BEZPEČNOSTNÍ ŘÁD

ČESKÉ ZEMĚDĚLSKÉ UNIVERZITY V PRAZE

PŘÍLOHA Č. 1

BEZPEČNOSTNÍ POLITIKA INFORMACÍ

ČESKÉ ZEMĚDĚLSKÉ UNIVERZITY V PRAZE

Verze 2.0

2008

PŘÍLOHA Č. 1 BEZPEČNOSTNÍHO ŘÁDU - BEZPEČNOSTNÍ POLITIKA INFORMACÍ ČESKÉ ZEMĚDĚLSKÉ UNIVERZITY V PRAZE

Verze	2.0
Účinnost od	1. 3. 2008
Klasifikace	Veřejné
Počet stran	24
Garant	Šup Libor, Bc., bezpečnostní technik ICT
Zpracoval	Šup Libor, Bc., bezpečnostní technik ICT Hradecký Ondřej, Ing., vedoucí OIKT ČZU Kéri František, Ing., konzultant, ClarioNet, s.r.o. Vlček Peter, Ing., projektový manažer, ClarioNet, s.r.o. Novák Jan, vedoucí manažer, ClarioNet, s.r.o. Kadeřávková Pavla, Ing., supervisor, ClarioNet, s.r.o.
Ověřil	Doc. Ing. Vladimír Vít, CSc., útvar interního auditu ČZU JUDr. Tomáš Hándl, právní oddělení ČZU
Schválil	Hron Jan, prof. Ing. DrSc., dr.h.c., rektor ČZU
Působnost	Všichni zaměstnanci ČZU, studenti ČZU. Dále zástupci externích subjektů a třetích stran, kteří spolupracují s ČZU, nebo se nacházejí v lokalitách a prostorách ČZU a u kterých vzniká potřeba tato bezpečnostní pravidla realizovat.

Registr změn

Číslo změny	Verze	Účinnost od	Popis změny	Změnu provedl
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

Obsah

1. Úvod

Bezpečnostní politika informací České zemědělské univerzity v Praze (dále BPI ČZU, bezpečnostní politika) je definována jako prohlášení univerzity na nejvyšší úrovni o očekáváních, zásadách, cílech, a obecných požadavcích k dosažení bezpečnosti informací ČZU.

BPI ČZU je určena pro všechny zaměstnance ČZU, studenty ČZU, jakož i pro třetí smluvně vázané strany jako základní vodítko pro cíle, zásady a pravidla, které ČZU v oblasti bezpečnosti informací prosazuje.

BPI ČZU je nedělitelnou součásti „Bezpečnostního řádu České zemědělské univerzity v Praze“ (dále BŘ ČZU, bezpečnostní řád).

2. Působnost

Pravidla bezpečnosti jsou platná pro všechny zaměstnance ČZU, studenty ČZU. Dále pro zástupce externích subjektů a třetích stran, kteří spolupracují s ČZU, nebo se nacházejí v lokalitách a prostorách ČZU a u kterých vzniká potřeba tato bezpečnostní pravidla realizovat.

Pravidla bezpečnosti uvedená v tomto bezpečnostním řádu a v interních řídících dokumentech mohou být dále rozpracována v interních směrnicích fakult a dalších součástí univerzity. Takové směrnice jsou podřízeny tomuto řádu a navazujícím interním řídícím dokumentům vydaných rektorem ČZU.

Pro zajištění trvalého rozvoje univerzity a jejich součástí je nezbytné udržovat bezpečnost univerzity minimálně na úrovni, která vylučuje nebo omezuje vliv zjištěných rizik na procesy ČZU.

Cílem organizace bezpečnosti je vytvořit uvnitř univerzity takové vědomí potřeby bezpečnosti, které se stane neoddělitelnou součástí každodenního chodu univerzity a součástí celkové politiky a kultury akademického prostředí na ČZU.

Bezpečnostní řád a bezpečnostní politika informací jsou dále upřesňovány dalšími bezpečnostními dokumenty, které řeší konkrétní požadavky na jednotlivé části aktiv univerzity.

3. Východiska

Východiskem pro celkové postavení, působnost, tvorbu a strukturu BPI ČZU je norma:

- ČSN ISO/IEC 27001,
- ČSN ISO/IEC 17799.

4. Účel

Účelem BPI ČZU je zejména:

a) Definice základních cílů a celkového směru a principů činnosti ČZU v oblasti bezpečnosti informací.

b) Zohlednit aktuální a relevantní normativní, smluvní a organizační bezpečnostní požadavky a poskytnout pro ně jednotnou a koncepční platformu.

c) Vytvořit odpovídající platformu a relevantní vazby na prostředí ČZU, tedy na organizační strukturu ČZU, základní strategii a řídící vazby a procesy.

d) Ustanovit a definovat základní kritéria pro hodnocení rizik a základní strukturu procesu analýzy a informačních řízení rizik.

e) Vyjádření jednoznačné vůle vedení ČZU systematicky chránit informace ČZU, přiřazení informacím ČZU odpovídající vážnost a vyjádření jednoznačné vůle k vytvoření vhodných podmínek pro zajištění odpovídajících prostředků k realizaci patřičných bezpečnostních opatření.

5. Definice bezpečnosti

5. 1. Cíle bezpečnosti

Mezi hlavní cíle bezpečnosti patří zejména:

a) Hlavním cílem bezpečnosti informací ČZU je zajištění trvalé podpory činnosti ČZU ze strany IS ČZU a minimalizace rizika selhání v oblasti dostupnosti, integrity a důvěrnosti informací ČZU.

b) Míra ochrany poskytovaná informacím a vlastnímu IS ČZU musí být úměrná hodnotě informací a předpokládaným hrozbám, kterým jsou vystaveny.

c) Bezpečnostní opatření musí trvale pokrývat všechny významné hrozby vůči aktivům IS ČZU.

d) Jednotlivá bezpečnostní opatření v rámci IS ČZU musí být realizována takovým způsobem a v takových oblastech, aby bylo dosaženo dostatečné bezpečnosti s optimálními náklady a minimálním omezením požadovaných funkčních vlastností IS ČZU.

e) Informace musí být chráněny ve všech formách a na všech nosičích a médiích, ve kterých se mohou v rámci IS ČZU vyskytnout.

f) Používané i nově zaváděné informační systémy v rámci ČZU musí být upraveny a vybírány tak, aby splňovaly zásady v této bezpečnostní politice uvedené.

g) Veškerá aktiva IS ČZU musí být využívána pouze oprávněnými uživateli a pouze k účelům souvisejícím s plněním pracovních povinností.

h) Bezpečnost informací ČZU musí být vyžadována všemi řídícími pracovníky, musí být řízena, musí být stanoveny odpovědnosti a povinnosti jednotlivých osob a musí být všeobecně respektována.

6. Systém řízení bezpečnosti informací ČZU (SŘBI / ISMS ČZU)

Pro zajištění komplexního a systematického přístupu k řešení bezpečnosti informací, musí ČZU vybudovat a udržovat zdokumentovaný systém řízení bezpečnosti informací ISMS (Information Security Management System), který bude zahrnovat komplexní zmapování informačních rizik, návrh a zavedení opatření na jejich snížení, zdokumentování procesu údržby, řízení a zlepšování těchto opatření (bezpečnosti informací) a zajištění dlouhodobé, systematické a konzistentní bezpečnosti informací, jak v listinné (papírové), tak i v elektronické (datové) formě.

7. Organizace bezpečnosti informací

7. 1. Role a odpovědnosti

Pravidlo oddělení klíčových rolí a odpovědností při návrhu, implementaci, provozu, kontrole a zlepšování je aplikováno dle požadavků „Bezpečnostního řádu ČZU“. Pro prosazení bezpečnostní politiky informací jsou určeny následující základní bezpečnostní role a odpovědnosti:

Role	Odpovědnosti
Administrátor OS, SW, DB, sítě (souhrnně „Administrátor IS“) či správce IS	• Administrace přístupových práv rolím a uživatelským účtům dle schválených žádostí vedoucích / garantů / projektových manažerů a dodavatelů v závislosti na použitém procesu řízení přístupu. • Zablokování a přesměrování přístupových práv odcházejících zaměstnanců na jiné osoby dle pokynů vedoucích oddělení.
Bezpečnostní inspektor IS ČZU	• Kontrola dodržování formálních administrativních kroků a postupů. Kontrola existence záznamů (formulářů) a dodržování směrnic a souvisejících organizačních bezpečnostních opatření a postupů. • Zná odbornou problematiku informačních systémů, jež spadají do jeho působnosti. Zaměřuje se svou činností především na kontrolní činnost a na prevenci selhání bezpečnosti informačního systému. Ve své činnosti zejména kontroluje prosazování požadavků bezpečnostní politiky informací a bezpečnostních pravidel v činnosti konkrétního pracoviště v rámci ČZU; průběžně sleduje stav bezpečnosti informací ČZU; posuzuje navrhované změny bezpečnostních směrnic ČZU.
Bezpečnostní manažer ČZU	• Posouzení návrhu, implementace a provozu bezpečnostních systémů. Návrh adekvátních bezpečnostních opatření a odpovědnost za kontrolu bezpečnostních opatření. Pro podrobnosti viz. kap. 7. 3. Bezpečnostní manažer ČZU.

Role	Odpovědnosti
Bezpečnostní správce IS	• Instalace, konfigurace, údržba a zajištění funkčnosti schválených bezpečnostních opatření. Kontrola instalace, nastavení a provozu bezpečnostních opatření. Ad-hoc kontrola bezpečnostních logů. • Bezpečnostní správce IS působí jako prostředník v prosazení vztahu bezpečnosti informací a vztahu mezi jednotlivými skupinami a odděleními v celé organizaci. • Bezpečnostní správce musí připravovat prováděcí bezpečnostní dokumenty, podílet se na interních projektech rozvoje systému, asistovat při řízení implementace, vyšetřovat porušení bezpečnosti informací a vykonávat další aktivity nezbytné pro zajištění bezpečné manipulace s informacemi. Jeho pracovní náplň vyplývá z bezpečnostních předpisů. Je odborně odpovědný bezpečnostnímu manažerovi ČZU.
Garant/Vlastník informací a dat (procesů a modulů IS)	• Odpovídá za zpracování konkrétního informačního aktiva. • Předmětem činnosti této role je řízení a dohlížení na adekvátní zabezpečení zpracování svěřeného informačního aktiva tak, aby bylo minimalizováno riziko ztráty, prozrazení, změny, poškození a zneužití informačních aktiv.
Pracovník personálního odboru ČZU	• Definice bezpečnostních kritérií pro jednotlivé pracovní pozice. • Kontrola plnění personálních bezpečnostních požadavků.
Projektový manažer IS	• Koordinace činností projektového týmu ČZU při vývoji a implementaci nových projektů (aplikací, služeb a subsystémů) ve spolupráci s projektovým týmem dodavatele. • Předávání informací mezi garanty informací a dat, administrátory IS a projektovým týmem dodavatele z hlediska správné specifikace požadavků, rolí a oprávnění a implementace jednotného procesu řízení přístupu v probíhajících projektech IS. Role projektového manažera IS je přidělovaná zaměstnancům ČZU vedoucím OIKT ČZU.
Fórum pro bezpečnost informací ČZU	• Posouzení a schválení změn bezpečnostní politiky a hlavních odpovědností. Pro podrobnosti viz. kap. 7. 2. 7. 2. - Fórum pro bezpečnost informací ČZU
Uživatel IS ČZU	• Dodržování a plnění všech stanovených provozních bezpečnostních zásad, povinností, a odpovědností.
Vedoucí oddělení/odboru	• Schvalování a podávání žádostí o založení, změnu a zrušení uživatele a jeho oprávnění v IS ČZU. Pokyny administrátorům IS k přesměrování přístupových práv k elektronické poště, datům a souborům odcházejících zaměstnanců na jiné pracovníky oddělení/odboru. • Schvalování požadavků na založení, změnu a zrušení uživatele a jeho oprávnění v IS ČZU. Delegování vybraných podřízených pracovníků do role garanta informací a dat pro jednotlivé procesy ČZU v působnosti svého oddělení/odboru.

Role	Odpovědnosti
Vedoucí OIKT ČZU	• Návrh, výběr, schválení, implementace a provoz IKT zajišťující funkčnost IS ČZU. Spolupráce při návrhu bezpečnostních opatření. Zajištění implementace a funkčnosti bezpečnostních opatření. V kompetenci vedoucího OIKT ČZU je přidělování, změna, přesun • a zrušení zde uvedených odpovědností.
Vývojář a dodavatel aplikací	• Návrh, vývoj a implementace aplikací, služeb a subsystémů IS ČZU, které zajišťují funkčnost a podporu procesů ČZU. • Implementace principů řízení přístupu a administrace rolí, oprávnění a transakcí procesů ČZU v modulech aplikací, služeb a subsystémů IS, dle požadavků projektových manažerů IS a garantů informací a dat.

7. 2. Fórum pro bezpečnost informací ČZU

Pro potřeby řízení a zvládání bezpečnosti informací ČZU se ustanovuje „Fórum pro bezpečnost informací“. Složení řídícího výboru:

a) Kvestor ČZU.

b) Bezpečnostní manažer ČZU.

c) Vedoucí OIKT ČZU.

d) Bezpečnostní inspektor IS ČZU.

e) Vedoucí personálního odboru ČZU.

f) Vedoucí ekonomického odboru ČZU.

g) Vedoucí provozně technického odboru ČZU.

Fórum pro bezpečnost se schází minimálně jednou za půl roku pod vedením kvestora ČZU, aby:

a) Zhodnotil sledování hlavních hrozeb působících na aktiva ČZU a vystavení riziku.

b) Zhodnotil analýzy a kontrolu bezpečnostních incidentů.

c) Schválil hlavní iniciativy směřující ke zlepšení bezpečnosti informací.

7. 3. Bezpečnostní manažer ČZU

Pro potřeby koordinace bezpečnosti informací v rámci celé ČZU plní roli hlavního koordinátora bezpečnostní manažer ČZU:

a) Schvaluje specifické role a odpovědnosti za bezpečnost informací v rámci celé univerzity.

b) Schvaluje specifické metodologie a postupy v oblasti bezpečnosti informací, např. hodnocení rizik, systém bezpečnostní klasifikace.

c) Přijímá a podporuje iniciativy v oblasti bezpečnosti informací dotýkající se celé ČZU, (např. program zvyšování bezpečnostního vědomí).

d) Zajišťuje, aby bezpečnost byla součástí procesu plánování v oblasti informatiky.

e) Koordinuje realizaci specifických opatření bezpečnosti pro nové systémy nebo služby.

f) Uděluje výjimky z bezpečnostních pravidel a kontroluje je.

g) Prosazuje, aby podpora organizace bezpečnosti informací byla viditelná v celé organizaci.

7. 4. Bezpečnostní správce IS

Základní povinností bezpečnostního správce IS je spravovat bezpečnost systému tak, aby byly dodržovány všechny požadavky bezpečnostní politiky systému uvedené v bezpečnostních směrnicích jednotlivých pracovišť, zejména:

a) Zavádění nových uživatelů do systému IS ČZU.

b) Vedení a údržbu přístupových hesel a včasnou obměnu bezpečnostních hesel a kódů.

c) Kontrolu a správné vedení autorizačních záznamů jednotlivých uživatelů IS ČZU s důrazem na to, aby přesně odpovídaly skutečnému oprávnění jednotlivých uživatelů, především při definování přístupu již existujícího uživatele v jiné skupině.

d) Správnou definici přístupových práv ke zdrojům systému pro každou skupinu nebo jednotlivého uživatele.

e) Podchycení, dokumentaci a vyhodnocení všech případů selhání bezpečnosti IS (ztráta dat, přístup k cizím datům, neoprávněné použití výpočetních prostředků apod.) ve formě zprávy o bezpečnostním incidentu.

f) Vyhodnocení revizních záznamů s důrazem na zjišťování neoprávněných pokusů o přihlášení do systému, o obejití bezpečnostních mechanismů, o zásahu do autentizačních, autorizačních nebo jiných evidenčních souborů, a o jakékoli narušení bezpečnostních mechanismů systému.

g) Archivaci revizních záznamů.

h) Sledování bezpečnosti informačního systému a hlášení každého jeho narušení (bezpečnostní incident) formou hlášení o bezpečnostním incidentu, které adresuje bezpečnostnímu manažerovi.

8. Evidence a klasifikace aktiv

8. 1. Evidence aktiv

Jednotlivá aktiva IS ČZU musí být řádně evidována. Pro každé důležité aktivum IS ČZU se jasně stanoví jeho garant/vlastník. Jde zejména o:

a) Informační aktiva: databáze a datové soubory, systémová dokumentace, uživatelské manuály, školící materiály, provozní nebo podpůrné procedury, havarijní plány, dohody o záložním provozu a podobně.

b) Programová aktiva: aplikační programové vybavení, systémové programové vybavení, vývojové nástroje, utility a podobně.

c) Fyzická aktiva: počítače a komunikační zařízení, magnetická média (pásky a disky), další technická zařízení (napájecí zdroje, klimatizační zařízení), nábytek, prostory a podobně.

d) Služby: počítačové a komunikační služby, další technické služby (topení, osvětlení, napájení, klimatizace a podobně).

8. 2. Klasifikace informací

V rámci IS ČZU jsou zpracovávány důležité a citlivé informace, které jsou vlastněny ČZU nebo souvisejí s její činností, (případně jsou jí svěřené nebo poskytnuté), jejichž vyzrazení, ztráta, chybné použití, neoprávněná modifikace nebo přístup neoprávněné osoby k nim mohou ztížit činnost ČZU nebo způsobit újmu fyzické nebo právnické osobě, která informaci poskytla, nebo jíž se informace týká.

Základní klasifikace informace v IS ČZU je klasifikována stupni:

a) Diskrétní.

b) Osobní.

c) Interní.

d) Veřejné.

Stupně bezpečnostní klasifikace informací zohledňují potřeby ČZU sdílet nebo omezovat šíření informací a také následky na fungování ČZU spojené s neautorizovaným přístupem k informacím nebo jejich zničením.

Za klasifikaci informačního aktiva, např. dokumentu, datového záznamu, datového souboru nebo diskety, a za pravidelné přezkoumání stanovené klasifikace, nese odpovědnost vlastník informace nebo ustanovený garant dat.

Další podrobné informace určuje interní řídící dokument - Pravidla pro klasifikaci informací.

9. Personální bezpečnost

9. 1. Přijímání nových zaměstnanců

V rámci provozu IS ČZU musí být provedena opatření proti riziku lidské chyby, krádeže aktiv, podvodu nebo zneužití aktiv ČZU. Požadavky na bezpečnost musí být personálním odborem ČZU zapracovány do personalistických postupů. Požadavky ze strany bezpečnosti IS ČZU musí být zahrnuty v přijímacím řízení nových zaměstnanců, jakož i v popisech jejich práce a pracovních smlouvách. Následně musí být jejich dodržování kontrolováno personálním odborem ČZU a bezpečnostním inspektorem IS ČZU během celého trvání zaměstnání.

9. 2. Povinnost mlčenlivosti

Podle doporučení personálního odboru ČZU nebo bezpečnostního manažera ČZU musí být se zaměstnancem ČZU, který plní funkce vybrané pozice ČZU, uzavřena dohoda o mlčenlivosti. Všichni uživatelé třetích stran využívající IKT prostředky IS ČZU musí podepsat dohodu o dodržování mlčenlivosti (zachování důvěrnosti) o všech skutečnostech, které mohou narušit bezpečnost informací ČZU s uvedením sankce v případě porušení dohody. Dohoda o mlčenlivosti se uzavírá současně při uzavírání pracovní smlouvy. Povinnost zachovávat mlčenlivost trvá i po ukončení pracovního poměru, a to po dobu přiměřenou důležitosti aktiv (zpravidla po dobu 2 let, pokud není dáno jinak).

9. 3. Povinnosti zaměstnanců

Pracovníci personálního odboru ČZU musí zajistit, aby do popisu práce byly zahrnuty všechny odpovědnosti a povinnosti, které vyplývají z požadavků bezpečnosti aktiv ČZU. Potencionální kandidáti o zaměstnání by měli být náležitě prověřováni, zejména pokud se jedná o citlivá pracovní místa v rámci ČZU. Citlivá pracovní místa v rámci ČZU identifikuje personální odbor ČZU nebo bezpečnostní manažer ČZU.

9. 4. Školení zaměstnanců

Všichni zaměstnanci a uživatelé ze strany smluvních partnerů třetích stran by měli absolvovat odpovídající školení (v rámci všeobecného vzdělávání zaměstnanců nebo zvlášť organizované OIKT ČZU) týkající se zásad a postupů v oblasti bezpečnosti informací IS ČZU, včetně seznámení se s bezpečnostními požadavky na ně kladenými a dalšími opatřeními a důsledky.

9. 5. Bezpečnostní incidenty

Všichni zaměstnanci ČZU, studenti ČZU a smluvní strany, by měli být seznámeni a znát postupy hlášení různých typů incidentů (narušení bezpečnosti, možné hrozby, slabiny nebo chybné fungování IS), které by mohly mít dopad na bezpečnost aktiv ČZU. Zjištěné bezpečnostní incidenty nebo podezření na ně by měli ihned hlásit bezpečnostnímu správci IS, bezpečnostnímu manažerovi ČZU nebo svému nadřízenému.

10. Fyzická bezpečnost a bezpečnost prostředí

10. 1. Bezpečnostní zóny

Prostředky IKT ČZU, které podporují kritické nebo citlivé činnosti ČZU musí být umístěny v bezpečných zónách. Tyto prostředky by měly být rovněž fyzicky chráněny proti neautorizovanému přístupu, poškození, haváriím nebo jinému nebezpečí. Měly by být umístěny v bezpečných zónách, chráněny určeným bezpečnostním perimetrem s příslušnými kontrolami vstupu a bezpečnostními zábranami.

10. 2. Zabezpečení zařízení IS ČZU

Při zabezpečení zařízení IS třeba respektovat zejména:

a) Výběr a návrh místnosti musí brát v úvahu možnost poškození požárem, zatopením, výbuchem i jinými druhy přírodních nebo lidských hrozeb.

b) Důležitá zařízení IS ČZU musí být umístěna tak, aby nebyla veřejně dostupná (řízený přístup), dveře a okna musí být uzavíratelná.

c) V místnostech se zařízeními nesmí být umístěny nebezpečné nebo snadno hořlavé látky, pro tyto látky musí být určeny speciální lokality s charakterem zabezpečení protipožární ochrany.

d) Zařízení musí být chráněna proti ztrátě, poškození nebo proti jinému ohrožení aktiv ČZU, které by způsobily hmotnou újmu ČZU nebo přerušení činnosti organizace. Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.

e) Důležitá zařízení musí být chráněna před výpadkem elektrického proudu nebo před jinými odchylkami.

f) Pro zajištění dostupnosti a integrity musí být zařízení udržováno v souladu s pokyny výrobce nebo dokumentovanými postupy.

g) Pro ochranu zařízení ČZU, které je použito mimo objekty ČZU, musí být uplatněny relevantní bezpečnostní postupy a opatření.

h) Zařízení, která se používají mimo lokality ČZU, podléhají schválení příslušnému vedoucímu zaměstnanci a jejich stupeň zabezpečení by měl být stejný jako pro ekvivalentní prostředky v lokalitách ČZU.

i) Před tím, než je zařízení zničeno nebo opakovaně použito (např. poskytnuté jiné straně), musí být informace v něm uložené úplně zničeny bez možnosti obnovení (jednoduché vymazání není postačující).

j) Zařízení nesmí být ponechána bez dozoru nebo zabezpečení. Musí být respektovány bezpečnostní pokyny výrobce a další potřebná bezpečnostní opatření.

11. Správa informační a komunikační techniky, sítí a informačních systémů

Správu informačních a komunikačních technologií a současně celého informačního systému na ČZU i všech jejích částech zajišťuje Odbor informačních a komunikačních technologií ČZU nebo jím pověřená osoba (dále jen OIKT ČZU).

11. 1. Provozní postupy a odpovědnosti

Pro zajištění správného a bezpečného provozu počítačů a síťových prostředků v rámci IS ČZU musí být stanoveny pravomoci, odpovědnosti a postupy pro řízení a správu všech počítačů a sítí, které spadají do IS ČZU. Tyto činnosti musí být podporovány vhodnými interními řídícími dokumenty a postupy při reakci na incidenty. V případě potřeby je nutno uplatňovat princip oddělení povinností, aby se snížilo riziko úmyslného zneužití systému nebo zneužití z nedbalosti.

11. 2. Plánování a schvalování IS ČZU

Pro zajištění dostupnosti IS ČZU, patřičného výkonu systému a přiměřených zdrojů je nutné provedení plánovacích a přípravných činností před tím, než je IS ČZU uveden do provozu. OIKT ČZU (a dále i jeho podřízené složky) ve spolupráci s jednotlivými odbory nebo odděleními musí vypracovat odhad budoucích požadavků na kapacitu, aby se snížilo riziko přetížení systému. Měly by být stanoveny provozní požadavky na nové části systému v rámci IS ČZU, zdokumentovány a před jejich přijetím také otestovány. Měla by být provedena analýza potřeby na řešení havarijních situací u služeb, které podporují více aplikací a tato analýza by měla být pravidelně posuzována.

11. 3. Antimalwarová ochrana

Pro předcházení a detekování škodlivého programového vybavení (malware – viry, trojské koně, spyware, adware atd.), působícího v rámci IS ČZU jsou vyžadována patřičná opatření. Pracovníci OIKT ČZU musí věnovat pozornost možnému nebezpečí škodlivého programového vybavení a v případě potřeby ve spolupráci s bezpečnostními správci IS a bezpečnostním manažerem vypracovat a aplikovat zvláštní opatření pro jeho předcházení a detekování. Zejména je nezbytné, aby se učinila opatření pro předcházení a detekování počítačových virů na osobních počítačích a serverech ČZU.

11. 4. Organizačně administrativní opatření

Pro udržení integrity a dostupnosti služeb IKT ČZU musí být vytvořena patřičná administrativní opatření. Běžná praxe v rámci postupů IS ČZU musí zahrnovat pravidelné pořizování záložních kopií dat, vedení záznamů o provozu a chybách v systému a v případě potřeby monitorování okolí zařízení IS ČZU.

11. 5. Správa prostředí IS ČZU

Mezi jeden z nejdůležitějších úkolů v rámci bezpečnosti informací je zajištění ochrany informací v počítačových sítích ČZU a zabezpečení infrastruktury správy systému. Správa bezpečnosti počítačových sítí, které přesahují hranice hlavní lokality ČZU, vyžaduje zvláštní pozornost. Speciální opatření jsou ČZU požadována pro zabezpečení citlivých dat přenášených veřejnými sítěmi, zejména při komunikaci s bankami nebo smluvními partnery ČZU.

11. 6. Bezpečnost práce s médii

Při práci s médii je nutno předcházet poškození aktiv ČZU a přerušení činnosti. Počítačová média musí být chráněna a fyzicky zabezpečena. Proto musí být také stanoveny náležité provozní postupy týkající se zabezpečení počítačových médií (pásky, disky, kazety), vstupních/výstupních dat a systémové dokumentace před poškozením, krádeží, zneužitím nebo neoprávněným přístupem.

11. 7. Bezpečnost dat a programového vybavení

V rámci IS ČZU musí být změna dat a programového vybavení smluvními partnery pod odpovídající kontrolou. Tyto změny musí být prováděny na základě platných formálních dohod. OIKT ČZU a právním oddělením ČZU musí být stanoveny postupy a standardy pro ochranu dat při přepravě a přenosu. Pozornost by měla být věnována možným dopadům na bezpečnost a činnost ČZU v souvislosti s elektronickou výměnou dat a elektronickou poštou, jako i požadavkům na bezpečnostní opatření.

11. 8. Soukromá zařízení a IS ČZU

Používání soukromých počítačů, softwaru, periferních zařízení a jiného vybavení podléhá interním bezpečnostním předpisům a zásadám bezpečnostních politik ČZU. Tato zařízení musí splňovat celkovou bezpečnostní politiku ČZU. V opačném případě nebudou připojena k prostředkům informačního a komunikačního systému univerzity. Případné výjimky na základě písemné žádostí uděluje bezpečnostní manažer ČZU.

11. 9. Správa sítí ČZU a Internet

Připojení počítačů a dalších zařízení k sítí ČZU a Internetu podléhá schválení a kontrole OIKT ČZU a realizuje se výhradně prostřednictvím bezpečných rozhraní, na kterých jsou trvale spuštěna a realizována bezpečnostní opatření, která zabraňují útokům a neoprávněným použitím (např. detekce průniků, firewall, antimalwarové programy, filtrace adres, regulace pošty a další). Počítače, které nesplňují bezpečnostní kritéria určené bezpečnostní dokumentací nebudou do sítě ČZU připojena. Zařízení, která byla již připojena a z nějakého důvody přestala splňovat bezpečnostní kritéria, mohou být od sítě odpojena.

12. Systém řízení přístupu

12. 1. Přístup k IS ČZU

Pro zajištění odpovídajících bezpečnostních požadavků na IS ČZU musí být zajištěno řízení přístupu k aktivům spravovaných IS ČZU. Přístup k počítačovým službám a datům IS ČZU by měl být řízen na základě provozních požadavků, definovaných bezpečnostním manažerem a OIKT ČZU společně s požadavky jednotlivých součástí ČZU. V úvahu by se měly vzít principy šíření informací v rámci ČZU i mimo ní a potřeba přístupu k informacím ze strany oprávněných uživatelů.

12. 2. Uživatelský přístup k IS ČZU

Pro předcházení neoprávněnému přístupu k jednotlivým aktivům IS ČZU, musí existovat formální postupy pro přidělování uživatelských práv ke službám IKT. Postupy by měly pokrývat všechny etapy v životním cyklu uživatelského přístupu k IS ČZU (např. využití Identity Managementu), od prvotní registrace nového uživatele až po konečné zrušení registrace uživatele, který přístup ke službám IKT ČZU již dále nepotřebuje. V případě potřeby by měla být věnována zvláštní pozornost potřebě řídit přidělování práv privilegovaného přístupu, který umožňuje uživatelům překročit systémová opatření.

12. 3. Bezpečnost přístupu k síti

Bezpečnost připojení k síťovým službám IS ČZU by měla být řízena tak, aby bylo zajištěno, že připojení uživatelé nebo počítačové služby IS neohrožují bezpečnost jakýchkoliv dalších síťových služeb. Řízení by mělo zahrnovat zejména následující:

a) Náležité propojení mezi síťovými službami.

b) Patřičný mechanismus autentizace pro vzdálené uživatele a zařízení.

c) Řízení přístupu uživatelů ke službám IKT.

12. 4. Bezpečnost přístupu k počítačům

Přístup k jednotlivým počítačovým zařízením a prvkům by měl být řízen tak, aby byl umožněn přístup k IS ČZU pouze oprávněným uživatelům. Počítače, které využívá více uživatelů, by měly být schopné zejména:

a) Identifikovat a ověřit totožnost, a kde je to nezbytné, také PC, terminál nebo lokalitu každého oprávněného uživatele v rámci IS ČZU.

b) Zajistit, aby každý uživatel, který počítač využívá měl vlastní uživatelský účet a bylo jednoznačně možné určit, kdo dané zařízení v dané době obsluhoval.

c) Zaznamenávat úspěšné a neúspěšné pokusy o přístup k IS ČZU.

d) Umožňovat využívání systému správy hesel pro přístup k IS ČZU zajišťujícího bezpečná a silná hesla.

e) V případě potřeby omezit pro uživatele dobu spojení k IS ČZU.

12. 5. Bezpečnost přístupu k aplikacím

Pro předcházení neoprávněnému přístupu k informacím uložených v IS ČZU, musí být přístup k aplikačním systémům a datům řízen pomocí logického řízení přístupu. Logický přístup k programovému vybavení a datům počítačů nebo systémů by měl být omezen pouze na oprávněné uživatele IS ČZU.

Aplikační systém by měl zejména:

a) Řídit přístup uživatelů k datům a funkcím aplikací IS ČZU, v souladu s definovanou politikou řízení přístupu v rámci IS ČZU.

b) Poskytovat ochranu před neoprávněným přístupem k programovým nástrojům IS ČZU, které umožňují překročit systémová a aplikační opatření.

c) Zajistit bezpečnost jiných systémů, se kterými jsou sdíleny zdroje IKT.

12. 6. Monitorování přístupu k IS ČZU

Pro detekci neoprávněné činnosti, prováděné v rámci IS ČZU, musí být jednotlivé systémy IS ČZU monitorovány a kontrolovány tak, aby byl zajištěn soulad s politikou řízení přístupů IS ČZU a shoda s doporučenými bezpečnostními standardy. Toto opatření je nezbytné pro stanovení efektivity přijatých opatření a pro zajištění souladu s modelem politiky přístupu IS ČZU. Monitorování přístupu k IS ČZU ve smyslu toho odstavce zabezpečuje a koordinuje Odbor informačních a komunikačních technologií ČZU.

Kontrola a monitorování ve smyslu tohoto odstavce nezahraňuje monitorování obsahu přenášených dat (např. obsahu zpráv elektronické komunikace), musí být v souladu s platnou legislativou ČR, aby nebylo bezdůvodně narušováno právo uživatele na soukromí.

13. Vývoj a údržba

13. 1. Bezpečnostní požadavky na IS ČZU

Pro zajištění implementace bezpečnostních protiopatření do jednotlivých částí a systémů IKT, musí být určeny jednotlivé na ně kladené bezpečnostní požadavky, které jsou odsouhlaseny bezpečnostním manažerem a OIKT ČZU, ještě před vlastním vývojem systémů IKT v rámci IS ČZU. Z ekonomických důvodů musí být bezpečnostní opatření zahrnuta do aplikačního podsystému IS ČZU již ve fázi jeho specifikace a návrhu. Všechny bezpečnostní požadavky, včetně požadavků na havarijní

zpracování IS ČZU, by měly být určeny při definici požadavků na projekt a měly by být odsouhlaseny a zdokumentovány jako součást celkového odůvodnění potřeby IS ČZU.

13. 2. Bezpečnost vývoje a údržby aplikací IS ČZU

Pro předcházení ztráty, modifikace nebo jiného zneužití uživatelských dat v aplikacích IS ČZU musí být do nově vyvíjených aplikačních podsystémů IS ČZU navržena vhodná bezpečnostní opatření, včetně souboru inspekčních záznamů. OIKT ČZU musí zajistit, že návrh a provozování IS ČZU splňuje průmyslové a bezpečnostní standardy týkající se správných a doporučených bezpečnostních postupů daných bezpečnostní dokumentací. Pro části IS ČZU, které zpracovávají nebo mají vliv na zvláště citlivá, hodnotná nebo kritická aktiva mohou být požadována a realizována dodatečná opatření. Taková opatření by měla být stanovena bezpečnostním manažerem ČZU a bezpečnostním správcem IS na základě doporučení (i externích) bezpečnostních specialistů, jakož i určených bezpečnostních hrozeb a možného dopadu těchto hrozeb.

14. Bezpečnost přístupu třetích stran

Všechny přístupy třetích stran k informacím ČZU musí být smluvně ošetřeny nebo musí být jiným způsobem zajištěna ochrana těchto informací. Vyplývající rizika musí být ještě před umožněním takového přístupu identifikována a náležitě ošetřena.

Příkladem takového přístupu může být dodávka nového informačního systému (popis procesů, specifikace, data pro testování atd.) stejně jako přístup uklízecí nebo bezpečnostní služby do prostor ČZU.

Smlouvy musí obsahovat z hlediska bezpečnosti zejména:

a) Obecná pravidla bezpečnosti.

b) Ochranu aktiv.

c) Opatření umožňující ukončení nebo změnu smluvního vztahu bez bezpečnostního rizika.

d) Pravidla pro utajení, nešíření informací, neporušení integrity a dostupnosti aktiv.

e) Specifikaci každé zpřístupněné služby a její úrovně.

f) V případě potřeby podmínky vzájemného přechodu, příp. odchodu personálu třetí strany.

g) Konkrétní smluvní závazky.

h) Odpovědnosti smluvené a vyplývající z právních norem.

i) Ochranu duševního vlastnictví a autorského práva.

j) Podmínky, metody a oblasti přístupu.

k) Právo monitorovat a povolovat aktivity uživatele a/nebo zaměstnance třetí strany.

l) Právo kontrolovat smluvní povinnosti.

m) Pravidla pro řešení havarijních situací.

n) Odpovědnost za práci a vlastní produkty.

o) Systém hlášení a komunikace v oblasti bezpečnosti.

p) Pravidla procesu řízení změn.

15. Dodržování zákonných a jiných ustanovení

15. 1. Platná legislativa pro IS ČZU

Pro vyloučení porušení zákonných, trestních, případně i občanských povinností, musí být návrh, provoz a používání IS ČZU v souladu se zákonnými nebo smluvními bezpečnostními požadavky.

Pro IS ČZU musí být tyto požadavky vypracovány OIKT ČZU tak, aby bylo zajištěno, že veškeré odpovídající zákonné a smluvní požadavky jsou explicitně vyjádřeny a podchyceny. Odpovídající legislativní požadavky musí vycházet hlavně ze zákona o ochraně autorských práv ve znění vyhlášeném předpisem č. 121/2000 Sb., Zákona o ochraně osobních údajů č. 101/2000 Sb. a dalších předpisů.

15. 2. Kontrola a inspekce bezpečnosti IS ČZU

V průběhu všech fází životního cyklu jednotlivých částí a systémů IS ČZU musí být ze strany bezpečnostního inspektora IS zajištěn pravidelná inspekce (minimálně jednou za rok) shody IS ČZU s bezpečnostní politikou informací ČZU a bezpečnostními standardy. Dále musí být podána zpráva fóru pro bezpečnost informací a rektoru ČZU. Bezpečnost IKT by měla být pravidelně kontrolována také pracovníky OIKT ČZU a bezpečnostním manažerem ČZU.

Tyto kontroly a inspekce by měly být zaměřeny na identifikaci neshody s příslušnou bezpečnostní politikou ČZU, technickými platformami prostředků IKT a s bezpečnostními standardy implementace IS ČZU.

16. Kritéria hodnocení rizik

Bezpečnostní opatření jsou vybrána na základě prováděného hodnocení rizik a požadavků zákonných norem.

Hodnocení rizik je prováděno zejména na základě následujících kritérií:

a) Stanovení hodnot informačních aktiv ČZU z hlediska požadavků na jejich dostupnost, důvěrnost a integritu.

b) Určení požadavků relevantní legislativy a požadavků vyplývajících z uzavřených smluvních vztahů.

c) Určení možných dopadů identifikovaných hrozeb, reálné pravděpodobnosti jejich uskutečnění a určení úrovně rizik pro aktiva ČZU.

d) Určení akceptovatelné úrovně rizika pro informační aktiva ČZU.

17. Plánování kontinuity

Pro udržení nebo obnovení provozu IS ČZU v požadovaném čase po přerušení nebo selhání kritických procesů musí být vytvořeny plány obnovení činností IS ČZU.

V procesu plánování kontinuity činností se zejména zvažuje:

a) Určení a odsouhlasení všech odpovědností a nouzových postupů.

b) Zavedení nouzových postupů tak, aby bylo možné dokončit zotavení a obnovu v požadovaných lhůtách. Zvláštní pozornost je třeba věnovat ohodnocení vnějších závislostí ČZU a existujícím smlouvám.

c) Dokumentace odsouhlasených procedur a postupů.

d) Vhodné proškolení personálu o odsouhlasených havarijních procedurách a postupech, včetně krizového řízení.

e) Testování a aktualizace plánů.

Proces plánování se musí soustředit na požadované cíle, např. obnovení specifických služeb ČZU v akceptovatelné době. Měly by být zváženy všechny služby a zdroje, kterých by se toto mohlo týkat, včetně zaměstnanců, studentů, zdrojů nepředstavujících prostředky pro zpracování informací, jakož i náhradních prostředků pro zpracovávání informací.

Plán kontinuity IS ČZU by měl jasně specifikovat podmínky své aktivace, stejně jako osoby s odpovědností za vykonávání každého bodu plánu. Při vzniku nových požadavků by havarijní postupy, jako např. evakuační plány nebo jakékoliv existující smlouvy o zajištění náhradního provozu, měly být adekvátním způsobem doplněny. Systém plánování kontinuity by měl brát v úvahu zejména následující:

a) Podmínky aktivace plánů, které popisují postup, který by se měl dodržovat (jak vyhodnotit situaci, kdo aktivaci provede atd.), než dojde k aktivaci plánu.

b) Postupy obnovy popisující činnosti pro přesun důležitých aktivit ČZU.

c) Postupy popisující způsob opětovného uvedení procesů univerzity do normálního provozu.

d) Harmonogram údržby určující, jak a kdy bude plán testován, a proces aktualizace plánu.

e) Vzdělávací aktivity a aktivity k zlepšení povědomí určené pro vytvoření porozumění procesů plánování kontinuity a pro zajištění jejich efektivního průběhu.

f) Individuální odpovědnosti popisující, kdo odpovídá za kterou složku plánu. Mohou být podle potřeby stanoveny alternativy.

Každý plán musí mít stanoveného garanta.

Plány kontinuity IS ČZU mohou při testech selhat z důvodů nesprávných předpokladů, přehlédnutí nebo změn zařízení nebo personálu. Proto by měly být testovány pravidelně, aby se zajistila jejich aktuálnost a efektivita.

Takové testy rovněž zajišťují, že všichni členové havarijního týmu i ostatní relevantní personál má plány v povědomí.

Harmonogram testů plánů kontinuity stanovuje, jak a kdy je každý prvek plánu testován, různými testovacími technikami. Zejména se jedná o:

a) Ověření různých scénářů od stolu (projednání plánů obnovy IS ČZU podle příkladů různých narušení).

b) Simulace (zejména pro výcvik lidí s řídícími pozicemi v obnovovacích a krizových týmech).

c) Technické testy obnovy (prověření, zda IS ČZU mohou být efektivně obnoveny).

d) Testování externě zajišťovaných zařízení a služeb (prověření, že externě poskytované služby a produkty splňují smluvní podmínky).

e) Generální zkoušky (testování toho, zda a jak se organizace, personál, zařízení, prostředky a procesy mohou s přerušeními vypořádat).

Je nezbytné zajistit neustálou efektivnost plánů kontinuity. Stanovuje se odpovědnost za provádění pravidelných revizí každého plánu kontinuity. Po změně podmínek na univerzitě, které se ještě neodrazily v plánech kontinuity, by měla proběhnout odpovídající aktualizace těchto plánů.

18. Regulatorní, legislativní a smluvní požadavky na bezpečnost informací

Přehled dokumentů EU s ohledem na povinnosti ochrany informací osob:

a) Směrnice Evropského parlamentu a Rady 95/46/ES o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

b) Směrnice Evropského parlamentu a Rady 99/93/ES o zásadách Společenství pro elektronické podpisy.

Přehled vybraných zákonů a jiných právních předpisů s důrazem na povinnosti při ochraně informací:

a) Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

b) Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.

c) Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

d) Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů.

e) Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů.

f) Zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů.

g) Zákon č. 337/1992 Sb., o správě daní a poplatků, ve znění pozdějších předpisů.

h) Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).

i) Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

j) Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

k) Nařízení vlády č. 495/2004 Sb., kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.

Specifické povinnosti pro oblast bezpečnosti informací jsou stanoveny zejména v následujících oblastech:

a) Administrace autentizační a autorizační informace.

b) Ochrana soukromého klíče držitelů kvalifikovaných (zaměstnaneckých) certifikátů.

c) Ochrana hesla pro zneplatnění kvalifikovaných (zaměstnaneckých) certifikátů.

d) Řízení vztahů bezpečnosti s externími zpracovateli podle zvláštního právního předpisu.

e) Řízení vztahů bezpečnosti s externími poskytovateli služeb podle zvláštního právního předpisu.

f) Poskytování informací Národnímu bezpečnostnímu úřadu podle zvláštního právního předpisu.

g) Poskytování informací Policii České republiky podle zvláštního právního předpisu.

h) Poskytování informací zpravodajským službám podle zvláštního právního předpisu.

i) Předávání osobních údajů do třetích zemí podle zvláštního právního předpisu.

j) Poskytování informací správcům daně podle zvláštního právního předpisu.

k) Poskytování informací zdravotním pojišťovnám podle zvláštního právního předpisu.

l) Poskytování informací příslušné organizační složce Ministerstva školství podle zvláštního právního předpisu.

m) Ochrana informací, které jsou předmětem bankovního tajemství podle zvláštního právního předpisu.

19. Sankce

a) Nedodržení bezpečnostních řídících předpisů může být kvalifikováno jako porušení povinností zaměstnance ČZU, příp. porušení pracovní kázně s příslušnými důsledky pro zaměstnance, ve smyslu zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, pokud se nejedná o přestupek podle § 44 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, nebo trestný čin podle § 178 zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů.

b) Sankce za porušení bezpečnostních řídících předpisů studentem ČZU se řídí § 64 až 69 zákona č. 111/1998 Sb. o vysokých školách a disciplinárním řádem ČZU.

c) Porušení bezpečnostních řídících předpisů zástupci externích subjektů, třetími stranami a sankce z toho vyplývající řeší smlouvy s těmito subjekty a zákonné předpisy.

20. Závěrečná ustanovení

a) BPI ČZU nabývá platnosti a účinnosti dne 1. 3. 2008.

b) Případné výjimky z pravidel obsažených v tomto dokumentu musí být s vysvětlením jejich opodstatnění předloženy ke zvážení bezpečnostnímu manažerovi ČZU, který může pro jejich posouzení iniciovat proces analýzy rizik. Výjimka může být udělena jen v odůvodněných případech. Pokud jsou výjimky uděleny, musí být minimálně každých 6 měsíců přezkoumány, zda nepominuly důvody pro jejich udělení a zda se nemění úroveň rizik. Neakceptovatelné zvýšení rizik je důvodem pro neudělení nebo zrušení výjimky.

c) Změny uvedených pravidel budou prováděny na základě doporučení fóra pro bezpečnost informací ČZU a bezpečnostního manažera ČZU.