incidentov predstavuje plánované alebo simulované cvičenia zamerané na preverenie pripravenosti VŠZaSP sv. Alžbety na bezpečnostné a kybernetické incidenty. Tieto nácviky sú dobrovoľné a slúžia najmä na posilnenie prevencie a zvýšenie bezpečnostného povedomia používateľov a zamestnancov. Cieľom je overiť existujúce postupy a zlepšiť reakciu používateľov, zamestnancov a poverených osôb.

Do nácviku môžu patriť najmä:

Diskusné scenáre (tabletop) – preverenie rozhodovacích procesov a rolí pri incidentoch,
Technické simulácie – napr. phishing, malvér, výpadky systémov, obnova dát zo záloh,
Krízová komunikácia – overenie informačných tokov a koordinácie medzi zainteresovanými osobami,
Overenie rolí a postupov – praktické skúšky definovaných postupov a zodpovedností,

Vyhodnotenie cvičenia – identifikácia slabých miest, návrh nápravných opatrení a aktualizácia interných procesov.

Výstupy z nácviku sa dokumentujú, evidujú a používajú na audit, zlepšenie pripravenosti školy a doplnenie školení používateľov.

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

8.11. Previerka a kontrolná činnosť

V tejto časti sú upravené pravidlá vykonávania previerok informačného systému, zariadení, bezpečnostných opatrení a dodržiavania tejto smernice, ako aj pravidlá dokumentovania výsledkov a prijímania nápravných opatrení.

Cieľom previerky a kontrolnej činnosti je overiť, či sa informačný systém, údaje, prístupové práva a bezpečnostné opatrenia VŠZaSP sv. Alžbety používajú a spravujú v súlade s touto smernicou, právnymi predpismi a internými pravidlami vysokej školy.

8.11.1 Previerka informácií, zariadení a bezpečnostných opatrení informačného systému

Previerka informácií, zariadení a bezpečnostných opatrení informačného systému sa vykonáva na účely overenia stavu ochrany informačného systému, údajov a prístupových práv vysokej školy.

Previerka sa môže týkať najmä technických a programových prostriedkov, informačných systémov, aplikácií, serverov, databáz, úložísk, dátovej siete, používateľských účtov, prístupových práv, autentifikačných mechanizmov, auditných záznamov, zálohovania, ochrany osobných a dôverných údajov, bezpečnostných opatrení a dokumentácie informačného systému.

Previerka sa vykonáva v rozsahu primeranom účelu previerky, významu preverovaného systému, citlivosti spracúvaných údajov a bezpečnostným rizikám.

Previerka alebo kontrola môže byť vykonaná osobami určenými vysokou školou alebo externe oprávnenou osobou, ak je to potrebné na overenie stavu informačného systému, bezpečnostných opatrení alebo dodržiavania tejto smernice..

Previerka sa vykonáva na základe ustanovenia právnych predpisov, rozhodnutia štatutárneho orgánu, podnetu príslušnej IT role, ak došlo k zmene technických, organizačných alebo bezpečnostných podmienok, alebo na základe zisteného bezpečnostného incidentu, podozrenia na porušenie tejto smernice, technickej poruchy, organizačnej zmeny alebo zmeny informačného systému.

Pri previerke sa postupuje tak, aby nedošlo k neoprávnenému zásahu do údajov, narušeniu prevádzky informačného systému alebo neoprávnenému sprístupneniu informácií.

8.11.2 Kontrola dodržiavania smernice

Dodržiavanie tejto smernice podlieha kontrole zo strany oprávnených osôb VŠZaSP sv. Alžbety.

Kontrola dodržiavania smernice sa môže zamerať najmä na používanie informačného systému, technických a programových prostriedkov IT, používateľských účtov, hesiel, prístupových práv, elektronickej pošty, internetu, interných informačných služieb, dátovej siete, ochranu osobných a

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk

dôverných údajov, zálohovanie a obnovu údajov, prácu s dodávateľmi a tretími stranami, hlásenie a riešenie bezpečnostných incidentov a plnenie nápravných alebo preventívnych opatrení.

Previerka sa vykonáva na základe ustanovenia právnych predpisov, rozhodnutia štatutárneho orgánu, podnetu príslušnej IT role, najmä pri podozrení na porušenie tejto smernice, pri bezpečnostnom incidente, pri zmene technickej infraštruktúry alebo na základe rozhodnutia oprávnenej osoby. Vykonáva spôsobom primeraným jej účelu a nesmie neodôvodnene zasahovať do práv používateľov, ochrany súkromia alebo riadnej prevádzky informačného systému.

Používatelia, IT roly, vedúci zamestnanci, dodávatelia a ďalšie osoby, ktorých sa kontrola týka, sú povinní poskytnúť pri kontrole potrebnú súčinnosť v rozsahu svojich oprávnení a povinností.

8.11.3 Dokumentovanie výsledkov previerok a nápravné opatrenia

O vykonanej previerke alebo kontrole sa vyhotoví záznam, protokol, správa alebo iný dokument podľa povahy a rozsahu previerky alebo kontroly. Dokumentácia môže obsahovať najmä rozsah a dátum kontroly, zistenia, nedostatky alebo riziká, uložené alebo odporúčané opatrenia, termín ich splnenia a zodpovednú osobu alebo útvar.

Prístup k dokumentácii z previerok a kontrol majú iba oprávnené osoby v rozsahu potrebnom na plnenie ich pracovných, kontrolných, riadiacich, zmluvných alebo zákonných povinností.

Ak sa pri previerke, kontrole alebo audite zistia nedostatky, riziká alebo porušenia tejto smernice, VŠZaSP sv. Alžbety prijme primerané nápravné alebo preventívne opatrenia, najmä technickú nápravu, úpravu konfigurácie, aktualizáciu softvéru, zmenu prístupových práv, zmenu hesiel alebo autentifikačných mechanizmov, doplnenie bezpečnostných opatrení, monitorovania alebo auditných záznamov, aktualizáciu dokumentácie, preškolenie alebo upozornenie používateľa, úpravu interného postupu alebo zmluvných podmienok dodávateľa, prípadne postúpenie veci na riešenie zodpovednosti alebo postihu.

Za splnenie opatrenia zodpovedá osoba, útvar alebo iný subjekt určený v zázname z previerky, kontroly alebo auditu; termín splnenia sa určí podľa závažnosti zistenia, miery rizika, technickej náročnosti a dopadu na prevádzku informačného systému.

8.11.4 Oprávnené osoby na výkon kontroly

Kontrolu dodržiavania tejto smernice, previerku informačného systému alebo kontrolu plnenia nápravných opatrení môžu vykonávať iba oprávnené osoby určené VŠZaSP sv. Alžbety, najmä štatutárny orgán alebo ním poverené osoby, vedúci zamestnanci v rozsahu svojej pôsobnosti, určené IT roly, osoba poverená informačnou a kybernetickou bezpečnosťou, osoba určená pre oblasť ochrany osobných údajov, interný kontrolný alebo auditný útvar, externý audítor alebo poverený konzultant.

Oprávnené osoby sú pri výkone kontroly povinné postupovať odborne, primerane, nestranne a v rozsahu zodpovedajúcom účelu kontroly. Sú povinné zachovávať mlčanlivosť o informáciách, s ktorými

sa pri kontrole oboznámia, ak tieto informácie nie sú určené na zverejnenie alebo ďalšie oprávnené sprístupnenie.
Používatelia, IT roly, dodávatelia a ďalšie dotknuté osoby sú povinné poskytnúť oprávneným osobám primeranú súčinnosť potrebnú na výkon kontroly.

9. Prílohy

9.1. Bezpečnostné a prevádzkové opatrenia akademického informačného systému

(neverejná príloha Smernice o kybernetickej bezpečnosti a riadení IT)

9.2. Kontakty na IT podporu a hlásenie bezpečnostných incidentov

Dostupné komunikačné kanály na zadávanie IT požiadaviek a správu prístupov:

Email IT podpora: ferianc@vssvalzbety.sk ; po zriadení všeobecnej funkčnej adresy bude používaný príslušný kontaktný email IT podpory

Emailový kontakt na hlásenie bezpečnostných incidentov: incident@vssvalzbety.sk

Emailový kontakt na hlásenie GDPR incidentov: gdpr@vssvalzbety.sk

9.3. Kategórie a typy bezpečnostných incidentov

Typy incidentov:

Typ	Druh	Popis
Narušenie integrity	Neautorizovaná zmena údajov a informácií. Neautorizovaná zmena zdrojového kódu, Poškodenie hardvéru.	Úspešná neautorizovaná zmena údajov počas ich spracúvania, prenosu alebo uloženia (napr. ransomware, modifikácia údajov v IS,...), prostredníctvom infiltrácie útočníka do siete alebo IS.

Nedostupnosť	DoS, DDoS útok, sabotáž, výpadok/nedostupnosť služby.	Zahltenie siete alebo IS takým množstvom požiadaviek, že vykonávané činnosti sú oneskorené, alebo príde ku úplnému zahlteniu (DDoS, DoS...).Dostupnosť sietí a IS môže byť obmedzená aj lokálnou aktivitou (poškodenie, prerušenie napájania,...).
Nežiaduci obsah	Spam, obťažovanie, vyhrážanie, násilie, potláčanie práv a slobôd.	Nežiaduci obsah – spam, podvodné, obťažujúce, škodlivé alebo inak nevhodné elektronické správy alebo webový obsah.
Ohrozenie bezpečnosti informácií	Neoprávnený prístup k informáciám, únik informácií, poškodenie informácií.	Okrem lokálneho zneužitia dát a systémov, bezpečnosť informácií môže byť ohrozená aj úspešnou kompromitáciou aplikácie alebo účtu. Patria sem aj útoky, pri ktorých dochádza k zachytávaniu a pristupovaniu k informáciám počas ich prenosu (odpočúvanie, útoky typu man-in-the-middle...).
Podozrenie na úspešný prienik do systému	Kompromitácia privilegovaného účtu. Kompromitácia servisného alebo užívateľského účtu. Kompromitácia aplikácie, Botnet.	Úspešná kompromitácia systému alebo aplikácie (služby). Môže ku nej prísť na diaľku, prostredníctvom využitia známej alebo novej zraniteľnosti, ale aj neautorizovaným lokálnym prístupom.
Podvod	Neautorizované využitie prostriedkov, porušenie autorských práv, phishing, prevzatie identity,	Patrí sem využívanie zdrojov na neoprávnené účely vrátane neoprávneného zisku (napr. účasť na ilegálnych reťazových e-mailoch pre dosiahnutie zisku alebo pyramídové schémy). Patrí sem aj predaj a inštalácia nelicencovaných kópií komerčného softvéru alebo iných materiálov chránených autorskými právami. Ďalej sem patria útoky, pri ktorých jedna entita nelegitímne predstiera identitu druhej, aby z toho mala úžitok, ako aj phishing.
Pokus o prienik	Využitie známej zraniteľnosti. Opakované pokusy o prihlásenie.	Pokus o neoprávnený prístup alebo zneužitie zraniteľnosti siete alebo informačného systému; v prípade úspechu môže viesť ku kompromitácii systému alebo účtu.
Škodlivý kód	Vírus, malvér, ransomvér.	Programové prostriedky alebo údaje, ktoré zapríčiňujú alebo môžu zapríčiniť kybernetický bezpečnostný incident. Na ich aktiváciu je niekedy potrebná súčinnosť používateľa.

Získavanie informácií	Skenovanie siete, odpočúvanie, sociálne inžinierstvo.	Skenovanie znamená zasielanie špecifických požiadaviek na cieľový systém, s cieľom odhalenia jeho slabín. Odpočúvanie zahŕňa sledovanie a zaznamenávanie sieťovej prevádzky za účelom získavania informácií. Sociálne inžinierstvo znamená získavanie dôverných alebo osobných informácií prostredníctvom osôb.
Iné	Strata alebo krádež zariadenia, pripojenie neautorizovaného zariadenia.	

10. Záverečné ustanovenia

Táto smernica bola schválená zamestnávateľom dňa 28.08.2026.

Táto Smernica nadobúda účinnosť dňom jej schválenia.

Zamestnávateľ zabezpečí oboznámenie zamestnancov s touto Smernicou.

v Bratislave

.....

prof. MUDr. Stanislav Špánik, CSc., MHA, v.r.

poverený rektor

.....

Ing. Michal Krčméry, v.r.

riaditeľ

Vysoká škola zdravotníctva a sociálnej práce sv. Alžbety v Bratislave, n. o.
Palackého 1
811 02 Bratislava
www.vssvalzbety.sk