Paneurópska vysoká škola v Bratislave

Smernica rektora č. 4/2015

Bezpečnostná politika informačných systémov na Paneurópskej vysokej škole

Bratislava, 2015

OBSAH

Pojmy a skratky

Aktívum

Čokoľvek, čo má pre organizáciu hodnotu (dobré meno, údaje a informácie obchodného tajomstva, osobné údaje, informačné systémy a infraštruktúra využívaná v prevádzke, zamestnanci a objekty, procesy, vzťahy so zákazníkmi, duševné vlastníctvo, finančné údaje).

APV

Aplikačné programové vybavenie.

Autentifikácia

Je proces overenia identity používateľa žiadajúceho o službu alebo zdroj.

Autorizácia

Je proces overenia, či autentifikovaný používateľ má právo prístupu k požadovanej službe alebo zdroju.

Bezpečnostný incident

Bezpečnostný incident predstavuje udalosť s potenciálom možného narušenia informačnej bezpečnosti alebo poskytovaných služieb (t.j. dôvernosť, dostupnosť alebo integritu informačných aktív). Bezpečnostné incidenty môžu mať charakter prevádzkových problémov, resp. problémov nahlásených používateľmi ako je vírusová nákaza, nefunkčnosť klimatizácie, výpadok systému, ap. Medzi bezpečnostné incidenty patria aj situácie, ktoré indikujú porušenie politiky informačnej bezpečnosti, zlyhanie bezpečnostných mechanizmov, alebo neznámu situáciu s možným dopadom na informačnú bezpečnosť.

Bezpečnosť

Udržiavanie dôvernosti, integrity a dostupnosti aktív implementáciou vhodnej sady opatrení, ktorými môžu byť politiky, praktiky, procedúry, organizačné štruktúry, hardvérové mechanizmy, softvérové funkcie a pod.

Bezpečnostné opatrenie

Mechanizmus, ktorý znižuje zraniteľnosť informačného systému voči určitej hrozbe alebo jej dopad.

Dostupnosť

Atribút informácie alebo systému vyjadrujúci schopnosť byť dostupný a použiteľný na požiadanie autorizovanému používateľovi.

Dôvernosť

Atribút informácií, ktorý znemožňuje ich odhalenie neautorizovaným subjektom. Ide o zabránenie neoprávneného prístupu k informáciám a údajom.

Firewall

Logická alebo fyzická bariéra, ktorá bráni neautorizovanej alebo nechcenej komunikácii medzi časťami počítačovej siete alebo informačného systému.

Hrozba

Je akcia alebo udalosť, ktorá môže ohroziť bezpečnosť aktíva. Je to skutočnosť, ktorá reálne existuje nezávisle od existencie hodnoteného systému.

Identifikácia

Postup, umožňujúci jednoznačné zistenie, stanovenie alebo dokázanie totožnosti, t. j. identity entity podľa vlastností, ktoré sú pre danú entitu príznačné.

IKT

Informačno-komunikačné technológie.

Integrita

Vlastnosť zabezpečujúca presnosť a kompletnosť aktív. Integrita zaručuje, že objekt bol zmenený len špecifikovaným a autorizovaným spôsobom, bez skrytej manipulácie.

Informačný systém (IS)

Je funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických a programových prostriedkov, ktoré sú súčasťou informačného systému.

Oprávnená osoba

Je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovnoprávneho vzťahu, na základe poverenia, zvolenia alebo vymenovania a ktorá spracúva osobné údaje v rozsahu a spôsobom určeným v poučení podľa zákona č. 122/2013 o ochrane osobných údajov.

Osoba poverená výkonom dohľadu nad ochranou osobných údajov (Zodpovedná osoba)

Je osoba, ktorá je v zmysle požiadaviek zákona o ochrane osobných údajov poverená v rámci PEVŠ za výkon dohľadu nad ochranou osobných údajov.

PEVŠ

Paneurópska vysoká škola.

Používateľ

Zamestnanec PEVŠ, ktorý má oprávnenie používať daný informačný systém s vopred pridelenými používateľskými oprávneniami.

Riziko

Pravdepodobnosť, že zraniteľnosť v systéme ovplyvní overenie alebo dostupnosť, pravosť, integritu alebo dôvernosť spracúvaných alebo prenesených údajov, ako aj vážnosť dopadu úmyselného alebo neúmyselného využitia takejto zraniteľnosti.

Správca IS

Zodpovedá za správu a rozvoj daného informačného systému v prostredí PEVŠ.

Tretia strana

Spoločný názov pre všetky právnické osoby, ktoré spolupracujú, podporujú alebo ovplyvňujú služby realizované v prostredí PEVŠ.

Vlastník aktív

Vlastník aktíva zodpovedá za jeho správnu prevádzku a bezpečnosť, vlastníctvo aktív môže byť spravidla priradené konkrétnemu zamestnancovi, organizačnej role alebo organizačnému útvaru.

V súlade s čl. 12 ods. 2 Organizačného poriadku Rektorátu Paneurópskej vysokej školy v Bratislave (ďalej len „PEVŠ") vydáva rektor PEVŠ smernicu č. 4/2015, „Bezpečnostná politika informačných systémov na Paneurópskej vysokej škole."

Článok 1
Vyhlásenie vedenia o podpore informačnej bezpečnosti a základné ustanovenia

1. Poslaním tejto Bezpečnostnej politiky informačných systémov (ďalej len „IS") na Paneurópskej vysokej škole (ďalej len „PEVŠ") je spolu s ďalšími dokumentmi a vnútornými predpismi stanoviť stratégiu a konkrétne pravidlá bezpečného správania sa používateľov pri ich činnostiach v rámci práce s IS.

2. Táto Bezpečnostná politika IS sa vzťahuje na všetky aktíva PEVŠ, ktoré priamo súvisia so spracovaním informácií a dát v prostredí PEVŠ. Bezpečnostná politika IS je záväzná pre všetkých zamestnancov PEVŠ, ako aj pre všetkých zamestnancov tretích strán, ktoré pristupujú ku aktívam PEVŠ.

3. Vedenie PEVŠ, vedomé si zodpovednosti a potreby chrániť aktíva pred hrozbami a rizikami, považuje oblasť informačnej bezpečnosti za jednu zo svojich základných úloh, ktorej venuje dostatočnú pozornosť a finančnú podporu.

4. Vedenie PEVŠ schvaľuje túto bezpečnostnú politiku IS, podporuje ju a realizuje kroky na jej presadzovanie prostredníctvom poverených zamestnancov PEVŠ, najmä rektora PEVŠ, vedúceho oddelenia IT a vedúcich zamestnancov jednotlivých oddelení.

5. Bezpečnostná politika IS musí byť presadzovaná na všetkých úrovniach riadenia PEVŠ. Procesy súvisiace s realizáciou bezpečnostnej politiky IS spravidla koordinuje vedúci daného oddelenia. Za súlad každého aktíva s bezpečnostnou politikou IS a súvisiacimi predpismi zodpovedá správca daného aktíva.

Článok 2
Ciele v oblasti informačnej bezpečnosti

1. Základné ciele v oblasti informačnej bezpečnosti sú stanovené touto bezpečnostnou politikou IS a sú najmä:
   - dodržiavanie legislatívne stanovených požiadaviek relevantných pre oblasť informačnej bezpečnosti v PEVŠ,
   - minimalizácia finančných a iných strát súvisiacich s narušením prevádzky IS,
   - minimalizácia rizík ohrozenia aktív IS,
   - ochrana aktív PEVŠ pred ich zneužitím,
   - ochrana dát PEVŠ pred ich zneužitím alebo neoprávneným prístupom,
   - ochrana know-how a dobrého mena PEVŠ.

2. Na zaistenie dosahovania vyššie uvedených bezpečnostných cieľov je potrebné implementovať a kontinuálne realizovať najmä nasledovné princípy:
   - k ochrane informácií musia byť vytvorené zodpovedajúce technické a organizačné predpoklady,

- informácie spracúvané v IS musia byť chránené tak, aby nedošlo narušeniu ich dôvernosti, integrity a dostupnosti,
- účinnosť bezpečnostných opatrení slúžiacich k ochrane informačných aktív musí byť pravidelne vyhodnocovaná,
- pokrytie riešenia informačnej bezpečnosti musí byť súčasťou každého nového projektu súvisiaceho s ľubovoľným IS PEVŠ (existujúcim alebo novým),
- úroveň bezpečnostného povedomia všetkých zamestnancov PEVŠ musí byť pravidelne rozvíjaná v súlade s cieľmi bezpečnostnej politiky IS.

3. V každej oblasti informačnej bezpečnosti v tejto bezpečnostnej politike IS sú ďalej stanovené konkrétne bezpečnostné ciele pre danú oblasť a základné princípy a spôsoby/postupy, ktorými sa jednotlivé ciele v podmienkach PEVŠ dosahujú.

Článok 3
Organizácia bezpečnosti

1. Cieľom tejto oblasti bezpečnosti je kontinuálne a efektívne riadiť informačnú bezpečnosť v PEVŠ vrátane vzťahov s tretími stranami a servisnými organizáciami.

2. Základné princípy, ktorými sa ciele v podmienkach PEVŠ dosahujú:
   - musí sa periodicky vykonávať analýza rizík pri zmenách a rozšíreniach súvisiacich s IS a internými procesmi PEVŠ,
   - kľúčové role vo vzťahu k informačnej bezpečnosti musia byť definované a musia mať priradené činnosti, zodpovednosti a právomoci,
   - zodpovednosti za informačnú bezpečnosť v zmluvných vzťahoch s tretími stranami a servisnými organizáciami musia byť explicitne vymedzené.

3. Pre všetky významné IS musí byť zavedený proces riadenia rizík vykonávaný najmä prostredníctvom analýzy rizík a návrhu bezpečnostných opatrení na zmiernenie identifikovaných rizík na prijateľnú úroveň.

4. Analýza rizík musí byť realizovaná aj pri zmenách a rozšíreniach súvisiacich s IS a internými procesmi PEVŠ, všetky rozhodnutia o prijatí alebo neprijatí bezpečnostných opatrení je potrebné založiť na výsledkoch príslušnej analýzy rizík.

5. Zodpovednosti za informačnú bezpečnosť v zmluvných vzťahoch s tretími stranami a servisnými/dodávateľskými partnermi musia byť explicitne vymedzené.

6. Presadzovanie a monitorovanie informačnej bezpečnosti PEVŠ koordinuje vedúci oddelenia IT.

Článok 4
Klasifikácia a riadenie aktív

1. Cieľom tejto oblasti bezpečnosti je udržiavať adekvátnu ochranu aktív podľa ich hodnoty pre PEVŠ.

2. Základné princípy, ktorými sa ciele v podmienkach PEVŠ dosahujú:

- všetky významné informačné aktíva musia mať prideleného svojho vlastníka,
- musí byť zavedená druhová klasifikačná schéma informačných aktív (napr. osobné údaje, skutočnosti tvoriace obchodné tajomstvo a pod.),
- významné informačné aktíva musia mať explicitne určený svoj životný cyklus pokiaľ sú spracované v prostredí IS PEVŠ.

3. Vlastníctvo sa určuje najmä pre nasledovné typy aktív:
   a) zariadenia IKT,
   b) záznamové médiá podliehajúce evidencii,
   c) APV používané na zariadeniach PEVŠ,
   d) agendy a elektronické informácie spracovávané PEVŠ.

4. Každé aktívum uvedené v predchádzajúcom odseku musí mať konkrétneho vlastníka. Vlastníkom môže byť konkrétny zamestnanec, funkčné miesto, alebo organizačný útvar.

5. Z hľadiska požiadaviek na dôvernosť sa rozoznávajú v prostredí PEVŠ nasledovné typy informácií:
   a) citlivé informácie (chránené),
   b) interne prístupné informácie,
   c) verejné informácie (nechránené),
   d) špeciálne kategórie údajov.

6. Citlivé informácie sú informácie spracovávané PEVŠ, ktoré si vzhľadom na svoju povahu vyžadujú zvýšený stupeň ochrany. Určenie informácie ako citlivej je v kompetencii jej vlastníkov alebo ich nadriadených. Citlivé informácie sú povinne označené tak, aby pri manipulácii s nimi (ich posielaní, otváraní dokumentov a pod.) bol používateľ preukázateľne oboznámený so skutočnosťou, že pracuje s citlivými informáciami (napr. označením „citlivé" v záhlaví dokumentu").

7. Interne prístupné informácie sú tie informácie, ktoré sú voľne dostupné pre všetkých zamestnancov PEVŠ (napr. prostredníctvom intranetu), ale nie sú verejné.

8. Za verejné informácie sa považujú tie informácie, ktoré je PEVŠ povinná zverejňovať, zverejnila ich z vlastnej iniciatívy alebo ich získala z verejne dostupných zdrojov.

9. Špeciálne kategórie údajov sú najmä:
   a) osobné údaje (v zmysle zákona č. 122/2013 o ochrane osobných údajov),
   b) údaje tvoriace obchodné tajomstvo,
   c) údaje, ktorých obsahom je duševné vlastníctvo.

10. Vedenie evidencií (najmä zariadenia IKT vo vlastníctve PEVŠ, cudzie zariadenia IKT používané v PEVŠ, dôležité dátové médiá, APV) zabezpečuje oddelenie IT alebo iný poverený zamestnanec PEVŠ.

Článok 5
Bezpečnosť ľudských zdrojov

1. Cieľ tejto oblasti bezpečnosti je redukovať riziká súvisiace s ľudskými chybami, zlyhaniami, zneužitím práv, vedomými alebo nevedomými porušovaniami bezpečnostných zásad.

2. Základné princípy, ktorými sa ciele v oblasti bezpečnosti ľudských zdrojov v podmienkach PEVŠ dosahujú:
   - pri výbere nových zamestnancov musia byť zohľadnené kvalifikačné a osobnostné predpoklady,
   - bezpečnostné zodpovednosti musia byť jasne definované a zahrnuté do pracovných zmlúv,
   - zvyšovanie bezpečnostného povedomia (formou školení, inštruktáží a pod.) musí byť priebežné a kontinuálne,
   - musia byť realizované pravidelné školenia a preškoľovania zamestnancov PEVŠ v oblasti informačnej bezpečnosti.

3. Pred prijatím zamestnanca do pracovného pomeru musí byť preverované jeho personálne pozadie, a to najmä požadovaná úroveň znalostí a skúseností a potvrdenie profesijnej kvalifikácie.

4. Každý zamestnanec PEVŠ musí prejsť primeraným školením týkajúcim sa pracovných postupov súvisiacich s informačnou bezpečnosťou a správneho používania informačných systémov, do ktorých bude mať povolený prístup.

5. Každá oprávnená osoba musí byť poučená v zmysle § 21 zákona č. 122/2013 o ochrane osobných údajov.

6. Zodpovednosti a právomoci zamestnancov PEVŠ musia byť prideľované na základe funkčného zaradenia a typu vykonávanej práce. Zamestnancom musia byť prideľované prístupové práva iba v minimálnom rozsahu, ktorý je ešte postačujúci na vykonávanie pridelených pracovných úloh (princíp „najmenšieho privilégia"). Prístupy musia byť prideľované iba na nevyhnutne potrebnú dobu.

7. Všetci zamestnanci PEVŠ, ako aj zamestnanci ostatných tretích strán musia byť zaviazaní povinnosťou zachovania mlčanlivosti.

8. Zamestnanci musia byť informovaní o svojich zodpovednostiach a právomociach týkajúcich sa dodržiavania informačnej bezpečnosti. Každý zamestnanec, ktorý poruší svoje povinnosti, musí byť postihovaný v rámci procesov disciplinárneho konania.

9. Zamestnancom, s ktorými bol rozviazaný pracovný pomer, musia byť v dostatočnom predstihu odobraté prístupové práva k dôležitým informačným aktívam a zabezpečené vrátenie všetkých pridelených aktív PEVŠ.

Článok 6
Riadenie prístupu v IS

1. Cieľom tejto oblasti bezpečnosti je predchádzať neoprávnenému prístupu a neoprávnenému použitiu IS a zariadení v počítačových sieťach PEVŠ.

2. Základné princípy, ktorými sa ciele v oblasti riadenia prístupu v IS v podmienkach PEVŠ dosahujú:
   - prístup používateľa do IS je možné prideľovať iba v rozsahu nutnom na plnenie jeho pracovných povinností,
   - prideľovanie prístupov je explicitné a rešpektuje filozofiu „všetko čo nie je povolené, je zakázané“,
   - všetci zamestnanci PEVŠ sú viazaní mlčanlivosťou o spracúvaných údajoch, pokiaľ nie je explicitne stanovené inak,
   - interné LAN siete PEVŠ musia byť chránené tak, aby mohli byť považované za dôveryhodné prostredia,
   - interné LAN siete PEVŠ a externé dátové siete musia byť vzájomne oddelené tak, aby bolo možné efektívne riadiť a monitorovať tok dát medzi sieťami.

3. Prístup k dôverným alebo inak citlivým údajom PEVŠ musí byť povolený len na základe jednoznačnej identifikácie a autentifikácie používateľov.

4. Prístup používateľov do IS PEVŠ musí byť založený na princípoch autorizácie.

5. Každému používateľovi musí byť do IS PEVŠ pridelený len taký rozsah prístupových práv, ktorý umožní plnenie pracovných úloh, ale zároveň zabráni vykonávaniu iných neautorizovaných činností (princíp „najmenších privilégií“).

6. Všetky udalosti a aktivity súvisiace s bezpečnosťou musia byť zaznamenávané, sledované a pravidelne vyhodnocované. Neautorizované, neúspešné prístupy alebo prístupy, ktoré sú v rozpore s pravidlami riadenia prístupu v prostredí PEVŠ, musia byť zaznamenané a pravidelne vyhodnocované.

7. Musí byť zabezpečená nezávislosť kontroly auditných záznamov, musí byť aplikované oddelenie rolí medzi osobami, ktoré kontrolu vykonávajú a ktorých aktivity sa sledujú.

8. Na zabezpečenie dôverných a inak citlivých informácií spracovávaných na mobilných prostriedkoch spracovania mimo zabezpečených priestorov PEVŠ musia byť aplikované primerané bezpečnostné opatrenia.

Článok 7
Fyzická bezpečnosť a bezpečnosť prostredia

1. Cieľom tejto oblasti bezpečnosti je minimalizovať riziká neoprávneného fyzického prístupu k aktívam, ich krádeže, zneužitia, ohrozenia vyššou mocou (prírodný živel).

2. Základné princípy, ktorými sa ciele v oblasti fyzickej bezpečnosti a bezpečnosti prostredia v podmienkach PEVŠ dosahujú:

- v priestoroch PEVŠ musia byť vytvorené bezpečnostné zóny všade tam, kde je to potrebné,
- činnosť strážnej služby – ochrana objektov musí byť pravidelne vyhodnocovaná a kontrolovaná,
- mechanické a technické bezpečnostné opatrenia musia byť použité všade tam, kde to je potrebné a opodstatnené.

3. Priestory PEVŠ s dôležitými informačnými aktívami musia byť zaradené do bezpečnostných zón podľa toho, akú úroveň ochrany vyžadujú informácie a zariadenia, ktoré sa v nich nachádzajú. V jednotlivých priestoroch musia byť zavedené primerané bezpečnostné opatrenia, ktoré zabezpečia ich fyzickú ochranu pred neautorizovaným prístupom, poškodením a vplyvmi prostredia.

4. Prístup do bezpečnostných zón a priestorov, v ktorých sa nachádzajú dôležité zariadenia PEVŠ musí byť prideľovaný iba na základe pracovnej potreby a funkčného zaradenia zamestnanca.

5. Prístup k dôležitým zariadeniam musí byť riadený pomocou primeraných mechanických zábranných prostriedkov a technických zabezpečovacích prostriedkov.

6. Priestory, v ktorých sa nachádzajú dôležité zariadenia PEVŠ musia byť v neprítomnosti zamestnancov chránené primeranými bezpečnostnými opatreniami. Každé narušenie ako aj pokus o narušenie bezpečnostného mechanizmu musí byť hlásený, zaznamenaný a vyhodnotený.

7. Pohyb zamestnancov tretích strán v priestoroch, v ktorých sa nachádzajú dôležité zariadenia PEVŠ musí byť riadený a kontrolovaný, týmto osobám môžu byť sprístupnené len tie priestory, ktoré nevyhnutne potrebujú na svoju činnosť alebo vybavenie ich oprávnených požiadaviek.

8. Prístup zamestnancov tretích strán do chránených oblastí s dôležitými zariadeniami PEVŠ je možný iba v sprievode zamestnanca PEVŠ, ktorý je na to oprávnený.

9. Dôležité zariadenia, ktoré podporujú kritické operácie, musia byť zabezpečené pred výpadkami elektrickej energie (napr. prostredníctvom UPS, dieselového generátora).

Článok 8
Riadenie komunikácií a prevádzky IS

1. Cieľom tejto oblasti bezpečnosti je zabezpečiť spoľahlivú a bezpečnú prevádzku IS PEVŠ, predchádzať narušeniam bezpečnosti pri práci s médiami, predchádzať strate, modifikácii alebo zneužitiu informácií pri ich výmene s okolím (napr. zmluvní partneri).

2. Základné princípy, ktorými sa ciele v oblasti riadenia komunikácií a prevádzky IS v podmienkach PEVŠ dosahujú:
   - pracovné postupy musia byť štandardizované,

- pri zmenách v prevádzkovom prostredí (HW, aplikačné programové vybavenie, operačné systémy) nesmie byť podstatným spôsobom narušená prevádzka ani znížená bezpečnosť IS,
- predchádzanie zlyhaniam IS,
- predchádzanie únikom informácií prostredníctvom médií,
- pri výmene údajov sa musí vždy zohľadniť relevantná aplikovateľná legislatíva,
- dôvernosť a integrita pri prenose údajov musí byť zaručená.

3. Musia byť jednoznačne stanovené a udržiavané zodpovednosti a procedúry súvisiace so zabezpečením správy a prevádzky IS a zariadení PEVŠ.

4. Musí byť zabezpečené oddelenie zodpovedností v oblasti vývoja, prevádzky a kontroly IS s cieľom obmedziť riziko zneužitia zariadení a systémov.

5. V prípadoch, kedy spracovanie informácií alebo prevádzka IS a zariadení PEVŠ bude zverená tretím stranám, musia byť prijaté primerané bezpečnostné opatrenia na zabezpečenie ochrany spracúvaných informácií z hľadiska dôvernosti, dostupnosti a integrity.

6. Musí byť stanovený spôsob vytvárania a uchovávania dokumentácie IS. Dokumentácia IS (najmä prevádzková, administrátorská a používateľská) musí byť chránená pred prezradením, krádežou, narušením alebo stratou.

7. Všetky dôležité údaje musia byť zálohované, pre všetky dôležité údaje musia byť spracované plány zálohovania a archivácie, ktoré vychádzajú z požiadaviek na dostupnosť a integritu týchto údajov.

8. Všetka komunikácia medzi internými zabezpečenými sieťami a externými nezabezpečenými sieťami (napr. internet) musí byť zabezpečená firewallom.

9. Všetky pracovné stanice a ostatné zariadenia musia byť chránené adekvátnymi a účinnými bezpečnostnými opatreniami na ochranu pred škodlivým softvérom, bezpečnostné mechanizmy na ochranu pred škodlivým softvérom musia byť pravidelne aktualizované.

10. Všetky zariadenia a systémy musia byť spravované zaškoleným personálom, opravu a servis zariadení môžu vykonávať len autorizovaní zamestnanci PEVŠ alebo zamestnanci zmluvných tretích strán.

11. Zmluvy o údržbe IS a zariadení musia zabezpečiť rýchlu a efektívnu podporu dodávateľa. Ak je to relevantné, musia zmluvy o údržbe obsahovať dohody o dodržiavaní bezpečnostných požiadaviek a zmluvné záväzky dodávateľov týkajúce sa napr. doby odozvy či realizácie opravy.

Článok 9
Nákup, vývoj a údržba IS

1. Cieľom tejto oblasti bezpečnosti je počas vývoja a nasadzovania nových prvkov IT zabezpečiť identifikáciu a implementáciu bezpečnostných opatrení nutných na

bezpečnú prevádzku nových IT a zaistiť, aby projekty IT prebiehali bezpečným spôsobom.

2. Základné princípy, ktorými sa ciele v oblasti nákupu, vývoja a údržby IS v podmienkach PEVŠ dosahujú:
   - súčasťou každého IT projektu musí byť analýza rizík súvisiacich s vývojom a prevádzkovým prostredím nových prvkov IT,
   - pre každý IT projekt musia byť identifikované a špecifikované bezpečnostné požiadavky,
   - súčasťou každého IT projektu musí byť návrh bezpečnostných testov a návrh formy overenia dostatočnosti bezpečnosti nových prvkov IT pred ich zavedením do rutinnej prevádzky,
   - súčasťou každého IT projektu musí byť špecifikácia rolí, ktoré budú vykonávať údržbu nových prvkov IT po ich zavedení do rutinnej prevádzky,
   - súčasťou každého IT projektu musí byť vypracovanie príslušnej projektovej dokumentácie.

3. Prostredia na vývoj a testovanie systémov a produkčné prostredie musia byť fyzicky aj logicky oddelené. IS alebo ich časti sa môžu nasadiť do prevádzkového prostredia až po ich dôkladnom otestovaní.

4. Na testovanie môžu byť použité len databázy neobsahujúce osobné údaje, resp. obsahujúce anonymizované osobné údaje. V opačnom prípade musí byť použitie osobných údajov na testovanie schválené vedením PEVŠ a musí byť zabezpečená dostatočná ochrana týchto údajov.

5. Pri zabezpečovaní vývoja IS tretími stranami musia byť podmienky výkonu prác ako aj bezpečnostné požiadavky zachytené v zmluve s treťou stranou.

6. Zamestnanci PEVŠ ani externí dodávatelia nesmú svojvoľne zasahovať do konfigurácie prevádzkovaných systémov a zariadení, všetky realizované zmeny musia byť autorizované vlastníkom aktív, všetky zmeny musia byť zdokumentované v prevádzkovej dokumentácii.

7. Všetky zmeny v IS musia byť predmetom formálneho zmenového konania, výber nových zariadení a systémov musí byť vykonaný na základe stanovených akceptačných kritérií, ktorých súčasťou musia byť aj bezpečnostné požiadavky.

8. Súčasťou každého IT projektu musí byť vypracovanie príslušnej projektovej dokumentácie, najmä prevádzkovej, administrátorskej a používateľskej dokumentácie.

Článok 10
Bezpečnosť v spolupráci s tretími stranami

1. Cieľom tejto oblasti bezpečnosti je zabezpečiť ochranu aktív PEVŠ, ku ktorým majú prístup zamestnanci tretích strán.

2. Základné princípy, ktorými sa ciele v oblasti bezpečnosti v spolupráci s tretími stranami v podmienkach PEVŠ dosahujú:

- prístup tretích strán ku aktívam PEVŠ je možný len na základe zmluvného vzťahu,
- všetky prístupy tretích strán ku aktívam PEVŠ musia byť zdokumentované,
- všetky prístupy tretích strán ku aktívam PEVŠ musia byť pravidelne monitorované a preskúmavané.

3. Požiadavky informačnej bezpečnosti na zníženie rizík spojených s prístupmi tretích strán ku aktívam PEVŠ musia byť komunikované a odsúhlasené s treťou stranou a formálne zdokumentované.

4. Zmluvy s tretími stranami musia byť vypracované pred udelením prístupu tretím stranám k aktívam PEVŠ, aby sa zabránilo nedorozumeniam týkajúcich sa povinností obidvoch strán a aby sa splnili všetky relevantné požiadavky informačnej bezpečnosti.

5. Služby tretích strán je potrebné pravidelne monitorovať, preskúmavať, prípadne uskutočňovať audity úrovne služieb poskytovaných tretími stranami.

6. Zmeny v ustanoveniach služieb musia byť riadené, berúc do úvahy kritickosť príslušných informačných systémov a procesov a opakovaného ohodnotenia rizík vyplývajúcich so spolupráce s treťou stranou.

Článok 11
Zvládanie bezpečnostných incidentov

1. Cieľom tejto oblasti bezpečnosti je zabezpečiť nahlasovanie bezpečnostných incidentov spôsobom, ktorý umožní včasnú reakciu vedúcu k náprave a k minimalizácii škôd a zaistiť účinný prístup k zvládaniu identifikovaných bezpečnostných incidentov.

2. Základné princípy, ktorými sa ciele v oblasti zvládania bezpečnostných incidentov v podmienkach PEVŠ dosahujú:
   - bezpečnostné incidenty musia byť nahlasované definovaným spôsobom okamžite bez zbytočných prieťahov,
   - všetci zamestnanci PEVŠ a súvisiace tretie strany sú povinné definovaným spôsobom bezodkladne hlásiť akékoľvek zistenia alebo podozrenia na bezpečnostné slabiny v IS PEVŠ,
   - musia byť definované a zavedené jasné postupy pre zvládanie bezpečnostných incidentov,
   - pre prípady legislatívneho pokračovania riešenia bezpečnostného incidentu musí byť zaistené zhromažďovanie dôkazov.

3. Kontaktná osoba pre nahlasovanie bezpečnostných incidentov súvisiacich s informačnou bezpečnosťou v prostredí PEVŠ je:
   - Vedúci oddelenia IT.

4. Zamestnanci PEVŠ, zmluvní partneri PEVŠ ako aj externí používatelia IS PEVŠ v pozícii tretej strany sú povinní:

- ohlásiť svoje poznatky alebo vážne podozrenia o výskyte bezpečnostného incidentu súvisiaceho s IS PEVŠ vedúcemu oddelenia IT prípadne svojmu nadriadenému pracovníkovi,
- zabezpečiť náležité zdokumentovanie svojich zistení a časových údajov pre potreby evidencie a vyhodnocovania bezpečnostného incidentu,
- nepodnikať svojvoľne žiadne nápravné kroky.

5. Pri zaznamenaní bezpečnostnej udalosti, vyhodnotí určený zamestnanec oddelenia IT dostupné informácie a rozhodne či:
   - ide o falošný poplach/neopodstatnené podozrenie na bezpečnostný incident,
   - bol zistený bezpečnostný nedostatok systému (napr. chýbajúca bezpečnostná záplata, nesprávne konfiguračné nastavenie, chýbajúci antivírový softvér),
   - je opodstatnené podozrenie na bezpečnostný incident.

6. V prípade podozrenia, že zistený incident je prejavom cielenej aktivity voči PEVŠ a jej aktívam, informuje vedúci oddelenia IT nasledovné osoby:
   - štatutárny zástupca PEVŠ,
   - zástupca zmluvnej tretej strany zabezpečujúcej údržbu IKT dotknutých incidentom.

7. Podľa závažnosti zistení a vyhodnotených informácií je potrebné rozhodnúť o prípadnom spôsobe informovania orgánov činných v trestnom konaní. Pokiaľ dôjde k medializácii bezpečnostného incidentu, informácie o jeho príčinách a postupe riešenia je potrebné bezodkladne poskytnúť aj štatutárnemu zástupcovi PEVŠ a hovorcovi PEVŠ.

8. V prostredí PEVŠ je potrebné viesť interný register bezpečnostných incidentov, v ktorom sa evidujú všetky záznamy a informácie o riešení ohlásených bezpečnostných incidentov súvisiacich s IS PEVŠ.

9. Podľa závažnosti bezpečnostného incidentu je potrebné formálne sumarizovať a vyhodnotiť:
   - príčiny vzniku bezpečnostného incidentu,
   - navrhnuté opatrenia na jeho odstránenie,
   - dopady bezpečnostného incidentu na ďalší chod a bezpečnosť IS PEVŠ,
   - minimalizovanie možností opakovania výskytu bezpečnostného incidentu.

10. Ak príčinou incidentu alebo spôsobených škôd bolo porušenie pracovnej disciplíny zo strany zamestnanca PEVŠ, ďalšie konanie sa riadi disciplinárnym konaním definovaným v pracovnom poriadku PEVŠ.

Článok 12
Riadenie kontinuity činností IS

1. Cieľom tejto oblasti bezpečnosti je zabezpečiť funkčnosť procesov závislých na IS počas výpadkov IS a včasné zotavenie sa z výpadku IS.

2. Základné princípy, ktorými sa ciele v oblasti riadenia kontinuity činností IS v podmienkach PEVŠ dosahujú sú:

- musia byť definované priority obnovy pri globálnom výpadku IS,
- musia byť spracované náhradné postupy práce počas výpadku IS,
- musia byť spracované postupy obnovy funkčnosti jednotlivých IS pri ich výpadku (napr. vo forme havarijných plánov).

3. Pre potreby zabezpečenia kľúčových činností závislých od IS počas výpadkov IS musia byť spracované havarijné plány IS a postupy náhradného výkonu činností.

4. Havarijné plány IS a postupy náhradného výkonu činností sú dôverné materiály, musia byť uložené a chránené tak, aby k nim bol umožnený prístup len pre oprávnené osoby.

5. Havarijné plány IS musia byť v pravidelných intervaloch kontrolované a testované.

6. Všetky záložné a archívne médiá musia byť uložené v geograficky oddelených lokalitách, prístup k nim musí byť obmedzený iba pre oprávnené osoby a musia byť v pravidelných intervaloch testované.

Článok 13
Súlad s požiadavkami

1. Cieľom tejto oblasti bezpečnosti je vyvarovať sa porušeniam legislatívnych prvkov trestného a občianskeho práva, zákonných a zmluvných povinností a bezpečnostných požiadaviek, pravidelne, efektívne a objektívne kontrolovať dodržiavanie a napĺňania bezpečnostnej politiky IS.

2. Základné princípy, ktorými sa ciele v oblasti dosahovania súladu s požiadavkami v podmienkach PEVŠ dosahujú sú:
   - všetky legislatívne a zmluvné požiadavky s dopadmi na IS musia byť priebežne identifikované a zdokumentované,
   - opatrenia a zodpovednosti za naplnenie legislatívnych požiadaviek musia byť zdokumentované a zavedené do praxe,
   - výkon vnútornej kontroly musí pokrývať aj kontrolu dodržiavania ustanovení tejto bezpečnostnej politiky IS.

3. Na aktívach PEVŠ môže byť nainštalovaný a používaný softvér len v súlade s jeho licenčnými podmienkami. PEVŠ nenesie zodpovednosť za obsah a aktivitu súkromných počítačov a iných súkromných zariadení študentov, zamestnancov a iných osôb.

4. Spracovanie osobných údajov podlieha zákonu o ochrane osobných údajov, za jeho dosahovanie zodpovedá zodpovedná osoba poverená dohľadom nad ochranou osobných údajov v PEVŠ.

5. Musí byť vykonávaný pravidelný audit stavu informačnej bezpečnosti v PEVŠ, auditná činnosť prebieha formou interných alebo externých auditov so zameraním na jednotlivé oblasti bezpečnosti IS.

Článok 14
Záverečné ustanovenia

1. Tento vnútorný predpis – smernica rektora č. 4/2015 Bezpečnostná politika informačných systémov na Paneurópskej vysokej škole nadobúda platnosť a účinnosť dňa 1. apríla 2015.

V Bratislave dňa 31.3.2015

RNDr. Michal Mutňanský
riaditeľ PEVŠ n. o.,

Prof. JUDr. Ján Svák, DrSc.,
rektor PEVŠ