Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-003**
Název dokumentu:	**Provozní postupy**
Typ dokumentu:	Interní dokument - typ B – směrnice
Určeno pro:	všechny zaměstnance, studenty a účastníky CŽV JU, zejména pro správce IS a serverů JU
Prvek normy ISO:	27001
Datum vydání:	30.1.2012
Datum účinnosti:	15.2.2012
Platnost do:	odvolání
Počet stran + příloh:	11 + 5
Verze:	2.3 - aktualizace 07/2019 T.Linhart MIB JU
Účel:	Stanovení závazných postupů pro informační systémy a technologie provozované na JU
Uložení:	Portál ISMS - https://isms.jcu.cz/
Ruší dokumenty:	verze 2.2 tohoto dokumentu
Zpracovatel:	Ing. Jana Kolářová - MIB JU, zdroj Doc. Milan Berka - Comguard, a.s.
Přezkoumal:	ITM součástí JU, manažeři a správci CIT
Schválil:	RNDr. Josef Milota - ředitel ISMS a CIT

OBSAH

A. ÚVODNÍ USTANOVENÍ

CÍL PROCESU A ÚČEL

Cílem směrnice je stanovit závazné postupy pro provoz informačních systémů (IS) a technologií, zejména pak uvedení IS či serveru do provozu, jejich další provozování, provádění změn, způsob a formu vedení provozní dokumentace, plánování kapacit provozovaných systémů a ukončení provozu IS či serveru.

POJMY, DEFINICE A ZKRATKY

1. POJMY A DEFINICE

- **Antivirová ochrana (AVO)** – soubor organizačních a softwarových opatření, jehož účelem je ochrana počítačů a počítačové sítě JU před průnikem a šířením parazitních kódů.
- **Bezpečnostní incident -** jedna nebo více nežádoucích a neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činnosti JU a ohrožení bezpečnosti informací.
- **Garant IS –** vedoucí pracovník, v jehož působnosti je provozování konkrétního informačního systému, případně subsystému.
- **Havarijní plán -** soubor činností, postupů a vazeb pro krizové situace provozu informačních systémů.
- **HelpDesk –** technická podpora uživatelů (studentů, zaměstnanců a účastníků CŽV) JU, prostřednictvím níž mohou uplatňovat své požadavky (problém, chyba, návrh změny apod.). Na JU jde o portál https://rt.jcu.cz/, kam lze po přihlášení zadat požadavek k vyřešení v určitém IS či operačním prostředí. Požadavek lze zaslat i e-mailem na adresu obecně vyjádřenou jako „…@rt.jcu.cz“, kde je třeba nahradit … názvem IS či služby (konkrétní adresy jsou uvedeny v příloze 1 této směrnice).
- **Identifikační karta (IK)** - plastová čipová bezkontaktní identifikační karta přidělovaná zaměstnancům,i studentům, účastníkům CŽV či absolventům pracovištěm IPS CIT JU v rámci systému JIS, která obsahuje jejich identifikační údaje nutné pro fyzický přístup do objektů JU a přístup do vybraných IS JU. Může také obsahovat certifikáty pro přihlášení z PC do sítě JU, certifikát pro elektronický podpis, případně další údaje.
- **Heslo** – na JU stanoven řetězec min. osmi znaků (kombinace alfanumerických, ev. speciálních s výjimkou mezery a diakritiky). Mělo by obsahovat znaky alespoň tří znakových sad ze čtyř (velké písmeno, malé písmeno, číslice nebo speciální znaky). Obecně platí, že čím je heslo delší, tím hůře je odhalitelné. Prvotně vygenerované heslo univerzitního účtu v IDM je povinen si uživatel po prvním přihlášení změnit na své vlastní a přitom v něm nesmí použít své jméno, příjmení, ani název účtu (Username).
- **Outsourcing** – zajišťování části provozu organizace jinou externí firmou na základě uzavřené smlouvy za účelem úspory nákladů. Vychází ze dvou základních slov - "out" = vnější a "source" = zdroj. Např. v oblasti ICT správa systémů, vývoj SW apod.
- **Schvalovatel** - osoba, která provádí schválení požadavku.
- **Služba** – nabídka elektronicky realizované činnosti IS, sítě či jiného systému IT, kterou JU nabízí svým studentům, zaměstnancům a účastníkům CŽV.
- **Správce IS** - určený zaměstnanec JU, jehož úkolem je odborná správa, obsluha a údržba systémů informačních a komunikačních technologií.
- **Správce počítačů** – zaměstnanec JU pověřený údržbou operačních systémů a dalšího software na osobních počítačích (PC nebo NB) JU. Každá součást má jednoho či více lokálních správců počítačů, tzv. LS PC, kteří jsou metodicky vedeni hlavním správcem PC – HS PC.
- **Uživatel** – je zaměstnanec, student nebo účastník CŽV JU.
- **Uživatel IS –** uživatel, který má právo v předem definovaném rozsahu používat informační a komunikační systém JU.
- **Vlastník aktiva –** viz Garant IS.

2. ZKRATKY

- **AD** (Active Directory) - je implementace adresářových služeb LDAP pro PC s OS Windows, nástroj pro správu uživatelů, skupin, počítačů a sítí.
- **AVO –** antivirová ochrana počítače pomocí antivirového software.
- **CIT –** Centrum informačních technologií – celoškolské pracoviště JU.
- **CŽV –** celoživotní vzdělávání
- **GDPR -** General Data Protection Regulation, je nařízení EU 2016/679, které vstoupilo v platnost 25.5.2018. Jedná se o právní rámec ochrany osobních údajů.
- **HS –** hlavní správce počítačů, AVO nebo sítě JU
- **HW** (HardWare) - technické prostředky ICT.

- **ICT** (Information and Communication Technologies) – Informační a komunikační technologie - zahrnují veškeré technologie používané pro komunikaci a práci s informacemi.
- **IPS** – Identifikační a přístupový systém – pracoviště CIT, které na JU provozuje a spravuje JIS a další IS.
- **IS** – Informační systém = systém pro sběr, udržování, zpracování a poskytování informací a dat pomocí počítačů.
- **ISMS** (Information Security Management System) – Systém řízení bezpečnosti informací.
- **IT** (Information technology) – Informační technologie - zjednodušeně řečeno počítače a vše co s nimi souvisí.
- **ITM** – IT manažer, který zajišťuje IT služby své součásti (fakulty, ústavu).
- **JIS** – Jednotný identifikační systém = informační subsytém JU, který spravuje a udržuje pracoviště IPS CIT.
- **JU** – Jihočeská univerzita v Českých Budějovicích.
- **LDAP** (Lightweight Directory Access Protocol) - protokol pro ukládání a přístup k datům na adresářovém serveru. Slouží k autentizaci uživatelů.
- **LS PC -** lokální správce počítačů na každé součásti JU.
- **MIB –** Manažer informační bezpečnosti JU.
- **OS** – operační systém počítače- Windows, Linux, UNIX, Mac, atd.
- **PC** (Personal Computer) – osobní počítač ve vlastnictví JU. Není-li v textu explicitně uveden konkrétní typ počítače, zahrnuje i přenosné počítače typu notebook (NB) či netbook.
- **RT** (Request Tracker) – systém podpory řešení provozních problémů, dále viz pojem **HelpDesk**.
- **SLA** (Servis Level Agreement) – dohoda o úrovni poskytovaných služeb.
- **SW** (SoftWare) - programové vybavení počítače.
- **VPN** (Virtual Private Network) **–** virtuální privátní síť. Vzdálený přístup přes koncentrátor VPN JU je popsán na http://vpn.jcu.cz/ .

ODPOVĚDNOSTI A PRAVOMOCI

Pravomoci a odpovědnosti jsou součástí dokumentu.

ZMĚNY OPROTI PŮVODNÍ VERZI

Toto je druhá verze, první modifikace 2.1dokumentu.
Změna ve verzi 2.0 - proti původní verzi 1.0 změna kapitoly 1.9.5., životní cyklus uživatele (06/2017)
Změna ve verzi 2.1 – v kapitole 1.9.5. doplněn název dokumentu, popisující životní cyklus uživatele (07/2017)
Změna ve verzi 2.2 – v části C doplněny související dokumenty (05/2018)
Změna ve verzi 2.3. – v kapitole 1.9.4.upraven popis generování prvotního hesla (07/2019)

B. POPIS

1. OBECNÉ PROVOZNÍ POSTUPY

Všechny HW a SW prostředky v majetku JU musí být spravovány správci ICT podle doporučení a dokumentace výrobce. Seznam správců informačních systémů (IS) JU je uveden v příloze 1 – *ISMS-003-P1*. Dokumentace výrobců HW i SW jsou běžně dostupné na jejich internetových stránkách.

Správce IS musí být vždy řádně vyškolen pro správu svěřeného IS a postupuje podle administrátorské dokumentace zpracované k jednotlivým systémům dodavatelem či interně.

1.1. POSTUP INSTALACE SYSTÉMŮ

Závazné postupy pro instalaci serverů s OS Windows, s OS Linux/Unix a instalaci síťových komponent jsou uvedeny v přílohách této směrnice - *ISMS-003-P2* až *P4*.

1.2. DOKUMENTACE

Administrátorská dokumentace k jednotlivým IS provozovaným na JU je přístupná pouze stanoveným pracovníkům a nachází se na portálu ISMS (https://isms.jcu.cz/) ve složce „Aktiva IT“ u příslušného IS. Prioritně se to týká celouniverzitních IS spravovaných pracovištěm CIT.

Pro koncové uživatele informačních systémů je k dispozici uživatelská dokumentace. Tato dokumentace je dostupná u správců IS a na IT portálu JU (http://itportal.jcu.cz).

1.3. HAVARIJNÍ PLÁNY OBNOVY

Ke všem významným IS – např. STAG, FIS, MIS, PaM a dalším - budou zpracovány havarijní plány a plány obnovy pro případ výskytu nenadálých chybových stavů, tyto plány zahrnují základní popis systému a postupy pro jeho obnovu v případě poruchy nebo jiné chyby, včetně kontaktů na správce IS a servisní organizace.

Plány budou aktualizovány průběžně při změnách a jejich správnost pak vyhodnocována - nejméně 1x ročně. Záznamy budou uloženy na pracovišti SIS CIT. Za aktualizaci plánů obnovy je odpovědný správce IS a za jejich vyhodnocení vlastník IS. Havarijní plány obnovy pro jednotlivé systémy by měly být fyzicky uloženy v papírové formě na bezpečném místě (trezor CIT) a elektronicky na sdíleném síťovém zařízení s řízeným přístupem, aby byly k dispozici v případě potřeby k obnově.

1.4. TESTOVÁNÍ HAVARIJNÍCH PLÁNŮ

Testování havarijních plánů obnovy se provádí v rámci řešení konkrétních výpadků/havárií systémů, které jsou nahlášeny správci IS nebo na základě bezpečnostního incidentu. Výsledky testů jsou uvedeny v provozním deníku IS nebo v popisu řešení bezpečnostního incidentu.

1.5. ULOŽENÍ HESEL K IS

Pro případ havárie centrálních IS musí mít správce IS také svého zástupce s privilegovaným účtem. V případě, že tento zástupce neexistuje, je heslo k účtu správce uloženo v uzavřené obálce, podepsané správcem IS v trezoru CIT, kam má přístup pouze ředitel CIT a manažer SIS CIT.

1.6. PROVÁDĚNÍ ZMĚN V IS

Změny v informačních systémech lze provádět následovně:

- **uživatelé** žádají o provedení změny v systémech prokazatelným způsobem (např. e-mailem) správce IS nebo přes HelpDesk CIT (role Žadatel) – dále viz bod 1.7. a příloha 5 této směrnice
- všechny změny v informačních systémech jsou buď schváleny, případně zamítnuty **vlastníkem** aktiva (role Schvalovatel)
- **správce IS** po dohodě s dodavatelem IS a po zvážení finanční náročnosti před aplikováním změny vyhodnotí její vliv na provoz IS, v případě potřeby (např. při zásadních změnách velkého rozsahu) je provedena analýza rizik
- **správce IS** je odpovědný za stanovení postupu provedení změny, případně přerušení změny a návrat k původnímu stavu
- ke změně IS, která se týká informační bezpečnosti, se vyjadřuje **manažer informační bezpečnosti JU** (MIB) prokazatelnou formou (např. e-mailem), jinak není taková změna implementována. Jedná se o změny, které se negativně dotýkají následujících oblastí:

- autentizace a autorizace uživatelů
- přenosového protokolu
- kryptografických metod
- kontrol vstupních dat.

K jiným typům změn – např. změna vzhledu nebo formátu aplikací apod. - se **MIB** nemusí vyjadřovat.

- Změny v systémech jsou zaznamenávány do provozního deníku, za což je odpovědný správce IS a ITM.

1.7. ŘEŠENÍ POŽADAVKŮ PŘES HELPDESK

HelpDesk – na JU systém RT (Request Tracker) - poskytuje uživatelům IS či služeb možnost řešit problémy, incidenty či jiné požadavky buď formou e-mailu nebo webového rozhraní (http://rt.jcu.cz). Schéma řešení požadavků či změn a základní informace o tomto systému jsou uvedeny v příloze 5 této směrnice s názvem „*ISMS-003-P5_HelpDesk-řešení požadavků*“. E-mailové adresy pro požadavky na jednotlivé IS či služby lze nalézt v příloze 1 - „*ISMS-003-P1_Klíčové IS*“.

1.8. ZÁLOHOVÁNÍ, ARCHIVACE A OBNOVA DAT

Vytváření pravidelných záloh provozních dat je na JU z důvodu bezpečnosti povinné. Základní pravidla a odpovědnosti budou popsány v samostatném směrnici ISMS **Zálohování, archivace a obnova dat**. Dokumentace k zálohování a obnově dat IS či serverů je uložena na portálu ISMS ve složce „Aktiva IT“ u příslušného IS či serveru buď jako samostatný dokument nebo jako součást komplexní dokumentace IS.

1.9. ŘÍZENÍ PŘÍSTUPU K SYSTÉMŮM

1.9.1. Automatická identifikace počítače

V prostředí Windows poskytuje základní zabezpečení počítačů systém Active Directory (doména ad.jcu.cz). PC v majetku JU musí být přidán do databáze AD správcem AD dané součásti, případně jeho zástupce*m*. Výjimky schvaluje správce AD dané součásti JU, který vede jejich evidenci. V době vydání této směrnice může existovat samostatná doména pro správu PC součásti JU. Postupně bude docházet k začleňování PC z těchto domén do centrální domény AD, která je spravována pracovištěm CIT.

1.9.2. Přihlašovací postupy

Všechny neúspěšné pokusy o přihlášení do Active Directory jsou zaznamenány (logovány) na řadiči domény a jsou dohledatelné.

1.9.3. Identifikace a autentizace uživatelů

Všichni uživatelé včetně administrátorů používají k identifikaci výhradně svůj jedinečný účet (login ID). Použití obecného účtu s vysokým oprávněním jako např. „administrator“ nebo „root“ je možné pouze v krizových situacích. I v tomto případě je doporučeno se vždy přihlásit jako konkrétní uživatel a následně se do administrátorského účtu přepnout.
Systémoví správci se mohou autentizovat v AD pomocí identifikační karty s certifikátem.

Společné (servisní) účty lze použít pro běh jednotlivých služeb IS a nikoli pro ověření přístupu na server.

1.9.4. Systém správy hesel

Přístupová hesla uživatelů jsou jako základní prostředek pro ověřování uživatelů použita na principu individuální odpovědnosti. Jednorázové heslo (jen pro první použití) je automaticky generováno při zavedení uživatele do systému IDM a je povinností uživatele si jej při prvním přihlášení změnit a dále jej měnit periodicky. V případě pochybností o utajení hesla má uživatel rovněž povinnost si jej neprodleně změnit. Uživatel je veden bezpečnostní politikou k zvýšení bezpečnosti a musí dodržovat stanovená pravidla - délku hesla, platnost, složení hesla, změnu hesla (historie) atd. Hesla nejsou při zadávání nikdy zobrazována na obrazovce. Zašifrování hesla na PC je řešeno přes OS počítače. Totéž platí pro šifrování hesel na serverech, případně při vzdáleném přístupu.

V případě zapomenutí hesla má uživatel tyto možnosti:

- Navštíví pracoviště HelpDesk - pokud na JU existuje – a tam uplatní svůj požadavek.

- Zadá svůj požadavek elektronicky prostřednictvím HelpDesku (https://rt.jcu.cz). Při přihlašování do IS STAG jsou studenti a účastníci CŽV informováni o řešení problémů s autentizací upozorněním na úvodní stránce portálu STAG. Své požadavky mohou realizovat v souladu s touto informací elektronicky e-mailem přímo na adresu HelpDesku, tj. idm@rt.jcu.cz, případně stag@rt.jcu.cz .

- Osobně nebo telefonem kontaktuje lokálního správce PC své součásti (seznam správců je uveden na portálu ISMS ve složce „Kontakty“) nebo - v závislosti na typu účtu - správce IDM, správce poštovního serveru, případně správce jiného IS. Při osobní návštěvě se uživatel identifikuje kartou zaměstnance, studenta, účastníka CŽV či absolventa, při telefonickém kontaktu musí uživatel před nastavením nového hesla uvést údaje, kterými je možné ověřit jeho identitu a jež na něm bude vyžadovat správce systému (např. jméno, příjmení, požadovanou část rodného čísla, uživatelské jméno, případně email z IDM).

- Řídí se interními předpisy své součásti JU, pokud existují, např. na web portálu fakulty.

V případě ztráty identifikační karty – používá-li se k autentizaci - je toto třeba okamžitě nahlásit pracovišti IPS CIT a správci AD, který dočasně zablokuje uživateli přístup.

1.9.5. Životní cyklus uživatele

Nový uživatel je zařazen do systému IDM JU z autoritativních zdrojů dat, kterými jsou personální aplikace, studentská aplikace a aplikace pro CŽV. Tím jsou uživateli přiřazeny odpovídající přístupové údaje – uživatelské jméno a heslo, které je po prvním přihlášení nutné neprodleně změnit a toto si zapamatovat.
Pokud dochází ke změně pracovního zařazení či studia, tato změna je opět zaznamenána do systému IDM z výše uvedených zdrojů dat. Při ukončení zaměstnackého poměru, studia či CŽV je tato skutečnost rovněž z výše uvedených zdrojů propagována do systému IDM a tím jsou takovému uživateli zrušena všechna přístupová práva. Při ukončení pracovního poměru zaměstnance personální oddělení do výstupního listu potvrdí, že zaměstnanec také vrátil všechna zapůjčená zařízení ICT. Bez tohoto potvrzení není možné vydat zaměstnanci výstupní list.
Životní cyklus uživatele je zdokumentován v příloze k tomuto dokumentu *ISMS-003-P6*

1.9.6. Použití systémových nástrojů

Systémové nástroje pro správu PC uživatelů používají pouze správci PC. Heslo pro přihlášení lokálního administrátora na jednotlivých stanicích uživatelů a serverech je vždy jedinečné a zná ho buď správce stanice nebo jeho zástupce.

1.9.7. Vzdálený přístup

Vzdálený přístup do sítě JU je možný přes VPN koncentrátor za použití individuálního účtu uživatele a je šifrovaný. Popis vytvoření účtu, nastavení počítače pro tento přístup, možnost ověření správnosti údajů i kontakt na správce VPN je uveden na http://vpn.jcu.cz/.

1.10. PROVOZNÍ DENÍKY

Provozní deník (PD) je dokument vytvořený na základě uvedení aktiva ICT do provozu, do něhož správce IS, serveru, síťového či jiného zařízení ICT průběžně zaznamenává důležité SW a HW změny a havarijní stavy či jiné podstatné události. Jeho existence je předepsaná v základní směrnici *ISMS-002_Celková bezpečnostní politika JU.*
Provozní deníky jsou pro informační aktiva vedeny v elektronické formě s řízením úrovně přístupu k jednotlivým záznamům dle definovaných rolí. Za řádné zaznamenávání událostí a změn do provozního deníku je odpovědný správce aktiva a za kontrolu této činnosti je odpovědný vlastník aktiva nebo ITM.

Provozní deníky IS či dalších technologických zařízení ICT jsou dostupné ve složce „*Aktiva IT*“ na portále ISMS (https://isms.jcu.cz/) ve složkách jednotlivých součástí JU a přiřazeny k příslušným aktivům ICT.

1.11. SYNCHRONIZACE ČASU

Synchronizace času IT systémů je realizovaná prostřednictvím protokolu NTP (Network Time Protocol). Správce systému je povinen zajistit synchronizaci času. Všechny auditní záznamy musejí obsahovat čas, který je synchronizován s časovými servery. Synchronizace se buď provádí automaticky minimálně 1x za hodinu nebo se realizuje spuštěním NTP služby, která zajišťuje nepřetržitou synchronizaci. Diference času s časovým serverem nesmí překročit 1 sekundu, pokud se tak stane, je třeba zvýšit četnost synchronizace.

1.12. OCHRANA PŘED ŠKODLIVÝMI PROGRAMY

Správci systémů jsou povinni chránit systémy před škodlivými programy a stanovit postupy pro řešení

virového útoku. Tato opatření jsou součástí provozní dokumentace k systémům. Interní systémy jsou chráněny před škodlivými programy z externích sítí pomocí bezpečnostních prvků (firewallů) a instalací lokální antivirové ochrany.
Antivirová ochrana uživatelských PC je v kompetenci lokálních správců AVO a je popsána ve směrnici *ISMS-006_Antivirová ochrana počítačů JU*.

1.13. MOBILNÍ KÓDY

Pojem mobilní kód je v oblasti bezpečnosti ICT používán pro přenositelné programové kódy, které mohou ohrozit počítač. Šířit se mohou formou e-mailové přílohy, dokumentem či stahovanými soubory z Internetu, např. pomocí Active-X nebo JavaScripty v internetových prohlížečích. Ve vnitřní síti JU je omezeno používání nevěrohodných ActiveX a JavaScript komponent blokací v prohlížečích.

1.14. PLÁNOVÁNÍ KAPACIT

Pro zabezpečení plánování kapacit jednotlivých informačních a komunikačních prostředků jsou všechny používané systémy monitorovány. Jedná se zejména o sledování dostupnosti serverů a služeb. V případě problémů s dostupností služby se provádí měření zátěže jednotlivých subsystémů (CPU, RAM, obsazení disků, atd.)
Sledování kapacity internetového připojení JU provádí firma Cesnet - poskytovatel připojení JU do Internetu.

1.15. NAKLÁDÁNÍ S NOSIČI INFORMACÍ

Na JU jsou používána různá přenosná média, např. CD, DVD, datové pásky, přenosná USB zařízení (externí disky a flash disky).

Za likvidaci medií je odpovědný příslušný vlastník nosiče dat. Likvidace probíhá dle druhu média (např. fyzickou likvidací nebo přepsáním dat) a o každé fyzické likvidaci je proveden skartační protokol – viz Opatření prorektora R 189/2012 - Spisový řád JU + přílohy. O likvidaci celého média přepsáním dat provede správce aktiva záznam do Provozního deníku toho aktiva, které tento nosič používá (např. u serveru, jehož disk byl přepsán či zformátován).

Citlivá data na pevných discích či jiných datových úložištích v zařízeních musí být před jejich likvidací vždy zničena (např. zformátováním pevných disků PC nízkoúrovňovým formátem, přepisem dat, výmazem prázdných oblastí, fyzickou likvidací média apod.).

1.16. UMÍSTĚNÍ ZAŘÍZENÍ A BEZPEČNOST KABELÁŽE

Při umisťování zařízení zvažují vlastníci aktiv stavebně technické parametry, které by mohly ovlivnit aktivum. Konzultují umístění s ředitelem CIT, IT manažerem dané součásti nebo manažerem informační bezpečnosti, a to z hlediska předpokládaných hrozeb.

Bezpečnost kabeláže je zajištěna fyzickým umístěním kabeláže mimo veřejné prostory, přičemž je použit vždy materiál certifikovaný pro daný typ použití a na instalace je požadována záruka jakosti od dodavatele.

Kabely používané pro vedení optických okruhů sítě jsou buď vlastní nebo pronajímané od jiných telekomunikačních operátorů nebo vlastníků. Kabely jsou vedeny:

- v zemi v plastových chráničkách uložených dle ČSN 73 6005
- v kombinovaných zemních lanech vedení VVN (Velmi vysoké napětí)
- v budovách jsou optické kabely vedeny v kanálech, žlabech, stoupačkách, podhledech nebo ve zdvojené podlaze.

1.17. UKONČENÍ OPTICKÝCH KABELŮ

Je realizováno v optických rozvaděčích, které jsou umístěny:

- v uzavřených uzamykatelných místnostech
- v uzavřených uzamykatelných skříních v místnostech, pokud je JU sdílí s jinými subjekty (společné prostory).

2. VÝVOJ INFORMAČNÍCH SYSTÉMŮ

JU nevyvíjí IS, nýbrž jen drobné aplikace pro vlastní potřebu a nemá pracoviště vývoje SW. Stěžejní IS provozované na JU jsou od jiných dodavatelů, kteří splňují požadavky na bezpečnost jejich vývoje dle standardů ISO norem.

Standardní SW je nakupován u renomovaných výrobců. Možné způsobené škody SW vyvíjeného na míru jsou ošetřovány smluvně – dále viz kapitola 3. níže. Proto se tato kapitola podrobně nezabývá dalšími bezpečnostními aspekty vývoje SW.

S klíčovými IS provozovanými na JU pracují jen zkušení a důvěryhodní zaměstnanci CIT.

3. SPRÁVA EXTERNÍCH ZDROJŮ

3.1. SMLOUVY S DODAVATELI

Pokud je vývoj aplikace svěřen dodavatelské firmě, je to vždy na základě smluvního vztahu. Součástí smluvního dokumentu je vždy i dohoda o mlčenlivosti a v případě potřeby i soupis osob, které se ze strany dodavatele projektu účastní a mají oprávnění přistupovat k systémům JU. Toto oprávnění je udělováno pouze na nezbytně nutnou dobu.

Vývoj je potom ze strany JU řízen způsobem, kdy je zajištěna nutná součinnost mezi JU a dodavatelem.

Dodavatel vyvíjí SW mimo prostředí JU a dodává až hotové produkty. Tyto jsou umístěny v testovacím prostředí a testovány ze strany uživatelů JU. Testování je ukončeno podpisem akceptačních protokolů. Aplikace je nainstalována v produkčním prostředí a uvedena do provozu.

3.2. OUTSOURCING

Pokud je provoz aplikace/IS delegován na externího partnera, je to vždy na základě smluvního vztahu. Provoz aplikace systému formou outsourcingu musí schválit příslušný vlastník informačního aktiva.

Smlouva zpravidla obsahuje:

- vymezení pojmů
- rozsah poskytovaných služeb, (záruční a pozáruční servis, změnové řízení, …)
- způsob ohlášení a řešení závady
- SLA - úroveň poskytovaných služeb
- kvalitu (dodržování příslušných norem třídy ISO)
- kvalifikovanost podpory
- požadované výstupy
- reporting
- způsob kontroly prováděných činností (např. pravidelné kontrolní dny, …)
- odpovědnosti a závazky dodavatele i odběratele (povinnost dodržovat bezpečnostní pravidla odběratele)
- sankce za nedodržení SLA
- řešení případných sporů
- seznam odpovědných osob dodavatele a odběratele (obchodní, technické, …)
- doložku o mlčenlivosti
- požadovanou úroveň přístupových oprávnění (nastavuje a kontroluje pracoviště CIT)
- cenu a platební podmínky
- platnost smlouvy.

Schvalování smlouvy probíhá v souladu s příslušným procesem JU.

Řízení dodavatele probíhá v souladu s odpovídajícími ustanoveními smlouvy. Činnost dodavatele je pravidelně vyhodnocována a kontrolována na základě hlášení nebo domluvených výstupů, příp. kontrolních dnů. Dodavatel je seznámen s bezpečnostními pravidly a musí je dodržovat. V případě problémů je možné použít definované eskalační schéma, příp. uplatnit sankce. Fakturace probíhá pouze na základě odsouhlasených akceptačních protokolů / výkazů práce, které schvaluje garant příslušného projektu, vlastník informačního aktiva, příp. osoba určená ve smlouvě. Akceptační protokol / výkaz práce tvoří nedílnou součást faktury.

U systémů provozovaných v režimu outsourcing jsou dodržována pravidla bezpečnosti stanovená obecně platnými normami, směrnicemi ISMS a dalšími vnitřními předpisy JU.

4. MOBILNÍ PROSTŘEDKY VÝPOČETNÍ TECHNIKY

4.1. PRAVIDLA POUŽÍVÁNÍ

Níže uvedená pravidla platí v plné míře jak pro mobilní prostředky ve vlastnictví JU, tak i pro ty, které v jejím vlastnictví nejsou, ale jsou v rámci JU provozovány, instalovány a konfigurovány výhradně pro potřeby JU (např. zařízení v pronájmu, leasingu apod.).

Pro veškeré technické i netechnické prostředky instalované nebo provozované na JU platí následující pravidla:

- Provozování a využívání veškerých technických i netechnických prostředků schvalují odpovědní zástupci
- JU si vyhrazuje právo rozhodnout, které z těchto prostředků je možné využívat a které nikoliv, rozhoduje o tom pracoviště CIT
- jejich instalace, konfigurace nebo jiné nastavení provádí výhradně správci ICT JU
- nekompatibilní nebo nezpůsobilé prostředky nebudou instalovány, konfigurovány nebo provozovány
- veškeré prostředky musí být adekvátním způsobem chráněny proti:
    - zneužití třetími osobami (průnik do systému, aplikací apod.)
    - ztrátě nebo poškození (zničení, odcizení či poškození dat nebo prostředků ICT atd.)
    - neoprávněnému použití (přístup k důvěrným informacím, službám, tech. prostředkům)
    - použití, které není v souladu s účelem jejich pořízení
    - útokům třetích stran
- JU si vyhrazuje právo aktivního dohledu nad využitím mobilních prostředků v souladu s výše uvedenými pravidly
- bezpečnostní politika JU a směrnice ISMS vedou zaměstnance ke správnému zacházení s těmito prostředky a upozorňují na příslušná rizika, která s sebou odcizená zařízení, firemní a osobní data nesou.

Pro řádné spravování těchto aktiv si JU vyhrazuje právo veškeré informace přenášené na tato mobilní zařízení prověřovat a analyzovat.

4.2. EVIDENCE MOBILNÍCH PROSTŘEDKŮ

Evidence mobilních prostředků je součástí evidence majetku JU.

C. ZÁVĚREČNÁ USTANOVENÍ

Kontrolou dodržování této směrnice je pověřen ředitel CIT a ISMS nebo jím pověření zaměstnanci a IT manažeři součástí JU. Porušování cílů a zásad definovaných v této a další návazné dokumentaci ISMS zaměstnancem, studentem či účastníkem CŽV JU poškozuje dobré jméno a zájmy společnosti a může být považováno za porušování pracovních nebo studijních povinností.

SEZNAM PŘÍLOH

Označení přílohy	Název přílohy
ISMS-003-P1	Klíčové IS JU
ISMS-003-P2	Instalace Windows
ISMS-003-P3	Instalace OS LINUX-UNIX
ISMS-003-P4	Instalace síťových komponent
ISMS-003-P5	HelpDesk-řešení požadavků
ISMS-003-P6	Životní cyklus uživatele

SOUVISEJÍCÍ DOKUMENTY

Označení dokumentu	Název dokumentu
ČSN EN ISO 9001	Systémy managementu jakosti
ČSN ISO/IEC 27001	Systém řízení bezpečnosti informací - ISMS
ČSN ISO/IEC 17799	Soubor postupů pro řízení bezpečnosti informací
Zákon č.101/2000 Sb.	Zákon o ochraně osobních údajů
R 189/2012 + přílohy	Opatření prorektora – Spisový řád JU
ISMS-001	Politika ISMS JU
ISMS-002	Celková bezpečnostní politika JU
ISMS-006	Antivirová ochrana počítačů JU
ISMS-007	Správa a bezpečnost provozu počítačů
R85_2007	Užívání PC, SW, NET (Opatření rektora)
R378_2018	Pravidla pro ochranu a zpracování osobních údajů (Opatření rektora)
R379_2018	Ochrana osobních údajů v souvislosti s pracovněprávními vztahy (Opatření rektora)
Nařízení EU 2016/679	Nařízení Evropského parlamentu a Rady (EU) o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Představuje právní rámec ochrany osobních údajů (GDPR)