Vnútorné predpisy
Univerzity Komenského v Bratislave

Vnútorný predpis č. 2/2011

Smernica rektora
Univerzity Komenského v Bratislave,

ktorou sa upravujú pravidlá informačnej bezpečnosti Univerzity Komenského v Bratislave

Ročník 2011

Obsah

ODDIEL I Všeobecné ustanovenia 3
Čl. 1 Predmet úpravy 3
Čl. 2 Použité pojmy a skratky 3
Čl. 3 Bezpečnostná klasifikácia 5
Čl. 4 Nechránené systémy 6
Čl. 5 Neošetrené nastavenia 6
Čl. 6 Bezpečné heslo 6
Čl. 7 Spracovanie osobných údajov 6
Čl. 8 Zálohovanie dát 7
Čl. 9 Aplikácia bezpečnostných záplat 7
Čl. 10 Kritické služby 8

ODDIEL II Bezpečnosť pracovných staníc 8
Čl. 11 Všeobecné zásady 8
Čl. 12 Správa pracovných staníc 10
Čl. 13 Zoznamy povoleného a zakázaného softvéru 10

ODDIEL III Bezpečnosť počítačových sietí 10
Čl. 14 Sieťové bezpečnostné zóny 10
Čl. 15 Sieťové prístupové práva 10
Čl. 16 Nastavenia aktívnych sieťových zariadení 11
Čl. 17 Bezdrôtové siete 12
Čl. 18 Záznam 12

ODDIEL IV Bezpečnosť serverov 13
Čl. 19 Všeobecné zásady 13

ODDIEL V Fyzická bezpečnosť 14
Čl. 20 Všeobecné zásady 14

ODDIEL VI Povinnosti používateľov 15
Čl. 21 Všeobecné zásady 15
Čl. 22 Chránené informácie 15
Čl. 23 Heslá 16
Čl. 24 Pracovná stanica 16
Čl. 25 Zneužívanie počítačovej siete UK 17
Čl. 26 Kancelária 17
Čl. 27 Komunikácia 17
Čl. 28 Sankcie 18
Čl. 29 Povinnosti správcov 19

ODDIEL VII Záverečné ustanovenia 19

Čl. 30 19

Príloha č. 1: Žiadosť o odstránenie bezpečnostných nastavení pracovnej stanice

Rektor Univerzity Komenského v Bratislave (ďalej len „UK“ alebo „univerzita“) vydal dňa 26. januára 2011 na základe čl. 10 ods. 3 Organizačného poriadku UK túto smernicu, ktorou sa upravujú pravidlá informačnej bezpečnosti UK (ďalej len „smernica“):

ODDIEL I
VŠEOBECNÉ USTANOVENIA

Čl. 1
Predmet úpravy

Táto smernica upravuje pravidlá a podmienky bezpečného používania a bezpečnej správy informačných systémov na UK; vymedzuje bezpečnosť pracovných staníc, počítačových sietí a serverov UK, upravuje povinnosti používateľov informačných systémov, povinnosti správcov informačných systémov a ďalšie práva a povinnosti súvisiace so zabezpečením informačnej bezpečnosti.

Čl. 2
Použité pojmy a skratky

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.

Bezpečnostná politika – Bezpečnostná politika Univerzity Komenského v Bratislave - vnútorný predpis UK č. 12/2009.

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.

Bezpečnostný incident – udalosť ktorá bezprostredne ohrozila aktívum alebo činnosť univerzity v rozpore s platnou bezpečnostnou politikou.

CePIT – Centrum podpory Informačných Technológií Univerzity Komenského v Bratislave.

CIT – Centrum informačných technológií Univerzity Komenského v Bratislave.

Chránené informácie – najmä databázy osobných údajov a ďalšie informácie, ktoré správca označí za chránené.

Chránená pracovná stanica – pracovná stanica správcom označená ako chránená. Musí spĺňať požiadavky oddielu II tejto smernice.

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

Dôvernosť – zabezpečenie 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.

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 sa používajú 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.

Patch-panel – panel sieťových zásuviek.

Perióda zálohovania – časový interval medzi časmi vytvárania dvoch po sebe nasledujúcich záloh dát z toho istého systému.

Používateľ – osoba používajúca aktívum.

Pracovná stanica – počítač určený na priame fyzické používanie používateľom.

Produkčný systém – systém, ktorý zabezpečuje prevádzku služieb a zároveň neslúži ako záložný, vývojový ani testovací systém pre dané služby.

Rack – technologická skriňa.

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, respektíve ochrana informácií.

Správca príslušný používateľovi – správca, ktorý spravuje používateľom príslušné aktíva, respektíve 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.

Switch – sieťový prepínač.

Router – sieťový smerovač.

Firewall – sieťový filter.

VPN server – server poskytujúci pripojenie na virtuálnu privátnu sieť.

Fakulta – fakulta UK podľa čl. 9 ods. 2 a 3 Štatútu UK a podľa prílohy č. 2, tabuľky 1 Štatútu UK.

Samostatne hospodáriace súčasti – súčasti UK podľa prílohy č. 2, tabuľky 2 písm. B) Štatútu UK.

Štatút UK – vnútorný predpis č.10/2008 Štatút Univerzity Komenského v Bratislave v znení dodatku č. 1.

Čl. 3
Bezpečnostná klasifikácia

(1) V súlade s bezpečnostnou politikou môže byť aktívum klasifikované jedným zo stupňov:

a) chránené,
b) štandardné,
c) nechránené,
d) špeciálne.

(2) Pracovné stanice, na ktorých prebieha spracovanie osobných údajov sú klasifikované ako chránené. Klasifikáciu ostatných pracovných staníc určuje ich správca.

(3) Ak správca neurčí inak, pracovné stanice, ktoré sú majetkom univerzity sú klasifikované ako štandardné. Ak správca neurčí inak, pracovné stanice, ktoré nie sú majetkom univerzity sú klasifikované ako nechránené.

(4) Správca zmení klasifikáciu pracovnej stanice používateľa na nechránenú na základe žiadosti používateľa, ak sú splnené všetky nasledovné podmienky:

a) používateľ potrebuje odstrániť bezpečnostné opatrenia na vykonávanie svojich pracovných povinností a túto skutočnosť doloží písomným potvrdením svojho nadriadeného,
b) používateľ má dostatočné bezpečnostné povedomie, dokáže zaistiť bezpečnosť pracovnej stanice a dokáže zabrániť tomu, aby sa pracovná stanica stala zdrojom útoku,
c) na pracovnej stanici nebudú spracúvané osobné údaje,
d) technické podmienky to umožňujú,
e) manažér informačnej bezpečnosti nerozhodne inak.

(5) Za bezpečnosť nechránenej pracovnej stanice zodpovedá jej používateľ. Používateľ nechránenej pracovnej stanice stráca nárok na technickú podporu poskytovanú správcom,

týkajúcu sa nechránenej pracovnej stanice. Vzor žiadosti, ktorou používateľ žiada o odstránenie bezpečnostných nastavení pracovnej stanice, tvorí prílohu č.1 tejto smernice.

Čl. 4
Nechránené systémy

Bezpečnostné požiadavky uvedené v tejto smernici sa nevzťahujú na zariadenia, ktoré slúžia ako laboratórne vybavenie a používajú sa výhradne na vedecko-výskumnú činnosť alebo slúžia výhradne ako učebné pomôcky. Tieto zariadenia musia byť technicky zabezpečené tak, aby nemohli ohroziť bezpečnosť ostatných aktív univerzity. Nesmú byť zapojené v chránených sieťach a nesmú byť používané na prístup k osobným údajom.

Čl. 5
Neošetrené nastavenia

Bezpečnostné nastavenia systémov, ktoré nie sú presne stanovené príslušnými predpismi môže určiť manažér informačnej bezpečnosti. Pokiaľ ich neurčil manažér informačnej bezpečnosti, môžu ich určiť správcovia daných systémov.

Čl. 6
Bezpečné heslo

(1) Bezpečné heslo je heslo s minimálnou dĺžkou osem znakov, pričom v ňom musia byť zastúpené aspoň dve z týchto množín: malé písmená, veľké písmená, čísla, iné znaky. Bezpečné heslo nesmie byť ako celok všeobecne známe (tzv. slovníkové) slovo.

(2) Bezpečné heslo si musí používateľ zmeniť aspoň raz ročne.

(3) Autorizácia pomocou bezpečného hesla môže byť nahradená autorizáciou pomocou bezpečného hardvérového autorizačného mechanizmu schváleného manažérom informačnej bezpečnosti.

(4) Komplexnosť a ochrana hesla musí byť primeraná závažnosti dopadu jeho zneužitia. Bezpečné heslo, univerzitné prístupové (tzv. L1) heslo ani univerzitný bezpečnostný kód (tzv. L2 heslo) sa nesmú ukladať ani prenášať v nešifrovanej podobe, s výnimkou distribúcie nových hesiel používateľom.

Čl. 7
Spracovanie osobných údajov

(1) Používatelia môžu na spracúvanie databáz osobných údajov používať len chránené pracovné stanice.

(2) Každý informačný systém spracúvajúci osobné údaje na UK musí byť registrovaný a schválený manažérom informačnej bezpečnosti.

(3) Každý export osobných údajov mimo univerzity, s výnimkou zákonom požadovaných exportov, musí byť schválený manažérom informačnej bezpečnosti, pričom musia byť dodržané ustanovenia zákona o ochrane osobných údajov.

Čl. 8
Zálohovanie dát

(1) Ak nie je uvedené inak, pre všetky informačné systémy platí nasledovná stratégia zálohovania dát:

a) musia byť zálohované všetky používateľské dáta a konfigurácie systémov,
b) musia byť zálohované všetky dáta nevyhnutne potrebné k obnoveniu systému po strate dát daného systému z ich primárnych úložísk,
c) musia byť zálohované programy aj skripty vytvorené alebo modifikované špeciálne pre potreby UK,
d) minimálna perióda zálohovania je sedem dní,
e) zálohy musia byť uchovávané minimálne po dobu dvojnásobku periódy zálohovania,
f) nemusia byť zálohované používateľské dáta, o ktorých boli používatelia informovaní, že nie sú zálohované,
g) nemusia byť zálohované dáta z používateľských pracovných staníc,
h) nemusia byť zálohované dáta zo systémov, ktoré nie sú vo vlastníctve univerzity,
i) nemusia byť zálohované dáta z neprodukčných systémov,
j) zálohy musia byť fyzicky uložené mimo zálohovaných systémov,
k) zálohy chránených aj autorizačných informácií musia byť zašifrované,
l) obnovenie dát zo záloh musí byť otestované pre každý zálohovaný informačný systém.

(2) Správca informačného systému spolu s manažérom informačnej bezpečnosti môžu po vzájomnej dohode stanoviť pre daný systém inú stratégiu zálohovania.

Čl. 9
Aplikácia bezpečnostných záplat

(1) Manažér informačnej bezpečnosti zabezpečí informovanie správcov serverov o bezpečnostných zraniteľnostiach týkajúcich sa im zverených systémov.

(2) Správca musí aspoň raz denne počas pracovných dní sledovať dostupné informácie o aktuálnych bezpečnostných zraniteľnostiach týkajúcich sa jemu zverených systémov.

(3) Kritická zraniteľnosť je zraniteľnosť, ktorej zneužitím je útočník schopný spôsobiť aspoň jeden z nasledovných možných dôsledkov:

a) narušiť dôvernosť chránených informácií,
b) získať kontrolu nad systémom alebo službou,

c) systém alebo službu významne poškodiť.

(4) V prípade kritických zraniteľností systémov zverených správcovi zabezpečí daný správca odstránenie zraniteľnosti najneskôr do konca nasledujúceho pracovného dňa od obdržania informácie o výskyte kritickej zraniteľnosti. Ak nie sú v uvedenej lehote dostupné informácie potrebné na odstránenie zraniteľnosti, zabezpečí odstránenie zraniteľnosti v najkratšom možnom čase.

Čl. 10
Kritické služby

Kritické služby sú najdôležitejšie IT služby potrebné pre zabezpečenie prevádzky univerzity. Okruh kritických služieb určuje riaditeľ CIT.

ODDIEL II
BEZPEČNOSŤ PRACOVNÝCH STANÍC

Čl. 11
Všeobecné zásady

(1) Pracovné stanice klasifikované ako štandardné alebo chránené musia mať aplikované nasledovné bezpečnostné opatrenia a nastavenia:

a) Nastavenie automatickej inštalácie bezpečnostných záplat operačného systému s minimálnou periódou jeden deň.
b) Nainštalovaný certifikát koreňovej certifikačnej autority UK v operačnom systéme, webovom prehliadači aj v klientovi elektronickej pošty.
c) Záznam aktivít počítača (logovanie) vzdialene minimálne na úrovni záznamov o prihlásení a odhlásení používateľa.
d) Vynucovaná komplexnosť hesla minimálne na úrovni bezpečného hesla.
e) Vypnuté automatické zapamätávanie hesiel vo webovom prehliadači.
f) Používateľ nesmie mať práva:
    1. administrátora,
    2. odmietnuť aktualizáciu operačného systému,
    3. meniť nastavenia antivírusu,
    4. zapisovať do iných ako správcom špecifikovaných adresárov a jeho domovského adresára,
    5. spúšťať programy z iných ako správcom špecifikovaných adresárov,
    6. meniť systémové nastavenia rozhraní (okrem prenosných počítačov).
g) Nastavenia špecifické pre OS Windows:
    1. nastavenie automatickej aktualizácie antivírusu s minimálnou periódou jeden deň,

2. zapnutá on-line kontrola všetkých súborov minimálne pri spúšťaní, alebo kontrola lokálnych diskov počítača aspoň raz týždenne,
3. počítač musí byť zaradený do univerzitnej domény,
4. zákaz používania lokálnych kont.

h) Používateľská pracovná stanica nesmie zároveň slúžiť ako server pre iných používateľov.

i) Automatické spúšťanie programov z externých dátových médií (autorun) musí byť vypnuté.

j) Komunikácia medzi klientom a serverom elektronickej pošty pri posielaní aj prijímaní elektronickej pošty musí byť šifrovaná.

k) Zakázané automatické načítavanie komponentov správy elektronickej pošty (najmä obrázkov) z internetových zdrojov pri prehliadaní správy elektronickej pošty.

l) Zákaz bootovania z iných médií ako je primárny pevný disk.

m) Zmeny v BIOS-e chránené heslom.

n) Zapečatený kryt počítača.

o) Automatické zamknutie operačného systému prenosného počítača pri zatvorení displeja.

p) Pomenovanie pracovnej stanice také, aby z NetBIOS mena, DNS mena ani iného verejne sieťovo dostupného identifikátora pracovnej stanice nebolo možné odvodiť meno osoby, ktorej pracovná stanica prislúcha, jej pracovná pozícia ani miestnosť, v ktorej je pracovná stanica fyzicky umiestnená.

(2) Pracovné stanice klasifikované ako chránené musia spĺňať požiadavky uvedené v odseku 1 a navyše musia mať aplikované nasledovné bezpečnostné opatrenia a nastavenia:

a) Používateľ nesmie mať práva odmietnuť reštart, ak je potrebný pre účely aplikácie bezpečnostných záplat. Používateľ môže pozastaviť reštart najdlhšie však do konca pracovnej doby daného dňa.

b) Používateľ nesmie mať práva používať iné ako správcom nainštalované programy.

c) Blokovanie rizikových komponentov webových prehliadačov (napr. ActiveX) okrem správcom špecifikovaných dôveryhodných stránok.

d) Automatické zamknutie operačného systému pri neaktivite používateľa trvajúcej dlhšie ako 20 minút, pri prechode do režimu spánku alebo hibernácie.

(3) Všetky pracovné stanice bez ohľadu na klasifikáciu, ktoré sú pripojené k počítačovej sieti, musia byť nastavené tak, aby odpovedali na ICMP Echo Request (ping).

Čl. 12
Správa pracovných staníc

(1) Softvér môže na počítač inštalovať len jeho správca. Na chránené pracovné stanice môže správca inštalovať používateľom len softvér zo zoznamu povoleného softvéru. Na štandardné pracovné stanice správca nesmie inštalovať používateľom softvér zo zoznamu zakázaného softvéru.

(2) Správca musí pre každú ním spravovanú pracovnú stanicu evidovať minimálne:

a) fyzické adresy sieťových rozhraní,
b) identifikátor sieťovej zásuvky, do ktorej je počítač pripojený,
c) fyzické umiestnenie (budova, číslo miestnosti),
d) mená používateľov, ktorým bola primárne priradená (ak sa nezhodujú s používateľmi v danej miestnosti),
e) bezpečnostnú klasifikáciu.

(3) Správca môže nastavovať len také výnimky z uvedených systémových nastavení štandardných pracovných staníc, ktoré sú nevyhnutne potrebné pre chod regulárnych aplikácií.

Čl. 13
Zoznamy povoleného a zakázaného softvéru

Zoznam povoleného softvéru a zoznam zakázaného softvéru vedie manažér informačnej bezpečnosti. Pridávať a odoberať softvér z týchto zoznamov môžu správcovia vybraní manažérom informačnej bezpečnosti.

ODDIEL III
BEZPEČNOSŤ POČÍTAČOVÝCH SIETÍ

Čl. 14
Sieťové bezpečnostné zóny

Každý sieťový segment musí zodpovedať sieťovej zóne (ďalej len „zóna“). Rozoznávame nasledovné zóny:

a) chránená,
b) štandardná,
c) nechránená,
d) zóna správcov,
e) zóna serverov.

Čl. 15
Sieťové prístupové práva

(1) Príslušnosť zariadenia k zóne určujú tieto pravidlá:

a) Pracovné stanice klasifikované ako chránené prislúchajú k chránenej zóne.
b) Pracovné stanice klasifikované ako štandardné prislúchajú k štandardnej zóne.
c) Pracovné stanice klasifikované ako nechránené prislúchajú k nechránenej zóne.

d) Pracovné stanice správcov prislúchajú k zóne správcov.
e) Servery prislúchajú k zóne serverov.

(2) Pre každú zónu platí, že do nej môžu byť pripojené len:

a) zariadenia, ktoré prislúchajú k danej zóne,
b) zariadenia zabezpečujúce technickú prevádzku danej zóny,
c) sieťové tlačiarne a iné lokálne servery slúžiace výhradne pre danú zónu.

(3) Pracovné stanice môžu byť pripojené len do zóny, ku ktorej prislúchajú a do zóny správcov dočasne pre potreby ich správy.

(4) Ak nie je uvedené inak, sieťová komunikácia medzi rôznymi zónami je zakázaná. Do používateľských zón je dovolený prístup len zo zóny správcov a zo serverov schválených manažérom informačnej bezpečnosti. Správcovia môžu pristupovať ku všetkým nimi spravovaným zariadeniam z príslušnej zóny správcov, aj cez VPN server.

(5) Zamestnanec, ktorého počítač je pripojený k štandardnej zóne, nechránenej zóne alebo k zóne správcov, môže pristupovať k svojmu počítaču vzdialene cez VPN server.

(6) Z chránenej zóny je dovolený prístup len do zóny serverov a do internetu k presne špecifikovaným serverom, respektíve službám (napr. Sofia).

(7) Zo štandardnej a nechránenej zóny je dovolený prístup len do zóny serverov a do internetu s výnimkou explicitne zakázaných služieb a serverov.

(8) Prístup z internetu je dovolený len na presne špecifikované služby do zóny serverov, do ostatných zón je prístup zakázaný. Sieťové prístupové práva na servery určujú správcovia daných serverov.

(9) Pripojenie zariadenia k sieti UK s výnimkou miest určených na pripojenie cudzích zariadení (napr. sieť EduRoam) musí byť schválené príslušným správcom.

(10) Manažér informačnej bezpečnosti môže nastavovať ďalšie bezpečnostné obmedzenia sieťovej komunikácie.

Čl. 16
Nastavenia aktívnych sieťových zariadení

(1) Všetky sieťové zariadenia musia odpovedať na ICMP Echo request (ping) minimálne z centrálnych monitorovacích bodov.

(2) Pre každú sieťovú zónu musia byť prijaté opatrenia zabraňujúce neautorizovaným počítačom pripojiť sa do príslušnej siete.

(3) Systémový čas switchov, serverov a routerov musí byť synchronizovaný cez server ntp.uniba.sk.

(4) Všetky produkčné switche musia byť vzdialene manažovateľné, s výnimkou maximálne 8-portových hraničných switchov, v ktorých sú všetky zariadenia pripojené do rovnakej bezpečnostnej zóny a umiestnené v rovnakej miestnosti.

(5) Ak zariadenie také nastavenie umožňuje, prístupové práva k manažovateľným sieťovým zariadeniam musia byť nastavené tak, aby ich mohli spravovať len ich správcovia.

(6) Na switchoch v používateľských zónach musí byť aktivovaný DHCP snooping.

(7) Switche, ktoré túto funkcionalitu podporujú musia byť nastavené tak, aby do DHCP requestov pridávali informácie o zdrojovom switchi a porte, z ktorého request pochádza (DHCP Address Allocation Using Option 82). DHCP server musí tieto informácie zaznamenávať a uchovávať v súlade s Čl. 18.

Čl. 17
Bezdrôtové siete

(1) Na pripojenie zariadenia k bezdrôtovej sieti sa vzťahujú rovnaké bezpečnostné požiadavky ako na fyzické pripojenie zariadenia k zóne, ku ktorej je pripojená daná bezdrôtová sieť. Musia byť prijaté také opatrenia, aby sa k bezdrôtovej sieti mohli pripojiť len používatelia, ktorí majú právo pripojiť sa k príslušnej pevnej sieti.

(2) Na bezdrôtové prístupové body platia rovnaké bezpečnostné požiadavky ako na routre respektíve switche v príslušnej zóne (viď Čl. 16).

(3) Bezdrôtové siete pripojené k sieti UK musia mať zabezpečenie minimálne na úrovni technológie WPA2 s autorizáciou zdieľaným kľúčom (PSK) alebo 802.1X Extensible Authentication Protocol (EAP) s výnimkou EAP-MD5. Na autorizáciu musí byť použité bezpečné heslo.

(4) Pre potreby krátkodobých udalostí (napr. konferencia) môže správca dočasne pripojiť nezabezpečenú bezdrôtovú sieť do nechránenej zóny.

Čl. 18
Záznam

(1) Auditné záznamy (tzv. logy) z aktívnych sieťových zariadení a príslušných serverov musia byť zaznamenávané tak, aby bolo možné dodatočne do 180 dní nájsť priradenie medzi IP adresou a sieťovou zásuvkou na UK, do ktorej bolo vysielajúce zariadenie pripojené.

(2) U všetkých zaznamenaných aktivít musí byť zaznamenaný dátum aj čas. Záznamy musia byť fyzicky uchovávané mimo daných zariadení (napr. na univerzitnom syslog serveri).

ODDIEL IV
BEZPEČNOSŤ SERVEROV

Čl. 19
Všeobecné zásady

(1) Všetky servery musia spĺňať nasledovné požiadavky:

a) Používateľské kontá na úrovni operačného systému môžu mať len osoby, ktoré to potrebujú na zabezpečenie prevádzky, rozvoja a bezpečnosti servera a aplikácií, ktoré na serveri bežia.

b) Systém vzdialeného prístupu na server musí byť šifrovaný a bezpečný.

c) Každý server musí byť nastavený tak, že môže byť vzdialene korektne vypnutý.

d) Každý server musí byť nastavený tak, že po stlačení tlačidla Power na serveri sa korektne vypne.

e) Ak server používa operačný systém Windows, musí mať nainštalovaný antivírus. Tento musí buď kontrolovať súbory pri otváraní, respektíve spúšťaní, alebo musí kontrolovať celý lokálny pevný disk minimálne raz denne.

(2) Produkčné servery musia spĺňať požiadavky uvedené v odseku 1 a navyše musia spĺňať nasledovné požiadavky:

a) Každý fyzický server vrátane všetkých jeho sieťových služieb musí byť nastavený tak, aby bol schopný po vypnutí (plánovanom, aj neplánovanom, respektíve korektnom, aj tzv. tvrdom) korektne naštartovať.

b) Ak to nie je nutné, správcovia aplikácií bežiacich na serveri nesmú mať práva administrátora.

c) Server, s výnimkou terminálového servera, nesmie byť používaný ako pracovná stanica.

d) Server musí mať nasadené nasledovné bezpečnostné opatrenia:

1. Monitoring dostupnosti a vyťaženia servera s okamžitým informovaním zodpovedných osôb o prekročení stanovených limitov.
2. Vzdialený záznam aktivít používateľov minimálne na úrovni záznamov o prihlásení a odhlásení systémových používateľov.
3. Dostatočne výkonný a spoľahlivý hardvér.
4. Zálohovanie dát servera podľa vytvorenej stratégie.

(3) Server, ktorý poskytuje kritickú službu alebo server, od ktorého je vyžadovaná vysoká dostupnosť, musí spĺňať požiadavky uvedené v odsekoch 1 a 2 a navyše musí spĺňať nasledovné požiadavky:

a) Ak server používa vlastný pevný disk, musí mať aj redundantný pevný disk.
b) Server musí mať redundantné napájacie zdroje.
c) Musí byť vytvorené riešenie umožňujúce prebrať služby servera po jeho výpadku (napr. záložný server).
d) Musí byť pripravený havarijný plán minimálne pre prípad zlyhania hardvéru, operačného systému, aplikácií a sieťového pripojenia servera.

ODDIEL V
FYZICKÁ BEZPEČNOSŤ

Čl. 20
Všeobecné zásady

(1) Všetky kancelárie musia byť uzamykateľné.

(2) Sieťové uzly musia byť chránené proti vandalizmu a neoprávnenému fyzickému prístupu. Kabeláž v priestoroch, ktoré sú dostupné študentom musí byť fyzicky chránená tak, aby bez násilného vniknutia nebolo možné fyzické pripojenie sieťového zariadenia do inej ako nechránenej zóny.

(3) Káble, patch-panely a sieťové zásuvky musia byť označené tak, aby bolo možné zistiť, ktorý kábel vedie do ktorej zásuvky, respektíve miestnosti.

(4) Miestnosti, v ktorých sa nachádzajú produkčné servery musia:

a) byť zabezpečené proti neoprávnenému vniknutiu,
b) mať pevné steny, bezpečnostné dvere (vrátane bezpečnostného zámku) a mreže na oknách,
c) mať prostredie udržiavané tak, aby jeho parametre, hlavne teplota, vlhkosť a prašnosť, spĺňali prevádzkové požiadavky serverov a ďalších príslušných zariadení umiestnených v miestnosti,
d) byť chránené proti bleskom.

(5) Napájanie produkčných serverov musí byť chránené záložným zdrojom elektrickej energie (UPS) a prepäťovou ochranou triedy D.

(6) Vyhradená technologická miestnosť musí mať vlastný vypínač elektriny a osobitný istič.

(7) Servery spracúvajúce chránené informácie a servery nevyhnutne potrebné pre beh kritických služieb musia byť umiestnené v miestnosti, ktorá navyše spĺňa nasledovné bezpečnostné požiadavky:

a) bezpečnostné dvere (vrátane bezpečnostného zámku) triedy 3,
b) pohybový senzor napojený na alarm,
c) monitoring vstupu do miestnosti kamerami,
d) monitoring serverov kamerami,
e) záložný zdroj elektrickej energie (UPS),
f) uzemnenie rackov,
g) redundantné klimatizácie,
h) antistatická úprava miestnosti,
i) protipožiarne dvere,
j) dymový senzor a požiarny hlásič.

ODDIEL VI
POVINNOSTI POUŽÍVATEĽOV

Čl. 21
Všeobecné zásady

(1) Pri používaní informačných systémov univerzity sa musia používatelia riadiť:

a) používateľskými predpismi daných informačných systémov,
b) pokynmi správcov daných informačných systémov,
c) pokynmi im príslušného technického správcu IIKS.

(2) Ak používateľ nevie posúdiť bezpečnostné riziko, môže sa obrátiť na správcu, prípadne na CePIT.

Čl. 22
Chránené informácie

(1) Každý používateľ, ktorý disponuje prístupovými právami na prístup k databázam osobných údajov, musí byť poučený o zásadách ochrany informácií v súlade so všeobecne záväznými právnymi predpismi a vnútornými predpismi UK.

(2) Používatelia môžu spracúvať alebo uchovávať chránené informácie (napr. databázy osobných údajov) v nešifrovanej elektronickej forme len na chránených pracovných staniciach, prípadne v univerzitných informačných systémoch na to určených.

(3) Dočasne vytvorené dokumenty obsahujúce chránené informácie musia byť po použití bezpečne zmazané, prípadne z nich musia byť odstránené chránené informácie.

(4) Používateľ nesmie vystaviť riziku odcudzenia, prípadne poškodenia chránené informácie univerzity (napr. nesmie prenášať chránené informácie v nešifrovanej podobe na externých médiách mimo UK).

Čl. 23
Heslá

(1) Ak sa používateľ domnieva, že k jeho heslu získala prístup iná osoba, musí dané heslo okamžite zmeniť.

(2) Ak používateľ stratí hardvérový autorizačný prostriedok (napr. čipovú kartu) na prístup k univerzitným informačným systémom, musí túto stratu okamžite nahlásiť príslušnému správcovi.

(3) Ak je od používateľa požadovaná zmena hesla, nesmie si nastaviť také heslo, aké už používal v minulosti.

(4) Používateľ:

a) musí používať bezpečné heslo,
b) môže zadávať heslo umožňujúce prístup k databázam osobných údajov len na chránených pracovných staniciach,
c) nesmie v informačných systémoch UK používať rovnaké heslo ako v externých systémoch,
d) nesmie umožniť iným osobám prístup ku svojim autorizačným prostriedkom (napr. heslo, čipová karta),
e) nesmie uchovávať heslo na miestach dostupných iným osobám (napr. na papieri v kancelárii),
f) nesmie zadávať svoje prístupové heslo do webových aplikácií, ktoré nie sú zabezpečené univerzitným certifikátom alebo certifikátom dodávaným s webovým prehliadačom.

Čl. 24
Pracovná stanica

Používateľ nesmie:

a) robiť technické zásahy do počítača,
b) neautorizovane meniť systémové nastavenia počítača,
c) vynášať počítače z miestnosti bez povolenia správcu (s výnimkou prenosných počítačov),
d) zapájať svoje alebo cudzie súkromné (nie univerzitné) zariadenia do univerzitnej počítačovej siete s výnimkou na to vyhradených miest (napr. sieť Eduroam),

e) deaktivovať antivírus alebo iné bezpečnostné mechanizmy počítača,

f) na univerzitných počítačoch otvárať dátové nosiče, o ktorých sa domnieva, že obsahujú vírus,

g) brániť kontrole počítača správcom,

h) inštalovať softvér na chránenú pracovnú stanicu,

i) ignorovať bezpečnostné varovné hlásenia počítača.

Čl. 25
Zneužívanie počítačovej siete UK

(1) Používateľ nesmie používať počítačovú sieť univerzity na:

a) získavanie neautorizovaného prístupu k univerzitným alebo cudzím systémom,

b) šírenie škodlivého kódu (tzv. malware, napr. počítačových vírusov) a nevyžiadanej elektronickej pošty,

c) realizáciu sieťových útokov,

d) narušovanie práce iných používateľov,

e) znižovanie dostupnosti alebo kvality sieťových služieb,

f) ďalšej škodlivej činnosti namierenej proti iným používateľom alebo systémom,

g) činnosti v rozpore s platnou legislatívou SR.

(2) Používateľ môže používať iba prístupové práva, ktoré mu boli pridelené v súlade s platnými pravidlami o prideľovaní prístupových práv k danému informačnému systému, alebo správcom daného informačného systému.

(3) Používateľ nesmie vykonávať činnosť za účelom získania prístupových práv alebo informácií, ktoré mu neprináležia. Ak takéto práva získa náhodne alebo vedome, nesmie ich použiť a musí o tom informovať príslušného správcu.

Čl. 26
Kancelária

(1) Zamestnanec univerzity nesmie umožniť prítomnosť cudzích osôb bez dozoru vo svojej kancelárii.

(2) Ten, kto posledný opúšťa miestnosť, ju musí zamknúť. Po skončení pracovnej doby musí aj zatvoriť všetky okná a zapnúť alarm, ak je ním miestnosť vybavená.

Čl. 27
Komunikácia

(1) Pri vybavovaní žiadostí (napr. zadávanie informácií do informačného systému alebo poskytovanie informácií) si používateľ musí overiť, či žiadateľ má právo na požadovaný úkon a či je skutočne tou osobou, za ktorú sa vydáva.

(2) Pri posielaní neverejných informácií prostredníctvom elektronickej pošty si musí používateľ overiť, či adresa, na ktorú správu posiela, skutočne patrí osobe, ktorej je správa určená.

(3) Pracovník univerzity môže poskytovať informácie len autorizovaným osobám. Pracovník univerzity môže prijímať vstupné informácie pre svoju prácu len od autorizovaných osôb.

(4) Používateľ nesmie:

a) posielať chránené informácie (napr. osobné údaje) mimo sieť UK (napr. na súkromné e-mailové adresy),
b) poskytovať osobné údaje o študentoch alebo zamestnancoch univerzity tretím osobám,
c) preposielať reťazové správy elektronickej pošty a iné podozrivé správy požadujúce, aby ich používateľ preposlal čo najväčšiemu množstvu ľudí (tzv. hoax),
d) posielať nevyžiadané správy elektronickej pošty (tzv. spam),
e) meniť hlavičky správ (napr. meniť meno alebo adresu odosielateľa).

(5) Zamestnanci, ktorí spracúvajú osobné údaje, nesmú automaticky presmerovávať univerzitnú elektronickú poštu mimo univerzity.

(6) Ak používateľ v e-mailovej komunikácii vystupuje ako zamestnanec univerzity, musí používať jemu správcom pridelenú oficiálnu univerzitnú e-mailovú adresu, a to ako adresu odosielateľa, tak aj ako tzv. reply-to adresu.

(7) Pri odpovedaní alebo preposielaní správ elektronickej pošty musí používateľ skontrolovať zoznam adresátov a prípadnú predošlú komunikáciu, ktorá je obsahom preposielanej správy.

(8) E-mailová schránka a všetka elektronická komunikácia prechádzajúca cez počítačovú sieť univerzity je majetkom univerzity a univerzita ju môže kontrolovať.

(9) Používateľ musí nahlásiť zistené bezpečnostné incidenty (napr. únik osobných údajov, únik univerzitných hesiel iných používateľov, zneužitie informačných systémov) správcom príslušných systémov alebo na CePIT.

Čl. 28
Sankcie

(1) Porušenie tejto smernice a súvisiacich predpisov sa môže považovať za porušenie pracovnej disciplíny, prípadne za disciplinárny priestupok.

(2) Ak používateľ poruší ustanovenia tejto smernice, alebo ak jeho počítač alebo iné ním pripojené zariadenie narušuje chod informačných systémov univerzity, správca ho môže odpojiť od počítačovej siete alebo mu odobrať prístup k informačným systémom vrátane

počítačov. Zároveň správca bez zbytočného odkladu upovedomí o vykonaní tohto opatrenia priameho nadriadeného používateľa.

Čl. 29
Povinnosti správcov

Správca je povinný:

a) dôrazne chrániť vlastné prístupové práva, autorizačné prostriedky a vlastné pracovné stanice,
b) na správu systémov používať bezpečné heslá,
c) udržiavať dokumentáciu ním spravovaných systémov v súlade so skutočným stavom systémov,
d) udržiavať v tajnosti informácie, ktoré získal využitím nadštandardných prístupových práv jemu pridelených za účelom správy informačných systémov univerzity.

ODDIEL VII
ZÁVEREČNÉ USTANOVENIA

Čl. 30

(1) Univerzita môže pre vlastné potreby nakupovať len zariadenia schopné technicky spĺňať všetky touto smernicou na ne kladené bezpečnostné požiadavky.

(2) Nasadenie bezpečnostných opatrení na fakulte alebo samostatne hospodáriacej súčasti technicky zabezpečí technický správca IIKS danej fakulty alebo súčasti.

(3) Vedenie fakulty alebo samostatne hospodáriacej súčasti zabezpečí potrebnú súčinnosť aj prostriedky potrebné na splnenie bezpečnostných požiadaviek stanovených touto smernicou.

(4) CIT poskytne zamestnancom podieľajúcim sa na aplikovaní uvedených bezpečnostných opatrení dostupné informácie, nastavenia systémov a konzultácie.

(5) Manažér informačnej bezpečnosti bude koordinovať nasadzovanie bezpečnostných opatrení na úrovni univerzity.

(6) Fakulty a samostatne hospodáriace súčasti UK si môžu pravidlá informačnej bezpečnosti upravené touto smernicou podrobnejšie rozpracovať na svoje podmienky. Smernice informačnej bezpečnosti jednotlivých fakúlt a samostatne hospodáriacich súčastí musia byť v súlade s touto smernicou.

(7) V prípade rozporu vnútorného predpisu fakulty alebo samostatne hospodáriacej súčasti UK s touto smernicou platia ustanovenia tejto smernice.

(8) Táto smernica nadobúda platnosť a účinnosť 26. januára 2011.

V Bratislave dňa 26. januára 2011

doc. PhDr. František Gahér, CSc.
rektor UK

Príloha č. 1 k Vnútornému predpisu č. 2/2011 Smernici rektora UK

Žiadosť o odstránenie bezpečnostných nastavení pracovnej stanice

Technický správca IIKS
<Meno>
<Súčasť>

Žiadateľ

Meno: ....., loginUK: ....., e-mail: .....

Žiadam o odstránenie bezpečnostných nastavení pracovnej stanice s názvom: .....

HIM: ....., dátum: ..... z dôvodov:

….....

1. Na pracovnej stanici nebudem spracúvať ani uchovávať osobné údaje.
2. Som si vedomý/vedomá, že odstránením bezpečnostných nastavení **strácam nárok na technickú podporu** softvéru príslušnej pracovnej stanice. Môj počítač môže byť pripojený do samostatnej nechránenej siete pracoviska.
3. Som si vedomý/vedomá toho, že odstránenie bezpečnostných nastavení zvyšuje riziko poruchy pracovnej stanice, straty dát, vyzradenia mojich hesiel, nákazy počítačovým vírusom, inštalácie škodlivého softvéru s možnosťou páchania kriminálnych aktivít (napr. šírenie pornografie, porušovanie zákona o autorských právach, narušovanie bezpečnosti iných počítačov v sieti) pod mojou identitou, a to aj bez môjho vedomia.
4. Preberám plnú zodpovednosť za bezpečnosť pracovnej stanice.
5. Mám dostatočné povedomie v oblasti informačnej bezpečnosti.
6. Pracovnú stanicu budem spravovať a používať v súlade s internými predpismi UK. Na pracovnú stanicu budem inštalovať len legálny softvér v súlade s jeho licenčnými podmienkami.

.....
Podpis žiadateľa

Prehlásenie priameho nadriadeného žiadateľa
Prehlasujem, že žiadateľ potrebuje nadštandardné prístupové práva na vykonávanie pracovných úloh. Potvrdzujem uvedené informácie a súhlasím s odstránením bezpečnostných nastavení pracovnej stanice.

.....
Meno a priezvisko (čitateľne), podpis priameho nadriadeného