

PRAVIDLA PRO KLASIFIKACI INFORMACÍ

ČESKÉ ZEMĚDĚLSKÉ UNIVERZITY V PRAZE



Verze 2.0

2008

PRAVIDLA PRO KLASIFIKACI INFORMACÍ ČESKÉ ZEMĚDĚLSKÉ UNIVERZITY V PRAZE

Verze	2.0
Účinnost od	1. 3. 2008
Klasifikace	Interní
Počet stran	18
Počet příloh	1
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.
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	5
2.	Působnost	5
3.	Východiska	5
4.	Úvodní ustanovení	5
5.	Cíl klasifikace informací a dat	6
5. 1.	Všeobecná pravidla	6
5. 2.	Cíl klasifikace	6
6.	Požadavky na klasifikaci informací	6
7.	Klasifikace informací ČZU	6
7. 1.	Role a odpovědnosti	6
7. 2.	Klasifikační schéma	8
7. 2. 1.	Stupně klasifikace informací ČZU	8
7. 2. 2.	Postup určování klasifikačního stupně a kategorie informací	10
7. 2. 3.	Reklasifikace informací	11
7. 3.	Zacházení s informacemi a jejich označování	11
7. 3. 1.	Označování informací	11
7. 3. 2.	Zacházení (manipulace) s informacemi ČZU	12
8.	Závěrečná ustanovení	18

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 klasifikace informací a bezpečného nakládání s informacemi naplňují tyto cíle.

2. Působnost

Dokument „Pravidla pro klasifikaci informací České zemědělské univerzity v Praze“ (dále PPKI ČZU) definuje pravidla pro nakládání s informacemi a současně s daty (dále jen informace) v působnosti všech procesů ČZU, a to bez ohledu na to, v jaké formě a na jakém médiu se vyskytují.

3. Východiska

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

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

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 směrnících fakult a dalších součástí univerzity. Takové směrnice jsou podřízeny tomuto řádu a navazujícím interním řídicím 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. Cíl klasifikace informací a dat

5.1. Všeobecná pravidla

Informace a data (dále informace) mají různý stupeň citlivosti a mohou být různě kritické. Některé mohou vyžadovat vyšší úroveň bezpečnosti nebo zvláštní způsob zacházení. Proto musí být vytvořena pravidla pro klasifikaci informací, včetně určení definování stupňů klasifikace, na základě kterých mohou být informace rozdělovány, stanovovány požadavky na jejich ochranu a které dávají uživatelům informaci o nutnosti zvláštního zacházení s nimi. Zavedení klasifikace informací je tak nástrojem pro zajištění přiměřenosti ochrany informačních aktiv ČZU.

5.2. Cíl klasifikace

Cílem dokumentu je zajistit ochranu všech informací ČZU, a to adekvátně v závislosti na jejich kritičnosti, citlivosti a hodnotě, bez ohledu na to, na jakém médiu, resp. nosiči se informace vyskytují (listinná či jiná materiální podoba, elektronická podoba - dokumenty, obrazová data, zvukové záznamy apod.) a dále bez ohledu na to, zda jsou zpracovávány automatizovaně nebo ručně.

6. Požadavky na klasifikaci informací

Klasifikace informací a jí odpovídající bezpečnostní opatření musí brát ohled na potřeby univerzity, na sdílení informací nebo omezování přístupu k nim a především na výši potencionálních negativních dopadů při narušení jejich bezpečnosti.

Informace a výstupy ze systémů, které zpracovávají klasifikované informace, musí být označovány v souladu s jejich hodnotou a citlivostí. Výjimky v označování určuje tento příkaz.

Pro značení informací a zacházení s nimi je důležité definovat soustavu postupů v souladu s klasifikačním schématem, které bylo pro ČZU přijato. Tyto postupy musí pokrývat informační aktiva ve fyzické i elektronické podobě. Manipulační postupy by měly být definovány pro každou úroveň klasifikace tak, aby pokrývaly veškeré typy zpracování informací.

7. Klasifikace informací ČZU

7.1. Role a odpovědnosti

Celkovou odpovědnost za realizaci zásad klasifikace informací v ČZU má bezpečnostní manažer ČZU, který se za svou činnost zodpovídá vedení univerzity a fóru pro bezpečnost informací ČZU. Za realizaci technologických opatření v rámci IS ČZU odpovídá vedoucí OIKT ČZU a přeneseně bezpečnostní správce IS a administrátoři IS.

Jsou-li pochybnosti, do jakého klasifikačního stupně bezpečnosti osobní údaje spadají, je nutné navržený stupeň bezpečnosti konzultovat s bezpečnostním manažerem ČZU.

Zaměstnanci ČZU jsou odpovědní za ochranu informací ČZU před neautorizovaným přístupem, neoprávněnou modifikací, zničením nebo vyzrazením, ať již v důsledku úmyslného nebo neúmyslného jednání či nehody. Tuto povinnost mají i studenti ČZU, kteří se dostanou do styku s klasifikovanými informacemi ČZU.

Z pohledu klasifikace informací jsou v ČZU následující role pracovníků:

Role	Definice role
Vlastník/Garant	• Vedoucí oddělení/vedoucí samostatného oddělení/vedoucí odboru, v jehož oddělení informace vznikla, nebo se nejvíce využívá pro práci oddělení. Ve sporných případech o vlastnictví (a související odpovědnosti za určitý typ informace) rozhoduje fórum pro bezpečnost informací ČZU. • Vlastník odpovídá za stanovení stupně klasifikace informace a u diskrétních informací též za dobu platnosti této klasifikace, v okamžiku jejího vytvoření. Klasifikace je obvykle delegována na podřízené pracovníky, kteří dané informace reálně vytvářejí nebo přijímají od třetích stran. • Vlastník odpovídá za určení bezpečnostních požadavků na informace, v případě potřeby i za určení požadavků na nadstandardní bezpečnostní opatření (např. trezor), dále za autorizaci přístupu k informacím pro ty pracovníky, kteří je potřebují k výkonu svých pracovních povinností, a za odebrání přístupu těm, kteří nemají tuto oprávněnou potřebu s informacemi pracovat. • Vlastník dále odpovídá za reklasifikaci informací (po uplynutí doby platnosti klasifikace) v jeho působnosti.
Správce	• Správcem informací v nelistinné podobě je zpravidla OIKT ČZU a jeho podřízené složky. Pro konkrétní typ informace v nelistinné podobě může být vlastníkem informace určen i jiný správce. • Správcem informací v listinné podobě je zpravidla vlastník nebo vedoucí oddělení/vedoucí samostatného oddělení/vedoucí útvaru, kde listina vznikla nebo se nejvíce využívá pro práci oddělení/útvaru. V ostatních případech je správce informace určen jmenovitě fórem vlastníkem informace nebo pro bezpečnost informací ČZU. • Správce informace odpovídá za realizaci bezpečnostních požadavků definovaných vlastníkem a za správu bezpečnostních opatření (např. za přidělení přístupových práv uživateli k informacím daného typu, pokud byl autorizován vlastníkem.) Role správce a vlastníka může být sloučena.
Uživatel	• Pracovník, student a zaměstnanec třetí strany, který je autorizován vlastníkem k užívání informace. Uživatel, který je tvůrcem nebo příjemcem informace od třetí strany, nese přenesenou odpovědnost za stanovení stupně klasifikace. Uživatel odpovídá za užívání informace způsobem, který je v souladu s pravidly pro klasifikaci informací a zacházení s nimi.

7. 2. Klasifikační schéma

7. 2. 1. Stupně klasifikace informací ČZU

Veškeré informace ČZU a informace, které byly ČZU svěřeny třetími stranami, spadají do jednoho ze čtyř níže uvedených klasifikačních stupňů. Veškerým informacím ČZU musí být přiřazen stupeň klasifikace na základě následující tabulky.

Klasifikační stupeň	
DISKRÉTNÍ	Definice diskrétních informací: Informace, jejichž vyzaření by mohlo závažným způsobem poškodit fungování ČZU nebo její dobré jméno, způsobit závažné majetkové ztráty, zapříčinit přerušení nebo zmaření významných procesů realizovaných ČZU. Na tyto informace se nevztahují ustanovení zákona č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů.
	Přístup k diskrétním informacím: Přístup k takovým informacím musí být omezen pouze na úzkou, jmenovitě definovanou skupinu osob, která tyto informace potřebuje k výkonu svých pracovních povinností.
	Seznamování se s diskrétními informacemi: Pro seznámení se s těmito informacemi je nutný souhlas vlastníka, a pokud se jedná o smluvní třetí strany, pak také podepsaná „Smlouva o ochraně informací“.
	Evidence diskrétních informací: Důvěrné informace se vždy klasifikují spolu s uvedením doby platnosti klasifikace a musejí být evidovány v „Katalogu klasifikovaných informací ČZU“.
	Označování diskrétních informací: Tyto informace je povinností vlastníka označit viditelně klasifikačním stupněm, tj. návěstím „Diskrétní“.
	Reklasifikace/deklasifikace: Reklasifikaci/deklasifikaci provádí vlastník.
	Výjimky: Výjimky při označování diskrétních informací stanoví vlastník.
OSOBNÍ	Definice osobních informací: Informace týkající se určeného nebo určitého subjektu dle zákona č. 101/2000 Sb. (zaměstnanci, studenti a jiní). Subjekt je těmito informacemi určený nebo určitelný. Na tyto informace se vztahují ustanovení jmenovaného zákona.
	Přístup k osobním informacím: Tyto informace nesplňují kritéria diskrétních informací ani nejsou určeny ke zveřejnění. Přístup k takovým informacím musí být omezen pouze pro skupinu osob, která je potřebuje k výkonu svých pracovních povinností a to pouze za splnění podmínek daných zákonem č. 101/2000 Sb.

Klasifikační stupeň	
	Seznamování se osobními informacemi: Pro seznámení se s těmito informacemi je nutný souhlas vlastníka, a pokud se jedná o smluvní třetí strany, pak také podepsaná „Smlouva o ochraně informací“ podle §15 zákona č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů. Seznámení s informacemi je možné pouze pokud to zákon povoluje. Evidence osobních informací: Osobní informace se vždy klasifikují spolu s uvedením doby platnosti klasifikace a musejí být evidovány v „Katalogu klasifikovaných informací“. Označování osobních informací: Tyto informace je povinností vlastníka označit viditelně klasifikačním stupněm, tj. návěstím „Osobní“. Reklasifikace/deklasifikace: Reklasifikaci/deklasifikaci provádí její vlastník. Výjimky: Výjimky při označování osobních informací stanoví její vlastník v souladu se zákonem č. 101/2000 Sb..
INTERNÍ	Definice interních informací: Do tohoto stupně spadají veškeré informace, které jsou určeny pro interní použití všemi zaměstnanci pro výkon jejich pracovních a jiných povinností ve vztahu k ČZU. Veškeré informace, které nesplňují kritéria pro klasifikaci DISKRÉTNÍ nebo OSOBNÍ a současně nejsou určeny ke zveřejnění, jsou považovány za informace INTERNÍ. Přístup k interním informacím: Přístup k takovým informacím je omezen pouze na zaměstnance, kteří je potřebují k výkonu svých pracovních povinností. S interními informacemi se studenti ČZU seznamují jen v rozsahu definovaném vlastníkem a zákonnými předpisy. Z pohledu bezpečnosti je vhodné, aby ne všichni pracovníci měli přístup ke všem interním informacím, ale pouze k těm, které potřebují k výkonu svých pracovních povinností. Seznamování se s interními informacemi: Pro seznámení se s těmito informacemi je nutný souhlas vlastníka. Vlastník definuje útvary, nebo pokud je potřeba, definuje i konkrétní zaměstnance nebo studenty, kteří se mohou seznamovat s interními informacemi, jež jsou v držení vlastníka. Vlastník stanoví, která část dokumentu (nebo zda celý dokument) bude poskytnuta studentům ČZU, veřejnosti nebo třetí straně. Pokud se jedná o smluvní třetí strany, pak je potřeba, aby byla uzavřena „Smlouva o ochraně informací“. Předávání interních informací dle zákonných předpisů a na základě osobních smluv je možné bez uzavření „Smlouvy o ochraně informací“. Evidence interních informací: Interní informace se vždy klasifikují a v „Katalogu klasifikovaných informací ČZU“ se podrobně neuvádějí. Označování interních informací: Tyto informace je nutné označovat viditelně klasifikačním stupněm, tj. návěstím „Interní“. Reklasifikace/deklasifikace: Reklasifikaci/deklasifikaci provádí vlastník informace. Výjimky: Výjimky z pravidel pro nakládání s interními informacemi a výjimky při označování interních informací stanoví jejich vlastník.

Klasifikační stupeň	
VEŘEJNÉ	Definice veřejných informací: Informace, které jsou přístupné všem pracovníkům ČZU, studentům ČZU i veřejnosti a jsou schváleny vlastníkem ke zveřejnění. Informace nevyžadují zvláštní úroveň ochrany z pohledu důvěrnosti. (Je však nutné dbát na jejich ochranu z pohledu integrity, aby nedošlo ke zveřejnění informací, které neodpovídají skutečnosti.)
	Přístup k veřejným informacím: Přístup k veřejným informacím nesmí být omezován.
	Evidence veřejných informací: Veřejné informace, které jsou ve vlastnictví ČZU se vždy klasifikují, ale v „Katalogu klasifikovaných informací ČZU“ se podrobně nebo vůbec neuvádějí.
	Označování veřejných informací: Veřejné informace nepodléhají označování.
	Reklasifikace/deklasifikace: Reklasifikaci/deklasifikaci provádí vlastník.
	Výjimky: Výjimky z pravidel pro nakládání s veřejnými informacemi stanoví vlastník.

7. 2. 2. Postup určování klasifikačního stupně a kategorie informací

Výchozí stupeň klasifikace

Klasifikační stupeň INTERNÍ je považován za výchozí stupeň klasifikace. Nevyžaduje-li informace zvláštní ochrany, ani není informace schválena ke zveřejnění, je klasifikována jako INTERNÍ.

Pokud se zaměstnanec ČZU setká s neoznačenou informací, nakládá s ní jako s interní informací do té doby, než ověří skutečnou klasifikaci informace.

Postup klasifikace DŮVĚRNÝCH, OSOBNÍCH a INTERNÍCH informací

Při vzniku informace, resp. při přijetí informace od třetích stran, vlastník nebo zaměstnanec, který informaci přijal rozhoduje, zda informace vyžaduje zvláštní ochrany, na základě posouzení kritičnosti informace dle tabulky v kapitole 7. 2. 1. („Stupně klasifikace informací ČZU“) a na základě „Katalogu klasifikovaných informací ČZU“.

Není-li informace uvedena v „Katalogu klasifikovaných informací“ a nesplňuje-li informace kritéria klasifikačního stupně DISKRÉTNÍ a OSOBNÍ, bude pak klasifikována jako INTERNÍ.

Pokud informace není uvedena v „Katalogu klasifikovaných informací ČZU“, ale vzniká potřeba zvláštní ochrany, a tedy i klasifikace jako DISKRÉTNÍ nebo OSOBNÍ, vlastník (zaměstnanec, který informaci přijal) ve spolupráci s bezpečnostním manažerem ČZU provede klasifikaci a zavede informaci do „Katalogu klasifikovaných informací ČZU“.

Klasifikace VEŘEJNÝCH informací

Jako VEŘEJNÉ mohou být klasifikovány ty informace, které již byly jako veřejné přijaty do ČZU, nebo byly vlastníkem schváleny ke zveřejnění. Rozhodnutím vlastníka můžou být INTERNÍ informace deklasifikovány na VEŘEJNÉ.

7. 2. 3. Reklasifikace informací

Hodnota informací se může v průběhu času měnit. V průběhu času informace obvykle ztrácejí na hodnotě. Aby se zabránilo zbytečnému vynakládání prostředků na zabezpečení informací, které to již nevyžadují, je vlastník informace odpovědný za:

1. Uvedení časové platnosti klasifikace ve všech případech, pokud se jedná o DISKRÉTNÍ informace (stejně jako klasifikace samotná, je tato odpovědnost obvykle delegována.). Samotné vypršení časové platnosti klasifikace není automaticky považováno za důvod k reklasifikaci informace na jiný stupeň, pokud u informace není toto vlastníkem výslovně uvedeno. Při vypršení je třeba provést zhodnocení možnosti reklasifikace.
2. Za přezkoumání klasifikace – reklasifikaci informací, které jsou v působnosti vlastníka.
 - a. Informace, které již nesplňují kritéria pro DISKRÉTNÍ a OSOBNÍ informace, musí být deklasifikovány na INTERNÍ.
 - b. Přezkoumání se provádí minimálně jednou ročně.

Pokud u informací, které jsou informacemi INTERNÍMI, dojde ke změně jejich informačního obsahu, a v důsledku toho k potřebě zvýšit jejich klasifikaci na DISKRÉTNÍ nebo OSOBNÍ, musí být tato změna provedena bez zbytečného odkladu, podle postupu klasifikace diskretních a INTERNÍCH informací (viz kap. 7. 2. 2. Postup určování klasifikačního stupně a kategorie informací).

7. 3. Zacházení s informacemi a jejich označování

7. 3. 1. Označování informací

Označování informací musí být zajištěno bez ohledu na to, na jakém nosiči a v jaké podobě se informace nacházejí.

Informace se označují zřetelným návěštím uvedeném na dokumentu a v sestavách na každém listu. Informace v elektronické podobě se označují:

- výstupy z IS ČZU shodně jako listinná forma dokumentů,
- informace na výměnném elektronickém médiu – označují se jak jména souborů, tak i média samotná.

Informace, které jsou schváleny ke zveřejnění, je doporučováno označovat jako „VEŘEJNÉ“. V okamžiku vlastního zveřejnění a ve formě, která skutečně jde mimo ČZU, není nutné, aby bylo označení uvedeno.

7. 3. 2. Zacházení (manipulace) s informacemi ČZU

Informace v listinné podobě	DISKRÉTNÍ	OSOBNÍ	INTERNÍ	VEŘEJNÉ
Označování	Na všech stranách nahore textem „DISKRÉTNÍ“.	Na všech stranách nahore textem „OSOBNÍ“.	S informacemi, které nejsou označeny, je zacházeno jako s interními informacemi. Označování je doporučováno na všech stranách nahore textem „INTERNÍ“.	Dokumenty, které jsou schváleny pro zveřejnění, je doporučováno označovat na titulní straně nebo obálce návěštím „VEŘEJNÉ“. Při jejich vlastním zveřejnění toto návěští (označení) může být odstraněno.
Kopírování	Pouze se souhlasem vlastníka a po aktualizaci rozdělovníku. Může provádět pouze osoba, která je autorizována pro seznamování se s danou informací. Kopie ani originály nesmí být ponechávány na kopírovacím zařízení bez dozoru. Rozdělovník s informacemi o přesném počtu kopií zhotovených z originálu je přiložen jako samostatný list k originálu.	Pouze pro pracovní účely. Může být kopírována pouze autorizovanou osobou (Vlastník/Garant informace a jím pověřené osoby (např. pracovník oddělení/odboru)) a to pouze v souladu se zákonem č. 101/2000 Sb.	Pouze pro pracovní účely. Pokud je kopírována informace klasifikována, může být kopírována pouze autorizovanou osobou.	Bez omezení.

Informace v listinné podobě	DISKRÉTNÍ	OSOBNÍ	INTERNÍ	VEŘEJNÉ
Posílání poštou nebo kurýrem	Nelze v nechráněné podobě. (Lze pouze v podobě datového média s bezpečně šifrovaným obsahem. V žádném případě nesmí obsahovat klíče pro dešifrování!)	V zalepené obálce. Obálka bez označení stupně klasifikace. Označení je uvnitř na dokumentu.	V zalepené obálce. Obálka bez označení stupně klasifikace. Označení je uvnitř na dokumentu.	V zalepené obálce.
Skartace	Skartace fyzickým zničením provedená vlastníkem informace nebo jinou oprávněnou osobou za dozoru vlastníka.	Skartace fyzickým zničením.	Skartace fyzickým zničením.	Žádné zvláštní požadavky.
Ukládání dokumentů	Ukládány v uzamykatelném úschovném objektu dle standardů fyzické bezpečnosti. Požadavky bezpečnosti příslušející tomuto stupni klasifikace: „minimálně v uzamčených plechových skříních opatřených cylindrickým vložkovým nebo cylindrickým visacím zámekem.“ Vlastník rozhoduje, zda je potřebné zvýšit bezpečnostní požadavky na použití trezoru.	Ukládány v uzamykatelných nábytkových skříních. Požadavky bezpečnosti příslušející tomuto stupni klasifikace: „minimálně v uzamčených nábytkových skříních a kontejnerech opatřených cylindrickým vložkovým nebo cylindrickým visacím zámekem“. Vyžaduje se uzamykání kanceláří a dodržování pravidla „čistého stolu“.	Ukládány v uzamykatelných nábytkových skříních a kontejnerech opatřených cylindrickým vložkovým nebo cylindrickým visacím zámekem. V případě odůvodněné provozní potřeby, a pokud není ovlivněna úroveň bezpečnosti informace, lze za dostačující považovat uzamykání kanceláří a dodržování pravidla „čistého stolu“.	Žádné zvláštní požadavky.

Informace v listinné podobě	DISKRÉTNÍ	OSOBNÍ	INTERNÍ	VEŘEJNÉ
Přístup k dokumentům	Vlastník definuje přístupová práva ve formě rozdělovníku, což je jmenovitý seznam konkrétních osob, pro které je dokument určen. Dokumenty jsou přebírány oproti podpisu. Rozdělovník s informacemi o přesném počtu kopií zhotovených z originálu je uveden jako samostatný list při originálu.	Osobní složky a dokumenty nejsou přístupné všem zaměstnancům ČZU. Takto kategorizované informace jsou určeny buďto konkrétním osobám nebo konkrétnímu oddělení. V tomto případě rozhoduje vlastník informace.	Takto kategorizované informace jsou určeny buďto konkrétním osobám nebo konkrétnímu oddělení. V tomto případě rozhoduje vlastník informace.	Přístupné všem osobám jak v rámci ČZU, tak i veřejnosti.
Reklasifikace	Vlastník určuje přesné datum.	V rámci práce s dokumenty. Osobní informace a dokumenty nesmí být deklasifikovány na VEŘEJNÉ. V případě odůvodněné potřeby pak mohou být v klasifikaci povýšeny na DISKRÉTNÍ. Požadavek obvykle vzniká v případě zásadní změny informačního obsahu a změna musí být schválena vlastníkem.	V rámci práce s dokumenty. Interní dokumenty musí být před jejich zveřejněním schváleny. V případě odůvodněné potřeby pak mohou být v klasifikaci povýšeny na DISKRÉTNÍ. Požadavek obvykle vzniká v případě zásadní změny informačního obsahu a změna musí být schválena vlastníkem.	Žádné zvláštní požadavky.

Informace v IS	DISKRÉTNÍ	OSOBNÍ	INTERNÍ	VEŘEJNÉ
Označování informací – názvů souborů	Uvedení klasifikačního stupně v názvu souboru – na jeho začátku, vlastní název následuje za pomlčkou. (Např. Diskrétní – Mzdové výměry a odměny vedoucích pracovníků.doc)	Uvedení klasifikačního stupně v názvu souboru – na jeho začátku, vlastní název následuje za pomlčkou. (Např. Osobní – Hodnocení uchazeče o zaměstnání.doc)	Označení dle úvahy vlastníka, resp. delegovaně dle úvahy tvůrce/příjemce.	Dle úvahy vlastníka.
Informace uložené v IS s řízeným přístupem	Šifrování není vyžadováno.	Šifrování není vyžadováno.	Šifrování není vyžadováno.	Šifrování není vyžadováno.
Informace uložené v IS bez řízeného přístupu	Nutné šifrování schváleným šifrovacím programovým vybavením s využitím silného hesla nebo tokenu.	Nutné šifrování schváleným šifrovacím programovým vybavením s využitím silného hesla nebo tokenu.	Šifrování nutné pouze pro kategorizované interní informace, a to na úrovni, např. silným heslem zabezpečeného archivu.	Šifrování není vyžadováno.
Informace uložené na přenosném médiu. Za přenosná média se považují také notebooky, PDA a jakákoliv další zařízení, na která lze ukládat informace.	Nutné šifrování schváleným šifrovacím programovým vybavením s využitím silného hesla nebo tokenu.	Nutné šifrování schváleným šifrovacím programovým vybavením s využitím silného hesla nebo tokenu.	Šifrování doporučeno, a to na úrovni, např. silným heslem zabezpečeného archivu.	Šifrování není vyžadováno.

Informace v IS	DISKRÉTNÍ	OSOBNÍ	INTERNÍ	VEŘEJNÉ
Přístup k informaci, včetně jejího kopírování a mazání	Vlastník určuje přístupová práva pro jednotlivé uživatele buď sám, nebo dává pokyn správci informací.	Vlastník určuje přístupová práva pro jednotlivé uživatele buď sám, nebo dává pokyn správci informací.	Vlastník určuje přístupová práva nejčastěji na úroveň určité uživatelské skupiny nebo pro jednotlivé uživatele, a to buď sám, nebo dává pokyn správci informací.	Čtení se povoluje pro všechny, ale je nutné zajistit ochranu integrity informací a bránit jejich neoprávněnému vymazání a úpravě.
Tisk	Tisk je možný pouze se souhlasem vlastníka. Tisk musí být součástí řízeného procesu a každý výtisk je nutné evidovat. Tisk musí být směřován na tiskárnu, která je pod dohledem oprávněné osoby tak, aby se zabránilo neoprávněnému seznámení nebo odcizení tištěného dokumentu.	Vlastník definuje možnosti tisku.	Vlastník definuje možnosti tisku.	Žádné zvláštní požadavky.
Požadavky na mazání informace (za předpokladu schváleného mazání)	Mazání musí být provedeno bezpečným způsobem. Za bezpečný způsob se považuje mazání několikanásobným přepisem, běžné mazání šifrované informace a další způsoby, které povoluje bezpečnostní manažer ČZU.	Mazání běžným způsobem.	Mazání běžným způsobem.	Mazání běžným způsobem.
Likvidace elektronických médií	Fyzické zničení, které je provedeno komisionálně a o skartaci je učiněn záznam.	Fyzické zničení.	Fyzické zničení.	Žádné zvláštní požadavky.
Inspekce přístupu k informacím	Logují se veškeré pokusy o přístup, úspěšné i neúspěšné.	Logují se neúspěšné, resp. násilné pokusy.	Logují se neúspěšné, resp. násilné pokusy.	Žádné zvláštní požadavky.

Informace v IS	DISKRÉTNÍ	OSOBNÍ	INTERNÍ	VEŘEJNÉ
Požadavky na uchovávání inspekčních záznamů	Inspekční záznamy se zálohují a ukládají po dobu minimálně 1 roku.	Inspekční záznamy se zálohují a ukládají po dobu minimálně 1 roku.	Inspekční záznamy se zálohují a ukládají po dobu minimálně 1 roku.	Žádné zvláštní požadavky.

Informace v elektronické podobě	DISKRÉTNÍ	OSOBNÍ	INTERNÍ	VEŘEJNÉ
Faxem	Zakázáno	Pouze za dohledu nad odesíláním i přijetím faxu.	Žádné zvláštní požadavky.	Žádné zvláštní požadavky.
WAN	Nutné šifrování, vyžadováno potvrzení o přijetí.	Užití šifrování je na uvážení vlastníka.	Užití šifrování je na uvážení vlastníka	Žádné zvláštní požadavky.
LAN	Nutné šifrování, vyžadováno potvrzení o přijetí.	Užití šifrování je na uvážení vlastníka.	Užití šifrování je na uvážení vlastníka.	Žádné zvláštní požadavky.
Kurýrní službou	Lze pouze v podobě datového média se šifrovaným obsahem. V žádném případě nesmí obsahovat klíče pro dešifrování!	Média musí být uložena v zalepené obálce, na které není uveden stupeň klasifikace. Ten je uveden na médiu.	Žádné zvláštní požadavky.	Žádné zvláštní požadavky.
E-mail	Nutné šifrování za použití dostatečně silného šifrovacího algoritmu. Konkrétní typ a způsob určuje bezpečnostní manažer ve spolupráci s OIKT.	V rámci interní pošty bez omezení. E-mailem předávané informace vně ČZU musí být vhodným způsobem šifrovány běžnými prostředky.	V rámci interní pošty bez omezení. E-mailem předávané informace vně ČZU musí být vhodným způsobem šifrovány běžnými prostředky.	Žádné zvláštní požadavky.
Bezdrátovým / mobilním telefonem	Zakázáno.	Žádné zvláštní požadavky, avšak je nutné brát ohledy na okolí, ve kterém člověk hovoří.	Žádné zvláštní požadavky, avšak je nutné brát ohledy na okolí, ve kterém člověk hovoří.	Žádné zvláštní požadavky.

8. Závěrečná ustanovení

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

Přílohy

Příloha č. 1: Katalog klasifikovaných informací ČZU (KKI ČZU).

PRAVIDLA PRO KLASIFIKACI INFORMACÍ

Příloha č. 1 - Katalog klasifikovaných informací ČZU

Platný ke dni 1. 3. 2008

Verze 2.0

Název dat/informací/dokumentů	Klasifikační stupeň	Vlastník/Garant
D01 Vyhrazená data		
Smlouvy	Interní	Garant je jmenován.
Plány budov	Interní	Vedoucí provozně technického odboru ČZU
Nabídky na výběrové řízení	Diskrétní	Garant je jmenován
Osobní složky zaměstnanců (tištěné)	Osobní	Vedoucí personálního odboru ČZU
Osobní složky studentů (tištěné)	Osobní	Vedoucí příslušného studijního odd.
Knihy zkoušek	Diskrétní	Vedoucí odd./katedra kde je kniha uložena.
Dohody o pracovní činnosti	Osobní	Vedoucí personálního odboru ČZU
Testy pro přijímací řízení (tištěné)	Diskrétní	Garant je jmenován
Archiv (centrální archiv)	Interní	Vedoucí archívu
Výsledky interních auditů	Diskrétní	Vedoucí interního auditu ČZU
D02 Zaměstnanci		
Personální informace o zaměstnancích	Osobní	Vedoucí personálního odboru ČZU
Měsíční údaje (např. stravné)	Interní	Vedoucí personálního odboru ČZU
D03 IT a security data		
Technologické informace	Interní	Vedoucí OIKT
Poskytování HW a SW vybavení	Interní	Vedoucí OIKT
Záznamy z dohledového systému sítě	Interní	Vedoucí OIKT
Help-desk podpora systémů a aplikací	Interní	Vedoucí OIKT
Záznamy o incidentech	Diskrétní	Bezpečnostní manažer ČZU
Záznamy z kamer	Osobní	Bezpečnostní manažer ČZU
Archív a zálohy elek.pošty	Diskrétní	Vedoucí OIKT
Archiv a zálohy dat	Diskrétní	Vedoucí OIKT

Archív a zálohy sys. dat	Interní	Vedoucí OIKT
Zdrojové programy	Interní	Vedoucí OIKT
Výsledky analýzy rizik IS	Diskrétní	Bezpečnostní manažer ČZU
D04 Studenti		
Personální informace o studentech	Osobní	Vedoucí příslušného studijního odd.
Jiné informace o studentech	Interní	Vedoucí příslušného studijního odd.
Databáze hodnocení studentů	Osobní	Vedoucí příslušného studijního odd.
Databáze uchazečů o studium	Osobní	Vedoucí příslušného studijního odd.
Databáze hodnocení uchazečů	Osobní	Vedoucí příslušného studijního odd.
Data testů pro přijímací řízení (elektronická data)	Diskrétní	Garant je jmenován
D05 Účetní, ekonomická data		
Finanční plán-rozpočet	Interní	Vedoucí ekonomického odboru ČZU
Majetkové účetnictví	Interní	Vedoucí ekonomického odboru ČZU
Finanční účetnictví	Interní	Vedoucí ekonomického odboru ČZU
Databáze mezd	Interní	Vedoucí ekonomického odboru ČZU
Skladové hospodářství	Interní	Vedoucí ekonomického odboru ČZU
Hotovostní styk	Interní	Vedoucí ekonomického odboru ČZU
Informace o hospodaření	Interní	Vedoucí ekonomického odboru ČZU
Platební styk	Interní	Vedoucí ekonomického odboru ČZU
Účetní informace	Interní	Vedoucí ekonomického odboru ČZU
D06 Podpůrná data		
Evidence pošty	Interní	Vedoucí provozně technického odboru ČZU
Evidence licencí	Interní	Vedoucí OIKT
Interní dokumenty odborů/odd.	Interní	Grantem je vedoucí příslušného odborů/odd.
Data HelpDesku	Interní	Vedoucí OIKT