Klasifikace informací: Interní

PRAVIDLA PRO ZÁLOHOVÁNÍ A ARCHIVACI DAT

ČESKÉ ZEMĚDĚLSKÉ UNIVERZITY V PRAZE

Verze 2.0

2008

PRAVIDLA PRO ZÁLOHOVÁNÍ A ARCHIVACI DAT

ČESKÉ ZEMĚDĚLSKÉ UNIVERZITY V PRAZE

Verze	2.0
Účinnost od	1. 3. 2008
Klasifikace	Interní
Počet stran	9
Garant	Šup Libor, Bc., bezpečnostní technik ICT
Zpracoval	Šup Libor, Bc., bezpečnostní technik ICT Hradecký Ondřej, Ing., vedoucí odboru 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.
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

Vedení České zemědělské univerzity v Praze (dále ČZU) si uvědomuje důležitost zajištění bezpečnosti informačních systémů, informačních technologií a informací, které ČZU využívá pro naplnění svých cílů. Následující zásady, pravidla a odpovědnosti pro zajištění bezpečného zálohování a archivaci dát naplňují tento záměr.

2. Působnost

Dokument „Pravidla pro zálohování a archivaci dat České zemědělské univerzity v Praze“ (dále PZAD ČZU) definuje pravidla bezpečnostního zálohování a archivaci dát.

PZAD ČZU jsou určeny pro uživatele, administrátory a další specifikované role v IS ČZU, které využívají zálohování a archivací dat nebo se podílejí na jejich zajištění.

3. Východiska

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

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

4. Úvodní ustanovení

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 dokumentu 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.

5. Všeobecná pravidla

5. 1. Vytváření dat

Data mohou být v IS ČZU vytvořena nebo pořízena zejména vlastní tvorbou (uživatelská a databázová data), vlastním vývojem (programové vybavení), instalací (systémové a programové vybavení), zkopírováním z IS jiných subjektů či z Internetu (všechny typy dat) anebo mohou být vytvořena automaticky (záznamy událostí).

5. 2. Ukládání dat

Pro všechny typy dat, která slouží pro účely ČZU (dále pracovní data) platí, že musí mít definovaného vlastníka (zodpovědného za klasifikaci informací a definování přístupových práv k datům) – dokument „Pravidla pro klasifikaci informací“. Dle této klasifikace a určení jsou data ukládána buď na síťové nebo lokální disky zařízení.

V rámci IS ČZU je uživatelům IS tolerováno v přiměřené a únosné míře ukládání osobních (nepracovních) dat, avšak jen na lokálních discích pracovních stanic a mobilní výpočetní techniky a dále jen za podmínek, že výkon, účinnost, bezpečnost a dostupnost systémů, aplikací a pracovních dat ČZU nebudou tímto nijak omezeny nebo sníženy.

V rámci IS ČZU je zakázáno vytvářet nebo ukládat (kopírovat) data odporující zákonům ČR, normám a předpisům ČZU, dobrým mravů nebo obsahující jakékoli druhy pornografie, informace vedoucí k propagaci násilí, fašismu, rasismu a xenofobie, ohrožující práva a důstojnost osob nebo poškozující zájmy ČZU nebo České republiky.

5. 3. Zálohování dat

Zálohování dat slouží jako prostředek zajištění dostupnosti a integrity dat. V případě smazání původních dat, nebo jejich nežádoucí modifikace a v případě havárie IS slouží záložní data k obnovení původního, nebo zajištění záložního provozu dotčené části IS. Periodicita zálohování musí odrážet změny v datech i v konfiguraci IT. Administrátor každého IS je odpovědný za provádění zálohy a její testování pro případ obnovy.

5. 4. Archivace dat

Účelem vytváření archivů dat je jejich dlouhodobé uchování v nezměněné podobě ke dni jejich vyhotovení a slouží zejména pro účely kontroly.

6. Manipulace a ukládání dat v rámci IS ČZU

6. 1. Uživatelská data

Uživatelská data jsou taková data, která uživatel vytváří a ukládá mimo hlavní aplikace a databáze IS ČZU. Jedná se především o soubory z aplikací kancelářského balíku MS Office.

Uživatelská pracovní data musí být primárně vytvářena a ukládána na k tomu účelu vyhrazených síťových nebo lokálních discích. Pokud toto není možné technicky zabezpečit, data musejí být uživateli na síťové disky pravidelně kopírována (replikována) a aktualizována (synchronizována).

Pokud se jedná o data klasifikovaná, je zacházení s nimi a jejich označování popsáno a řešeno samostatným řídícím dokumentem – „Pravidla pro klasifikaci informací“.

6. 2. Aplikační a databázová data

Aplikační a databázová data jsou taková data, která uživatelé vytvářejí a ukládají prostřednictvím hlavních aplikací IS ČZU. Ukládání aplikačních a databázových dat musí být primárně zajištěno na k tomu účelu vyhrazených síťových discích. Pokud toto ukládání není možné ve výjimečných případech technicky zabezpečit, data musejí být na síťové disky pravidelně kopírována (replikována) a aktualizována (synchronizována) z lokálních disků pracovních stanic a mobilní výpočetní techniky. VE výjimečných případech lze tato data ukládat na discích lokálních.

Přístup uživatelů k aplikačním a databázovým datům IS ČZU je řízen interní směrnicí „Zásady řízení přístupu k IS“, která definuje formální proces žádostí, dokumentace, evidence a správy uživatelských oprávnění k informačním zdrojům IS.

6. 3. Systémové a programové vybavení

Systémové a programové vybavení může být v rámci IS ČZU vytvářeno a ukládáno pouze instalací nebo zkopírováním z vyhrazených instalačních zdrojů příslušnými administrátory IS. Uživatelé IS mají zakázáno instalovat nebo kopírovat jakékoliv systémové a programové vybavení a měnit jejich bezpečnostní parametry.

Administrátoři IS a externí dodavatelé služeb IS mohou instalovat pouze programové vybavení schválené a doporučené vedoucím OIKT ČZU a bezpečnostním manažerem ČZU.

Externí dodavatelé služeb IS mohou navíc instalovat nebo kopírovat systémové a programové vybavení pouze za osobní účasti příslušného administrátora IS.

a) Instalace na lokální disky - tuto instalaci na pracovní stanice a mobilní výpočetní techniku smí provést pouze administrátor IS a to v případě, že se jedná o jednouživatelské programové vybavení.

b) Instalace na síťové disky - pokud je třeba programy sdílet v rámci IS ČZU, je nutné, aby administrátoři IS provedli instalaci na síťový disk a vytvořili příslušnou uživatelskou skupinu.

6. 4. Záznamy událostí

Záznamy o významných událostech a chybách na úrovni operačních systémů, aplikací a databází, síťové komunikace či přístupu ke zdrojům IS jsou vytvářeny za účelem administrátorského a bezpečnostního monitoringu, kontroly a zpětného dohledání nestandardních provozních situací.

Každá část, služba nebo aplikace IS by měla mít nastaveno automatické logování minimálně těchto událostí:

a) Start a ukončení chodu systému.

b) Chyby systému a podniknuté nápravné kroky.

c) Evidence o manipulaci s důležitými záznamy, datovými soubory nebo médii.

d) Identifikace osob provádějících výše uvedené operace.

Pro aplikace, databáze a uživatelská data postačí zpravidla nastavení logování pouze typu a) a b).

Pro aplikace a databáze, zpracovávající klasifikovaná data, nebo uživatelská klasifikovaná data musí být nastaveno logování všech 4 typů záznamů a), b), c) a d).

Přístup k záznamům musí být nastaven pouze pro administrátora IS, bezpečnostního správce IS a bezpečnostního manažera ČZU tak, aby měli oprávnění pouze číst tyto záznamy bez jejich modifikace nebo smazání. Pokud toto nelze technicky zajistit, musí být aktivováno podrobné logování všech přístupů a operací s vybranými bezpečnostními záznamy.

7. Zálohování a archivace dat

Veškerá zálohovaná a archivovaná data, bez ohledu na médiu (nosiči) jsou uložena, jsou klasifikována stupněm který odpovídá informacím na nich uložených (vždy dle nejvíce citlivé informace). Nakládání s takovými daty, stejně tak jako jejich značení definuje interní řídící dokument – „Pravidla pro klasifikaci informací“.

Pravidla pro klasifikaci informací a dat ukládají zejména povinnost stanovit okruh osob oprávněných k přístupu a manipulaci se záložními a archivačními médii, povinnost označovat každé záložní médium a vést evidenci ukládání a manipulace se záložními médii u každého z úložišť (trezor, zálohovací knihovna apod.).

7. 1. Pravidelné denní zálohy serverů a dat

Na závěr každého pracovního dne musí být v nočních hodinách provedeny „Increment“ „On-Site“ zálohy přírůstků a změn dat na všech serverech, u kterých je zálohování nutné provádět (případně „Full-Backup zálohy, kde není možné zálohovat přírůstkově). Pásky s denními zálohami je třeba uchovávat min. 14 dní a po této lhůtě je možné tyto pásky recyklovat (přepisovat).

7. 2. Pravidelné týdenní zálohy serverů a dat

V průběhu víkendu se realizují plné „Full-backup“ „On-Site“ zálohy všech dat na všech serverech, , u kterých je zálohování nutné provádět, s dobou uchování minimálně 14 dnů.

7. 3. Pravidelné čtvrtletní archivy dat

Pravidelně každé 3 měsíce se musí vytvořit plný „Full-backup“ archiv všech dat na všech serverech, u kterých je zálohování nutné provádět. Tento archiv se musí uchovat minimálně po dobu 1 roku.

7. 4. Pravidelné roční archivy dat

Na začátku kalendářního roku (první pracovní týden) případně v jiném předem konkrétně stanoveném termínu se musí vytvořit plný „Full-backup“ archiv (Off-site) všech dat na všech serverech, u kterých je zálohování nutné provádět. Archiv se musí uchovat po dobu 5 let.

7. 5. Nepravidelné a jednorázové zálohy, archivy

U některých procesů v rámci IS ČZU existují, kromě pravidelných záloh a archivů, také požadavky na vytváření mimořádných archivů. Dále mohou být vytvořeny jednorázové zálohy některých serverů či aplikací z důvodu jejich reinstalace, upgrade apod.

Stejně jako v případě pravidelných záloh, musejí být mimořádné zálohy a archivy bezpečně uloženy dle typu a účelu (On-Site/Off-Site), evidovány v zálohovacím systému a pořízeny záznamy o manipulaci a přístupu k nim.

8. Závěrečná ustanovení

a) PZAD ČZU nabývá platnosti dnem 1. 3. 2008.

b) Případné výjimky z pravidel obsažených v tomto dokumentu musejí být s vysvětlením jejich opodstatnění předloženy ke schválení 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 přezkoumáno, zda nepominuly důvody pro jejich udělení a zda se nemění úroveň rizik. Neakceptovatelné zvýšení rizik je důvodem pro neudělení nebo zrušení výjimky.

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