Vnútorné predpisy
Univerzity Komenského v Bratislave

Vnútorný predpis č. 12/2009

Smernica rektora
Univerzity Komenského v Bratislave,

ktorou sa upravuje bezpečnostná politika integrovaného informačného a komunikačného systému Univerzity Komenského v Bratislave

Ročník 2009

Obsah

Rektor Univerzity Komenského v Bratislave (ďalej len „UK“ alebo „univerzita“) vydal dňa 10. novembra 2009 na základe čl. 10 ods. 3 Organizačného poriadku UK túto smernicu, ktorou sa upravuje bezpečnostná politika integrovaného informačného a komunikačného systému UK (ďalej len „smernica“):

Čl. 1
Predmet úpravy

(1) Táto smernica upravuje bezpečnostnú politiku integrovaného informačného a komunikačného systému UK (ďalej len „IIKS“). Predmetom smernice je stanovenie pravidiel bezpečného správania sa osôb pri ich činnostiach v rámci UK v súvislosti s elektronickým spracovaním informácií na zabezpečenie aktivít univerzity, a to najmä: organizáciu informačnej bezpečnosti, klasifikáciu a riadenie aktív, personálnu bezpečnosť, fyzickú bezpečnosť a bezpečnosť prostredia, komunikačný a prevádzkový manažment, riadenie prístupu, bezpečnosť vývoja softvéru, bezpečnostné incidenty a manažment nepretržitosti činností IIKS.

(2) Úprava bezpečnostnej politiky IIKS v štruktúre podľa odseku 1 je rozpracovaná v prílohe: Bezpečnostná politika IIKS, ktorá je neoddeliteľnou súčasťou tejto smernice.

Čl. 2
Záverečné ustanovenia

(1) Fakulty a ostatné súčasti UK si môžu bezpečnostnú politiku podrobnejšie rozpracovať na svoje podmienky. Bezpečnostná politika IIKS jednotlivých fakúlt a súčastí musí byť v súlade s touto smernicou.

(2) V prípade nesúladu vnútorného predpisu fakulty alebo súčasti UK s touto smernicou, bude rektor UK postupovať v súlade s ustanoveniami čl. 12 Organizačného poriadku UK[1].

(3) Táto smernica nadobúda platnosť a účinnosť 10. novembra 2009.

V Bratislave dňa 10. novembra 2009

doc. PhDr. František Gahér, CSc.
rektor UK

[1] Vnútorný predpis č. 3/2007 Organizačný poriadok UK v znení vnútorného predpisu č. 27/2008.

Príloha k vnútornému predpisu č. 12/2009 Smernici rektora UK

Bezpečnostná politika IIKS Univerzity Komenského v Bratislave

I. ODDIEL
VYMEDZENIE POJMOV

Čl. 1
Použité pojmy a skratky

Aktivity univerzity – vzdelávacie, výskumné, prevádzkové, rozvojové a iné aktivity vykonávané Univerzitou Komenského v Bratislave.

Aktívum – pozri Čl. 17- Definícia aktív.

IT aktívum – aktívum určené na elektronické spracovanie informácií.

Auditovateľnosť – schopnosť zistiť vybrané informácie o aktivitách subjektu.

Autenticita – pravosť, nefalšovanosť, zhoda informácie so skutočnosťou. Napríklad zabezpečenie toho, že osoba je tým, za koho sa vydáva.

Autorizácia – oprávnenie na prístup k aktívu, alebo na vykonávanie činnosti. Proces overovania, zisťovania prístupových práv.

Autorizovaná osoba – osoba, ktorá má oprávnenie na prístup k aktívu alebo na vykonávanie činnosti.

Bezpečnostné požiadavky – pozri Čl. 16 - Požadovaná úroveň informačnej bezpečnosti.

Bezpečnostná politika – tento dokument „Bezpečnostná politika IIKS Univerzity Komenského v Bratislave“.

Bezpečnostné povedomie – základné pravidlá bezpečného vykonávania činností.

Bezpečnosť – vlastnosť objektu alebo subjektu, ktorá určuje mieru jeho ochrany proti možným škodám. Taktiež stav, pri ktorom je riziko poškodenia aktív obmedzené na prijateľnú úroveň. Pozri aj Čl. 10 - Definícia bezpečnosti.

Bezpečnostný incident – udalosť, ktorá bezprostredne ohrozila aktívum alebo činnosť organizácie.

CIT – Centrum informačných technológií Univerzity Komenského v Bratislave.

Dostupnosť – zabezpečenie prístupu k aktívam pre autorizovaných používateľov vtedy, keď je to potrebné.

Dôvernosť – zaistenie toho, že k informáciám majú prístup len tí, ktorí majú na to autorizáciu.

Hrozba – čokoľvek, čo môže spôsobiť škodu. Akcia alebo udalosť, ktorá môže ohroziť bezpečnosť aktíva.

IB – Informačná bezpečnosť.

IIKS – Integrovaný informačný a komunikačný systém Univerzity Komenského v Bratislave.

Informačná bezpečnosť – bezpečnosť informácií a všetkých ostatných aktív informačných technológií a informačných systémov. Informačná bezpečnosť je súčasťou celkovej bezpečnosti.

Informačný systém – súbor technických a programových prostriedkov, záznamových médií, dát a personálu, ktoré spoločnosť používa na spracovanie informácií v určitej oblasti pôsobenia.

Integrita – neporušenosť, celistvosť, presnosť, kompletnosť.

IS – Informačný systém / Informačné systémy.

IT – Informačné technológie.

LAN – Lokálna počítačová sieť (Local Area Network).

Legislatíva – všeobecne záväzné predpisy a vnútorné predpisy UK.

Opatrenia, bezpečnostné opatrenia, ochranné opatrenia – prax, postupy, alebo mechanizmy, ktoré znižujú bezpečnostné riziká.

Osoby – zamestnanci univerzity, študenti univerzity alebo tretie osoby.

Osobné údaje – osobné údaje podľa zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov.

Používateľ – osoba používajúca aktívum.

Produkčný systém – systém nasadený v reálnej prevádzke.

Riziko – potenciálna možnosť, že daná hrozba využije zraniteľnosť aktív a spôsobí tak stratu alebo zničenie aktív.

Správca – osoba, ktorá má na starosti správu, prevádzku, údržbu aktíva.

Spracovanie informácií – manipulácia, uchovávanie, prezentácia, resp. ochrana informácií.

Správca príslušný používateľovi – správca, ktorý spravuje používateľom príslušné aktíva, resp. ktorý má na starosti správu pracoviska, na ktorom používateľ pracuje.

UK – Univerzita Komenského v Bratislave.

Univerzita – Univerzita Komenského v Bratislave.

Zákon o ochrane osobných údajov – zákon č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov.

Zamestnanec – osoba, ktorá má pracovnoprávny vzťah s univerzitou.

II. ODDIEL
BEZPEČNOSTNÁ POLITIKA

Čl. 2
Poslanie bezpečnostnej politiky

Poslaním tejto Bezpečnostnej politiky IIKS na Univerzite Komenského v Bratislave je spolu s ďalšími dokumentmi a vnútornými predpismi UK stanoviť stratégiu a konkrétne pravidlá bezpečného správania sa používateľov pri ich činnostiach v rámci univerzity.

Čl. 3
Vecná a personálna pôsobnosť bezpečnostnej politiky

Bezpečnostná politika sa vzťahuje na aktíva univerzity, ktoré priamo súvisia so spracovaním informácií na zabezpečenie aktivít univerzity. Je záväzná pre všetkých zamestnancov a študentov univerzity a ďalšie osoby, ktoré sa zaviažu ju dodržiavať.

Čl. 4
Vyhlásenie vedenia univerzity o podpore bezpečnostnej politiky

Rektor univerzity schvaľuje túto bezpečnostnú politiku, podporuje ju a realizuje kroky na jej presadzovanie prostredníctvom poverených zamestnancov, najmä príslušného prorektora, riaditeľa CIT a manažéra informačnej bezpečnosti.

Čl. 5
Zodpovednosť za vypracovanie a aktualizáciu bezpečnostnej politiky

Za vypracovanie a aktualizáciu bezpečnostnej politiky univerzity zodpovedá manažér informačnej bezpečnosti (Čl. 12). Štruktúra bezpečnostnej politiky vychádza z medzinárodnej normy ISO/IEC 27002.

Čl. 6
Presadzovanie bezpečnostnej politiky

Bezpečnostná politika je presadzovaná na všetkých úrovniach riadenia univerzity. Procesy súvisiace s realizáciou bezpečnostnej politiky spravidla koordinuje manažér informačnej bezpečnosti. Za súlad každého aktíva s bezpečnostnou politikou a súvisiacimi predpismi zodpovedá správca daného aktíva.

III. ODDIEL
VNÚTORNÉ PREDPISY

Čl. 7
Bezpečnostné smernice

Bezpečnostné smernice sú vnútorné predpisy univerzity, ktoré upravujú požiadavky na bezpečnosť aktív a vybrané zásady informačnej bezpečnosti. Vypracúva ich manažér informačnej bezpečnosti a vydáva ich rektor UK. Nedodržanie bezpečnostných smerníc sa považuje za porušenie bezpečnostnej politiky. Ak nie je uvedené inak, za ich aplikáciu zodpovedajú správcovia príslušných aktív.

Čl. 8
Bezpečnostné príkazy

Bezpečnostné príkazy sú vnútorné predpisy, ktoré majú jednorazový charakter. Vypracúva ich manažér informačnej bezpečnosti za účelom prevencie aktuálnych bezpečnostných hrozieb alebo pri potrebe prijatia konkrétnych bezpečnostných opatrení. Vydáva ich rektor UK ako príkazy rektora. Ich nedodržanie sa považuje za porušenie bezpečnostnej politiky. Ak nie je uvedené inak, za ich aplikáciu zodpovedajú správcovia príslušných aktív.

Čl. 9
Bezpečnostné odporúčania

Bezpečnostné odporúčania sú dokumenty, ktoré vydáva manažér informačnej bezpečnosti za účelom sumarizovania vybraných zásad informačnej bezpečnosti. Nepodliehajú ďalšiemu schvaľovaniu. Ich dodržiavanie je odporúčané.

IV. ODDIEL
ORGANIZÁCIA INFORMAČNEJ BEZPEČNOSTI

Čl. 10
Definícia bezpečnosti

Bezpečnosť znamená zaistenie požadovanej dostupnosti, dôvernosti a integrity aktív. Okrem uvedeného bezpečnosť zahŕňa aj autorizáciu používateľov, autenticitu používateľov a auditovateľnosť aktivít používateľov a systémov.

Čl. 11
Ciele bezpečnosti

Cieľom bezpečnosti na univerzite je najmä:

- chrániť bezpečnosť aktív univerzity,
- chrániť know-how a dobré meno univerzity,
- chrániť aktíva univerzity pred zneužitím,
- umožniť realizáciu aktivít univerzity,
- udržiavať súlad s legislatívou týkajúcou sa informačnej bezpečnosti,

- zvyšovať bezpečnostné povedomie zamestnancov univerzity.

Čl. 12
Manažér informačnej bezpečnosti

(1) Presadzovanie a monitorovanie informačnej bezpečnosti univerzity koordinuje manažér informačnej bezpečnosti. Manažéra informačnej bezpečnosti určuje riaditeľ CIT. V prípade, že pozícia manažéra informačnej bezpečnosti nie je obsadená, jeho práva a povinnosti vykonáva dočasne riaditeľ CIT.

(2) Manažér informačnej bezpečnosti môže v prípade, keď požadované bezpečnostné opatrenie nie je vzhľadom na konkrétny prípad nevyhnutne potrebné na zaistenie dostatočnej úrovne bezpečnosti udeliť jednorazovú výnimku z dodržiavania tejto bezpečnostnej politiky, bezpečnostných smerníc bezpečnostných príkazov alebo bezpečnostných odporúčaní (Čl. 7 až Čl. 9).

Čl. 13
Manažment rizík

Manažment rizík je sústavná činnosť vykonávaná za účelom dosahovania primeranej úrovne bezpečnosti aktív univerzity. Je riadená manažérom informačnej bezpečnosti. Pozostáva z analýzy a riadenia rizík. Z analýzy rizík vyplynú činnosti, ktoré je potrebné realizovať na zvýšenie bezpečnosti aktív (riadenie rizík). Nezávisle od tejto činnosti správcovia aktív musia samostatne zabezpečovať bezpečnosť svojich aktív.

Čl. 14
Analýza rizík

Analýza rizík je pre jednotlivé aktíva realizovaná manažérom informačnej bezpečnosti. Vychádza najmä z nasledovných informácií:

- dopady – následky bezpečnostných incidentov,
- hrozby – sily hrozieb a pravdepodobnosti ich výskytu,
- pravdepodobnosti – pravdepodobnosť, že daná hrozba spôsobí daný dopad.

Čl. 15
Riadenie rizík

Z analýzy rizík vychádza proces riadenia rizík. Proces riadenia rizík pozostáva z realizácie jednej z nasledovných možností pre každé špecifikované riziko:

- Správa rizika – aplikácia, úprava alebo vylepšenie bezpečnostných opatrení.
- Vyhnutie sa riziku, alebo prenos rizika – prenesenie zodpovednosti za riziko alebo zmena konceptu riešenia.
- Akceptovanie rizika – akceptovanie aktuálneho stavu bez zmeny.

Čl. 16
Požadovaná úroveň informačnej bezpečnosti

(1) Úroveň informačnej bezpečnosti aktíva sa považuje za dostatočnú (požadovanú), ak aktívum spĺňa všetky naň kladené bezpečnostné požiadavky.

(2) Bezpečnostné požiadavky sú požiadavky definované:

- legislatívou,
- bezpečnostnou politikou,
- bezpečnostnými smernicami,
- bezpečnostnými príkazmi,
- inou príslušnou dokumentáciou[1], no len tými časťami, ktoré sa týkajú informačnej bezpečnosti daného aktíva.

V. ODDIEL
KLASIFIKÁCIA A RIADENIE AKTÍV

Čl. 17
Definícia aktív

Za aktíva sa považujú najmä informácie a prostriedky, ktoré zabezpečujú ich zber, spracovanie, uchovávanie, ochranu a prezentáciu. Aktívami sú najmä:

- hardvér, dátové nosiče, komunikačné prostriedky, budovy a ich vybavenia,
- informácie/dáta - dokumenty, databázy, zálohy, nastavenia, záznamy,
- softvér,
- osoby.

Čl. 18
Klasifikácia aktív

(1) Z hľadiska bezpečnosti sú aktíva klasifikované a zaradené podľa nasledovných stupňov:

1. chránené,
2. štandardné,
3. nechránené,
4. špeciálne.

1 Napr. prevádzkovými predpismi, havarijnými plánmi, požiarno-poplachovými smernicami.

(2) Klasifikáciu aktíva podľa uvedenej stupnice určuje jeho správca. Manažér informačnej bezpečnosti môže v odôvodnených prípadoch zmeniť klasifikáciu aktíva. Jeden systém môže obsahovať aj časti s rozdielnymi klasifikáciami.

Čl. 19
Chránené aktíva

Chránené aktíva sú aktíva, v prípade ktorých narušenie bezpečnosti spôsobí vážne bezpečnostné dopady v rozsahu celej univerzity, prípadne jej súčasti. Tieto aktíva vyžadujú vysoký stupeň ochrany.

Čl. 20
Štandardné aktíva

Štandardné aktíva sú aktíva, v prípade ktorých narušenie bezpečnosti má dopad len na obmedzenú skupinu používateľov v rámci jednej súčasti univerzity. Tieto aktíva vyžadujú štandardnú ochranu.

Čl. 21
Nechránené aktíva

Nechránené aktíva sú aktíva, ktoré nemusia byť žiadnym spôsobom chránené. Musia byť prijaté opatrenia na to, aby nemohli ohroziť bezpečnosť chránených aktív. Správca môže odmietnuť poskytovať podporu a zabezpečovať funkčnosť nechránených aktív.

Čl. 22
Špeciálne aktíva

Špeciálne aktíva sú aktíva, ktoré svojim charakterom vyžadujú kombináciu vymenovaných stupňov ochrany a prístupových práv. Bezpečnosť týchto aktív musí byť riešená individuálne.

Čl. 23
Zodpovednosť za bezpečnosť aktív

Za bezpečnosť každého aktíva zodpovedá jeho správca. Za dodržiavanie bezpečnostnej politiky v rámci svojej činnosti zodpovedajú zamestnanci UK, študenti UK a všetky tretie osoby na základe zmluvných vzťahov s UK.

VI. ODDIEL
PERSONÁLNA BEZPEČNOSŤ

Čl. 24
Prijímanie zamestnanca

Každý zamestnanec univerzity musí mať jednoznačne vymedzené práva a povinnosti vyplývajúce z jeho pracovnoprávneho vzťahu a musí s nimi byť oboznámený. Na pracovné zaradenie správcu alebo iného zamestnanca, ktorý je v rámci svojej pracovnej činnosti zodpovedný za bezpečnosť IT aktív môže byť prijatý len uchádzač s dostatočným bezpečnostným povedomím.

Čl. 25
Zácvik používateľov

Používatelia, ktorí pracujú s chránenými aktívami, sú povinní rozvíjať svoje bezpečnostné povedomie, a to najmä prostredníctvom školení základného bezpečnostného povedomia, ktoré iniciuje manažér informačnej bezpečnosti. Príslušní nadriadení zamestnanci zodpovedajú za zaškolenie ich podriadených zamestnancov podľa pokynov manažéra informačnej bezpečnosti.

Čl. 26
Zmena pracovného zaradenia, skončenie pracovného pomeru

Pri každej zmene pracovného zaradenia zamestnanca, pri skončení pracovného pomeru, prípadne pri požiadavke na zmenu prístupových práv vedúci príslušného organizačného útvaru o tom upovedomí správcu príslušného danému pracovisku, ktorý zabezpečí prispôsobenie prístupových práv novému pracovnému zaradeniu. V deň skončenia pracovného pomeru musia byť zamestnancovi odstránené všetky neverejné prístupové práva.

Čl. 27
Zastupovanie

(1) Každý zamestnanec z oblasti IT, ktorého nedostupnosť by mohla vážnejšie ohroziť prevádzku súčasti univerzity, prípadne vykonávanie dôležitej činnosti v rámci univerzity, musí mať za seba určeného zastupujúceho zamestnanca, ktorý ho zastúpi počas jeho nedostupnosti.

(2) Zastupujúci zamestnanec musí byť na danú činnosť dostatočne vyškolený a počas zastupovania musí mať pridelené dostatočné právomoci na výkon zastupovaných úloh. Za zabezpečenie zastupovania zodpovedá príslušný nadriadený zamestnanec.

Čl. 28
Povinnosti používateľov

(1) Pri používaní aktív univerzity zodpovedá každý používateľ za svoju činnosť.

(2) Používatelia sú povinní:

- všestranne chrániť aktíva univerzity,
- chrániť vlastné prístupové práva,

- používať informačné systémy len s vlastným identifikátorom,
- nahlásiť neoprávnené použitie aktíva univerzity,
- nahlásiť im známe bezpečnostné zraniteľnosti aktív univerzity,
- dodržiavať bezpečnostnú politiku, príslušné prevádzkové a bezpečnostné predpisy,
- dodržiavať pokyny príslušných správcov.

(3) Používateľ nesmie:

- neoprávnene manipulovať s aktívami univerzity,
- používať prístupové práva, ktoré mu neprináležia,
- ničiť záznamy o svojej činnosti, falšovať ich alebo brániť ich vytváraniu,
- vyvíjať aktivity za účelom neoprávnenej zmeny prístupových práv, či získania iného privilegovaného stavu,
- vyvíjať aktivity za účelom neoprávneného prístupu k cudzím systémom, neoprávneného prístupu k chráneným informáciám a neoprávneného prístupu k údajom iných používateľov,
- vyvíjať aktivity za účelom zabránenia iným používateľom oprávnene používať aktíva univerzity.

Čl. 29
Komunikácia a spolupráca

(1) Zamestnanci, vedúci organizačných útvarov a správcovia sú povinní navzájom komunikovať o aktuálnych zmenách, potrebách a nejasnostiach, týkajúcich sa im príslušných aktív. Zároveň sú povinní spolupracovať pri ochrane aktív univerzity. Správcovia aktív v rámci dohodnutého spôsobu komunikácie a spolupráce s príslušnými používateľmi zabezpečujú primeranú vlastnú dostupnosť a rýchlosť reakcie na požiadavky používateľov.

(2) Ak zamestnanci alebo študenti univerzity zistia hroziace problémy alebo podozrivé skutočnosti súvisiace s informačnou bezpečnosťou, sú povinní upozorniť na to príslušných správcov aktív alebo nadriadených zamestnancov.

Čl. 30
Prevencia podvodov

(1) Zamestnanec môže prijímať požiadavky na vykonanie pracovných úkonov len od oprávnených osôb.

(2) Pri vykonávaní pracovných úkonov musí zamestnanec dbať na overenie autenticity (overenie, či je osoba naozaj tou, za ktorú sa vydáva) a autorizácie (overenie, či má osoba právo na to, čo žiada) osoby, s ktorou komunikuje.

Čl. 31
Monitoring

Pre potreby zaistenia bezpečnosti, prevádzky alebo rozvoja aktív univerzity môžu byť monitorované aktivity používateľov vykonávané s aktívami univerzity a charakteristika dát prenášaných prostredníctvom aktív univerzity.

Čl. 32
Porušenie bezpečnostnej politiky

(1) Závažné porušenie bezpečnostnej politiky a súvisiacich predpisov sa považuje za porušenie pracovnej disciplíny[2].

(2) V prípade bezpečnostného incidentu, alebo ak je to potrebné na primerané zaistenie bezpečnosti aktíva, môže byť používateľovi odobraný prístup k aktívu.

(3) V prípade porušenia bezpečnostnej politiky zo strany študenta bude takéto konanie považované za disciplinárny priestupok a riešené v súlade s disciplinárnym poriadkom UK[3].

VII. ODDIEL
FYZICKÁ BEZPEČNOSŤ A BEZPEČNOSŤ PROSTREDIA

Čl. 33
Všeobecné zásady

(1) Zamestnanci sú povinní chrániť majetok zamestnávateľa pred poškodením, stratou, zničením a zneužitím a nekonať v rozpore s oprávnenými záujmami zamestnávateľa.

(2) Ak nie je ustanovené inak, za fyzické zabezpečenie priestorov zodpovedá vlastník, resp. správca príslušného objektu.

(3) Univerzita môže monitorovať priestor prístupný verejnosti pomocou videozáznamu alebo audiozáznamu na účely bezpečnosti za podmienok stanovených zákonom o ochrane osobných údajov[4].

(4) Aktíva univerzity môžu byť prevádzkované len v primerane fyzicky zabezpečenom prostredí. Fyzickú bezpečnosť technologických miestností upraví osobitný vnútorný predpis.

(5) Pre neverejné priestory musia byť prijaté opatrenia na zabránenie prístupu neautorizovaných osôb bez dozoru,. Pre verejne dostupné priestory je potrebné prijať účinné opatrenia proti poškodeniu ich vybavenia a majetku, ktorý je v nich umiestnený.

[2] Článok 11 vnútorného predpisu č. 11/2008 Pracovný poriadok Univerzity Komenského v Bratislave.
[3] Vnútorný predpis č. 8/2008 Disciplinárny poriadok Univerzity Komenského v Bratislave pre študentov.
[4] § 10 ods. 7 a § 13 ods. 7 zákona o ochrane osobných údajov.

VIII. ODDIEL
KOMUNIKAČNÝ A PREVÁDZKOVÝ MANAŽMENT

Čl. 34
Všeobecné zásady

(1) Komunikačný a prevádzkový manažment zahŕňa najmä zálohovanie údajov, aktualizáciu a bezpečnostné záplaty, dokumentáciu a nasadzovanie systémov, správu aktív, aspekty prístupu tretích osôb, ochranu informácií.

(2) Prevádzkové aspekty súvisiace s bezpečnosťou, najmä:

- konfigurácie zariadení,
- ochranu voči škodlivému softvéru,
- bezpečnosť počítačových sietí,
- bezpečnosť pracovných staníc,
- bezpečnosť serverov

upravia bezpečnostné smernice.

Čl. 35
Zálohovanie údajov

Programové komponenty, konfigurácie, databázy, používateľské dáta na serveroch a iné dáta potrebné na fungovanie serverov musia byť zálohované tak, aby v prípade zničenia originálnych dát tieto bolo možné obnoviť zo zálohy. Dáta musia byť zálohované na úložisku, ktoré je fyzicky oddelené od úložiska originálnych dát.

Čl. 36
Aktualizácie a bezpečnostné záplaty

Pre každý softvér, ktorého novoobjavená zraniteľnosť by mohla spôsobiť závažný bezpečnostný incident musí byť zabezpečená aplikácia bezpečnostných záplat v primeranom čase. Ak toto nie je zabezpečené automaticky, správca softvéru je povinný sledovať informácie o novoobjavených zraniteľnostiach príslušného softvéru a bezpečnostné záplaty aplikovať manuálne.

Čl. 37
Dokumentácia systémov

(1) Pre každý informačný systém UK musí byť vypracovaná dokumentácia, ktorá by mala obsahovať minimálne:

- technickú dokumentáciu – popis štruktúry, funkcií, spôsobu fungovania systému a ďalšie informácie potrebné pre správcov systému a pre vývojových pracovníkov,
- používateľskú dokumentáciu – návody na použitie a prevádzku systému a ďalšie informácie potrebné pre používateľov systému,
- havarijné plány – návody na obnovu systému po havárii, najmä návody na ošetrenie porúch a reakcie na incidenty, ktoré aktívu pravdepodobne hrozia,
- dokumentáciu vyžadovanú platnou legislatívou.

(2) Do dokumentácie musia byť zapracované aj bezpečnostné aspekty. Informačné systémy môžu byť používané len v súlade s ich dokumentáciou. Dokumentácia musí byť priebežne prispôsobovaná zmenám v systémoch.

Čl. 38
Nasadzovanie systémov

(1) Systém môže byť nasadený do produkčnej prevádzky, až keď spĺňa všetky nasledovné požiadavky:
- má aplikované dostatočné bezpečnostné opatrenia,
- je dostatočne otestovaný,
- má vypracovanú príslušnú dokumentáciu,
- má presne stanovené povinnosti a zodpovednosti zúčastnených osôb,
- má stanovených a vyškolených správcov s dostatočnými právomocami,
- je v súlade s bezpečnostnou politikou a ostatnými bezpečnostnými požiadavkami,
- prešiel auditom informačnej bezpečnosti.

(2) Pri nasadzovaní systémov je potrebné zohľadniť požiadavky správcov všetkých aktív, ktoré systém svojou činnosťou priamo ovplyvňuje.

Čl. 39
Správa aktív

(1) Každé IT aktívum musí mať priradeného jedného hlavného a aspoň jedného záložného správcu. Správcovia môžu manipulovať s aktívami univerzity len na zabezpečenie prevádzky, rozvoja alebo bezpečnosti aktív univerzity.

(2) Vedenie príslušnej súčasti univerzity zabezpečí pre správcu dostatočné práva a informácie na zaistenie správy a bezpečnosti aktív. Správca musí byť informovaný o všetkých relevantných zmenách, ktoré sa týkajú ním spravovaných aktív.

(3) Spôsob určenia správcov IT aktív na UK určuje osobitný predpis[5].

[5] Opatrenie rektora UK č. 29/2002 - Organizačný a prevádzkový poriadok IIKS UK.

(4) Ak nie je stanovené inak, technický správca IIKS príslušnej fakulty, resp. súčasti univerzity je zároveň správcom všetkých IT aktív danej fakulty, resp. súčasti univerzity. Technický správca IIKS príslušnej fakulty, resp. súčasti univerzity môže ďalej poveriť jemu podriadených zamestnancov správou IT aktív. Títo zamestnanci sa potom v rozsahu poverenia stávajú správcami daných aktív.

(5) Správcovia IT aktív sú zodpovední za:

- prevádzku a bezpečnosť IT aktív,
- vytvorenie a aktualizáciu príslušnej dokumentácie,
- súlad IT aktív s bezpečnostnou politikou, ďalšími bezpečnostnými požiadavkami a prevádzkovými predpismi,
- reagovanie na požiadavky v súvislosti s IT aktívami,
- sledovanie stavu IT aktív a upozorňovanie nadriadených na zistené nedostatky a hroziace problémy.

(6) V prípade zistenia bezpečnostnej zraniteľnosti IT aktíva je jeho správca povinný bezodkladne prijať bezpečnostné opatrenia potrebné na zamedzenie zneužitia zistenej zraniteľnosti.

Čl. 40
Bezpečnosť prístupu tretích osôb

(1) Treťou osobou je externý dodávateľ alebo iná osoba, ktorá nie je zamestnancom univerzity a ktorá má nadštandardné prístupové práva umožňujúce ohroziť bezpečnosť aktív univerzity. S treťou osobou musí byť uzatvorený zmluvný vzťah.

(2) V rámci zmluvného vzťahu medzi UK a treťou osobou je potrebné upraviť aj ochranu aktív univerzity. Zamestnanec, ktorý je zodpovedný za realizáciu spolupráce s treťou osobou, musí dbať na ochranu aktív, ku ktorým má tretia osoba nadštandardné prístupové práva.

(3) Tretia osoba môže mať len také nadštandardné prístupové práva, ktoré potrebuje na plnenie práv a povinností vyplývajúcich zo zmluvného vzťahu s univerzitou. Po skončení zmluvného vzťahu musia byť všetky nadštandardné prístupové práva takej osobe odobraté.

Čl. 41
Monitorovanie a záznam aktivít

(1) Správcovia informačných systémov zabezpečia vytváranie, zber, uchovávanie a ochranu auditných záznamov aktivít informačných systémov (najmä prístupov používateľov) v primeranom rozsahu.

(2) Stav dôležitých prvkov informačných systémov musí byť automaticky monitorovaný a vyhodnocovaný tak, aby sa zabezpečilo včasné informovanie o hroziacich problémoch.

(3) Univerzita má právo monitorovať používanie svojich aktív používateľmi vrátane akejkoľvek elektronickej komunikácie, ktorá prechádza cez aktíva univerzity.

IX. ODDIEL
RIADENIE PRÍSTUPU

Čl. 42
Všeobecné zásady

(1) Jednotlivé aktíva majú definované pravidlá prístupov v rámci ich prevádzkových predpisov alebo inej príslušnej dokumentácie v súlade s ustanovením Čl. 37.

(2) Ak tieto nie sú definované, prístupové práva k danému aktívu určuje jeho správca.

(3) Manažér informačnej bezpečnosti môže na základe informácií od správcu daného aktíva udeliť výnimku z prístupových práv k danému aktívu.

(4) Prideľovanie prístupových práv sa riadi týmito všeobecnými zásadami:

- Pre chránené aktíva platí pravidlo minimálnych prístupových práv. Chránení používatelia majú len prístupy, ktoré nevyhnutne potrebujú a len na dobu nevyhnutne potrebnú na vykonávanie činností v prospech univerzity.
- Štandardné aktíva majú len obmedzený prístup k chráneným aktívam a málo obmedzený prístup k verejným systémom.
- Nechránené aktíva majú minimálne obmedzený prístup k verejným systémom a maximálne obmedzený prístup k chráneným aktívam.

(5) V odôvodnených prípadoch môže správca, resp. manažér informačnej bezpečnosti k príslušnému IT aktívu prideliť aj väčšie prístupové práva ako nevyhnutne potrebné, avšak nesmie sa tým znížiť bezpečnosť aktív univerzity.

Čl. 43
Vzdialený prístup

Vzdialený prístup k informačným systémom univerzity sa riadi pravidlami pre dané informačné systémy.

X. ODDIEL
BEZPEČNOSŤ VÝVOJA SOFTVÉRU

Čl. 44
Všeobecné zásady

(1) Pri vývoji softvéru je potrebné zohľadniť bezpečnosť jeho vývoja aj neskoršej prevádzky. Vývojoví pracovníci zabezpečia kompenzáciu známych bezpečnostných slabín použitých komponentov, programovacích jazykov a slabín typických pre podobné

systémy. Pred začatím vývoja dohodnú stratégiu ochrany zdrojových kódov a dokumentácie a prijmú opatrenia na ich ochranu zodpovedajúcu dohodnutej stratégii. Úroveň ochrany dôvernosti a integrity vývojových systémov musí zodpovedať minimálne zamýšľanej úrovni ochrany systému po jeho uvedení do produkčnej prevádzky.

(2) Pri vývoji a testovaní sa okrem nevyhnutných prípadov nepoužijú chránené informácie. Ak sa používajú, ich dôvernosť musí byť chránená v súlade s požiadavkami na produkčné systémy.

(3) Ak to nie je nutné, vývoj ani testovanie (s výnimkou testovacej prevádzky) neprebieha na produkčných systémoch.

Čl. 45
Dokumentácia

Nevyhnutnou súčasťou vytvoreného programu je technická dokumentácia umožňujúca ďalším oprávneným osobám pokračovať v jeho vývoji, prípadne realizovať požadované zmeny.

XI. ODDIEL
BEZPEČNOSTNÉ INCIDENTY

Čl. 46
Všeobecné zásady

(1) V prípade existujúceho alebo bezprostredne hroziaceho bezpečnostného incidentu sú správcovia aktív povinní v rámci svojich kompetencií bezodkladne podnikať kroky nevyhnutné na ochranu pred nim alebo zmiernenie jeho dopadov.

(2) Zamestnanci aj študenti univerzity sú povinní bezodkladne nahlásiť závažné bezpečnostné incidenty alebo iné podozrivé skutočnosti, ktoré sa bezprostredne týkajú aktív univerzity príslušnému nadriadenému zamestnancovi, prípadne správcovi dotknutého aktíva.

(3) Správca príslušného aktíva posúdi závažnosť incidentu a v prípade reálneho podozrenia, že ide o závažný bezpečnostný incident, okamžite oznámi zistené skutočnosti manažérovi informačnej bezpečnosti.

(4) Manažér informačnej bezpečnosti zabezpečí:

1. prešetrenie daného incidentu,
2. vyvodenie dôsledkov,
3. aplikáciu primeraných bezpečnostných opatrení.

(5) Ak ide o závažný bezpečnostný incident, manažér informačnej bezpečnosti bezodkladne informuje riaditeľa CIT. Osoby súvisiace s bezpečnostným incidentom sa pre potreby vyšetrovania incidentu riadia pokynmi manažéra informačnej bezpečnosti.

(6) Tento oddiel sa nevzťahuje na incidenty, ktoré sú zjavne prevádzkového charakteru (napr. náhodné poruchy zariadení).

Čl. 47
Klasifikácia bezpečnostných incidentov

Jednotlivé bezpečnostné incidenty klasifikuje manažér informačnej bezpečnosti, riaditeľ CIT alebo príslušný prorektor UK. Ak nie je povedané inak, platí:

1. Bezpečnostný incident je považovaný za závažný, ak je jeho dopadom:
   - únik databázy chránených informácií,
   - strata dostupnosti alebo integrity centrálne na UK poskytovanej služby,
   - narušenie dobrého mena univerzity,
   - iná skutočnosť analogickej závažnosti.

2. Bezpečnostný incident má nízku závažnosť, ak jeho dopad postihne len úzku skupinu osôb a príslušná fakulta, súčasť, resp. rektorát UK je ako celok naďalej schopný vykonávať svoje zvyčajné aktivity.

3. Všetky ostatné bezpečnostné incidenty sú považované za stredne závažné.

XII. ODDIEL
MANAŽMENT NEPRETRŽITOSTI ČINNOSTI

Čl. 48
Všeobecné zásady

(1) Univerzita má geograficky oddelené dátové centrá. Dôležité informačné systémy musia byť v primeranom rozsahu odolné voči výpadku celého jedného dátového centra.

(2) Nepretržitosť prevádzky informačných systémov univerzity zabezpečia príslušní správcovia prostredníctvom technických opatrení:

- redundancia dôležitých aktív,
- zálohovanie informácií,
- zastupiteľnosť správcov,
- znižovanie rizika výpadku služieb,
- monitoring bezpečnostných incidentov a včasné varovanie pred nimi,
- pripravenosť na obnovenie činnosti po havárii IT.

XIII. ODDIEL
DODRŽIAVANIE VŠEOBECNE ZÁVÄZNÝCH PRÁVNYCH PREDPISOV SR A VNÚTORNÝCH PREDPISOV UK

Čl. 49
Súlad so zákonnými požiadavkami

(1) Všeobecne záväzné právne predpisy SR sú nadradené všetkým vnútorným predpisom univerzity vrátane tejto smernice.

(2) Manažér informačnej bezpečnosti iniciuje kroky na zaistenie súladu so všeobecne záväznými právnymi predpismi SR v oblasti informačnej bezpečnosti.

(3) Manažér informačnej bezpečnosti vytvára a priebežne aktualizuje zoznam legislatívnych požiadaviek kladených na bezpečnosť informačných systémov univerzity.

Čl. 50
Legálny softvér

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

Čl. 51
Ochrana osobných údajov

Spracovanie osobných údajov podlieha zákonu o ochrane osobných údajov. V zmysle bezpečnostnej politiky osobné údaje patria do kategórie chránených aktív.

Čl. 52
Bezpečnostné audity

(1) Dodržiavanie bezpečnostných požiadaviek je overované najmä prostredníctvom auditov informačnej bezpečnosti, ktoré koordinuje manažér informačnej bezpečnosti.

(2) Manažér informačnej bezpečnosti má za týmto účelom právo na prístup k potrebným informáciám, ktoré sa týkajú bezpečnosti aktív univerzity.

(3) Audit pozostáva najmä z kontroly plnenia bezpečnostných požiadaviek kladených na príslušné aktíva. Pozri Čl. 14 - Analýza rizík.