Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-007**
Název dokumentu:	**Správa a bezpečnost provozu počítačů JU**
Typ dokumentu:	Interní dokument - typ B – směrnice
Určeno pro:	všechny zaměstnance, studenty a účastníky CŽV JU
Prvek normy ISO:	27001
Datum vydání:	10.11.2010
Datum účinnosti:	15.11.2010
Platnost do:	odvolání
Počet stran + příloh:	12 + 5
Verze:	3.1 – aktualizace 07/2019 T.Linhart
Účel:	Správa počítačů JU a stanovení bezpečnostních pravidel a požadavků na jejich provoz - kategorie uživatelů, personální zajištění, pokyny pro správce, uživatele PC a studenty a účastníky CŽV na učebnách, evidence PC a tvorba pasportu.
Uložení:	Portál ISMS - https://isms.jcu.cz/
Ruší dokumenty:	http://itportal.jcu.cz/Documentation/veskera-dokumentace-na-it-portalu/jak-na-to/ Bezpečnostní požadavky na provoz PC stanic na JU
Zpracovatel:	Ing. Jana Kolářová-MIB JU, František Kubeš,DiS.- HS PC, Josef Jann-HS AVO
Přezkoumal:	ITM součástí JU
Schválil:	RNDr. Josef Milota - ředitel ISMS a CIT

OBSAH

A. ÚVODNÍ USTANOVENÍ

CÍL PROCESU A ÚČEL

Směrnice obsahuje základní informace ke správě a provozu počítačů ve vlastnictví JU, personální zajištění, této správy, kategorie uživatelů a pokyny pro správce, uživatele a studenty či účastníky CŽV na učebnách. Zároveň stanovuje povinnost vedení evidence počítačů a vytvoření pasportu pro každý PC s bližší identifikací a HW i SW konfigurací. Cílem je dosáhnout postupného sjednocení správy PC na všech součástech JU s budoucím využitím centrální domény (služby AD) pro všechny provozované počítače na JU.

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.
- **Certifikační autorita** - je subjekt, který vydává digitální certifikáty (elektronicky podepsané veřejné šifrovací klíče) a zaručuje totožnost vlastníka certifikátu a pravdivost údajů, které jsou uvedeny ve veřejném klíči.
- **Certifikát** (digitální) – datový soubor, uložený ve formátu dle mezinárodní normy X.509, která jednoznačně popisuje strukturu certifikátu. Neboli digitálně podepsaný veřejný klíč, který identifikuje uživatele a lze jej kryptograficky ověřit. Každý certifikát musí obsahovat unikátní sériové číslo, datum platnosti, identifikační údaje uživatele, veřejný klíč a identifikaci vydavatele = certifikační autority + další údaje.
- **Freeware** – software, který je distribuován bezplatně. Jedná se tedy o volně šiřitelný program, bez placení autorského honoráře. Nedodává se k němu zdrojový kód a je zakázáno jej vnitřně upravovat. To je výhradně v kompetenci autora freeware.
- **Free SW** - neboli svobodný software, který mohou uživatelé spouštět, kopírovat, distribuovat, studovat, měnit a zlepšovat, přičemž mají k dispozici jeho zdrojový kód. V širším slova smyslu jde též o GNU neboli Open source SW, jehož použití není takto jasně a jednoznačně specifikováno.
- **Homeworking -** způsob práce, kdy zaměstnanec trvale pracuje z domova.
- **Identifikační karta (IK)** - plastová čipová bezkontaktní identifikační karta přidělovaná zaměstnancům, studentům či účastníkům CŽV popř. i absolventům oddělením CIT-IPS 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.
- **Infiltrace PC** – jakýkoli neoprávněný vstup do počítačového systému.
- **Netbook** – malý přenosný osobní počítač s nízkou hmotností (asi 1 kg) a spotřebou, jehož výkon odpovídá i nižší ceně.
- **Pasport** – identifikační list osobního počítače **JU** (PC, NB, netbook) – viz příloha 4 této směrnice.
- **Ping** (Packet InterNet Groper) – program, který umožňuje prověřit funkčnost spojení přes protokol TCP/IP mezi dvěma síťovými rozhraními (PC, síťová zařízení) v počítačové síti.
- **Heslo** – na JU stanoven řetězec min. osmi znaků (kombinace alfanumerických, ev. speciálních s výjimkou mezery a diakritiky). Musí obsahovat znaky alespoň tří znakových sad ze čtyř (velké písmeno, malé písmeno, číslice nebo speciální znaky). Heslo nesmí být totožné s názvem účtu a jménem a příjmením uživatele účtu. Obecně platí, že čím je heslo delší, tím hůře je odhalitelné.
- **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.
- **Traceroute** - program Unix OS pro analýzu počítačové sítě, mapuje komunikační cestu od zdroje k cíli, obdoba pro OS Windows se jmenuje tracert.
- **Uživatel** – je zaměstnanec, student nebo účastník CŽV JU.

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.

- **BS –** bezpečnostní správce ICT součásti JU (funkce popsaná v dokumentu *ISMS-002_Celková bezpečnostní politika JU)*.
- **CA** – viz Certifikační autorita.
- **CIT –** Centrum informačních technologií – celoškolské pracoviště JU.
- **CŽV –** celoživotní vzdělávání.
- **HS AVO –** hlavní správce antivirové ochrany na JU.
- **HS PC –** hlavní správce počítačů na JU, který informuje a metodicky řídí lokální správce součástí 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.
- **IK** – viz Identifikační karta.
- **IPS** – Identifikační a přístupový systém – pracoviště CIT, které na JU provozuje a spravuje JIS a další IS.
- **ISMS** (Information Security Management System) – Systém řízení bezpečnosti informací.
- **IT** – Informační technologie.
- **ITM** – IT manažer, který zajišťuje IT služby své součásti.
- **JIS** – Jednotný identifikační systém = informační subsytém JU, který spravuje a udržuje celoškolské pracoviště CIT IPS.
- **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 AVO –** lokální správce antivirové ochrany na každé součásti JU (fakulty, ústavy).
- **LS PC -** lokální správce počítačů na každé součásti JU.
- **MIB –** Manažer informační bezpečnosti JU.
- **MS (**MicroSoft) - zkratka firmy Microsoft, který obvykle předchází názvu SW produktu.
- **NB** (NoteBook) - přenosný počítač.
- **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.
- **PIN** (Personal Identification n umber) **-** osobní identifikační číslo jako identifikátor, pomocí kterého je možné se autorizovat např. u platební či identifikační karty, mobilního telefonu, vstupních kódů apod.
- **PKI** (Public Key Infrastructure) - pokročilá možnost přihlašování se pomocí digitálních certifikátů. Jde o infrastrukturu správy a distribuce veřejných klíčů u asymetrické kryptografie. PKI využívá certifikační autorita.
- **SW** (SoftWare) - programové vybavení počítače.
- **USB** (Universal Serial Bus) - je univerzální sériová sběrnice pro připojení periférií (tiskárna, flash disk, klávesnice, fotoaparát, modem,…) k počítači .

ODPOVĚDNOSTI A PRAVOMOCI

- **Hlavní správce PC JU** (**HS PC**)
  a) definuje a aktualizuje obecně závaznou metodiku správy PC na JU
  b) metodicky řídí činnost lokálních správců PC na jednotlivých součástech – vydává metodické pokyny pro LS PC
  c) kontroluje dodržování předpisů pro správu PC na JU
  d) řídí a spravuje centrální doménu AD
  e) spolupracuje s HS AVO při odstranění závažné infiltrace PC.

- **Lokální správce PC** (**LS PC**) - správce IT součásti JU (pracovník součásti, jehož funkce se mohou kumulovat – např. LS AVO, BS nebo ITM) pověřený správou počítačů své součásti - vykonává tyto činnosti:
  a) kontroluje dodržování předpisů pro správu PC na své součásti
  b) řídí se pokyny hlavního správce PC JU či jeho zástupce
  c) odpovídá za distribuci aktuálního licenčního SW uživatelům své součásti
  d) instaluje a konfiguruje PC podle pokynů HS PC a podle této směrnice, případně v souladu s platnou metodikou vydanou v rámci své součásti, která nesmí být v rozporu s touto směrnicí
  e) vede evidenci PC provozovaných na své součásti

f) vytváří Pasport pro každý počítač své součásti zaváděný do provozu (výjimkou mohou být stejné typy PC na učebnách), povinně u PC v režimu práce Homeworking, jinak volitelně - dále kapitola 5 této směrnice
g) informuje uživatele své součásti o důležitých změnách souvisejících s používáním PC
h) může vydávat interní pokyny pro uživatele své součásti týkající se práce na PC.

- **Uživatel** - zaměstnanec, student nebo účastník CŽV JU, který využívá počítač v majetku JU a jeho programové vybavení. Při činnostech na počítači musí dodržovat následující ustanovení:
  a) dodržuje pravidla vyplývající z této směrnice
  b) řídí se pokyny svého lokálního správce PC nebo jeho zástupce, případně HS PC a musí jim v případě potřeby umožnit přístup na PC
  c) využívá PC v rámci své pracovní náplně a v souladu s výzkumným a vzdělávacím posláním JU
  d) plně zodpovídá za negativní dopady způsobené nesprávnou manipulací na jemu svěřeném PC, pokud bylo prokázáno nedodržení této směrnice nebo jiných bezpečnostních zásad JU při práci na PC
  e) po obdržení Pasportu svého počítače od LS PC provádí průběžnou aktualizaci Pasportu v souladu s ev. změnami - dále kapitola 5 této směrnice
  f) v případě problémů na svém PC kontaktuje LS PC nebo jeho zástupce, má-li podezření na infiltraci PC, pak se obrací přímo na LS AVO součásti.

Další odpovědnosti jsou součástí textu.

ZMĚNY OPROTI PŮVODNÍ VERZI

Od 15.2.2011 je vedení Pasportu počítače povinné pouze v režimu práce Homeworking. Změny ve verzi 2.0 se vztahují k částem této směrnice, která dosud volitelnost nepřipouštěla. V oddílu C. Závěrečná ustanovení byly také doplněny další směrnice ISMS související s problematikou počítačů.
Verze 3.0 znamená přidání kategorie uživatele účastník CŽV.
Verze 3.1 upravuje informace o tvaru hesla IDM v kapitole 3.2

B. POPIS

1. KATEGORIE UŽIVATELŮ JU

1.1. BĚŽNÝ UŽIVATEL

Běžný typ uživatele (zaměstnanec, student JU či účastník CŽV) používající počítač v majetku JU, který má omezená oprávnění k práci s PC (není veden jako administrátor) a je zpravidla řízen službami Active Directory (AD) pro správu PC s OS Windows.

1.2. PRIVILEGOVANÝ UŽIVATEL

Uživatel s právy administrátora – obvykle správce serveru, sítě, počítačů či jiných zařízení IT nebo administrátor IS či DB, případně jiný zkušený uživatel, který má oprávnění provádět privilegované operace a řídit provoz na jemu svěřené technice či IS. Tyto výjimky povoluje ITM, BS nebo LS PC dané součásti. Pracovníci APS/CIT, ITM, BS, HS a LS součástí mají tato privilegia automaticky.

Privilegovaný uživatel zodpovídá za funkčnost svého PC a jeho případné neodborné zásahy do OS i činnosti, které nejsou v souladu s bezpečnostními směrnicemi ISMS JU, budou považovány za porušení pracovní kázně se všemi důsledky z toho vyplývajícími.

Všichni uživatelé PC musí umožnit HS nebo LS PC dané součásti v případě jeho potřeby přístup na jim svěřený počítač.

2. PERSONÁLNÍ ZAJIŠTĚNÍ SPRÁVY PC

2.1. HLAVNÍ SPRÁVCE PC (HS PC)

HS PC je zaměstnanec JU určený ředitelem CIT, který má pravomoc řídit lokální správce PC jednotlivých součástí a vydává dle potřeby doplňující metodické pokyny. Jeho odpovědnosti a další pravomoci jsou popsány v oddíle A. Nejedná se o samostatnou pracovní pozici, ale funkci spojenou obvykle s jinými činnostmi správy ICT. Musí mít svého zástupce.

2.2. LOKÁLNÍ SPRÁVCE PC (LS PC)

LS PC je určen vedoucím dané součásti JU nebo IT manažerem pro činnosti spojené se správou počítačů v rozsahu své působnosti. Nejde o samostatnou katalogovou funkci, ale bývá obvykle kumulovaná s dalšími činnostmi v oblasti ICT. Je doporučeno, aby byl LS PC totožný se správcem AVO, neboť jde o úzce propojené aktivity, které by měly být realizovány jedním zaměstnancem. Jeho odpovědnosti a pravomoci jsou popsány v oddíle A. Měl by mít svého zástupce.

Seznam správců PC na JU je uveden v příloze této směrnice – viz "*ISMS-007-P1_PC-Správci*" a bude dle potřeby aktualizován. Je také interně dostupný všem uživatelům JU po přihlášení na portál ISMS ve složce "*Kontakty*".

3. BEZPEČNOSTNÍ POŽADAVKY NA PROVOZ PC NA JU

Některé zásady a doporučení týkající se antivirové ochrany a chování uživatelů v souvislosti s bezpečným provozem osobních počítačů jsou obsaženy ve směrnici "*ISMS-006_Antivirová ochrana počítačů JU*". V této kapitole jsou uvedena další pravidla, která je třeba respektovat. Jsou rozdělena na pokyny pro správce, uživatele PC a studenty či účastníky CŽV na učebnách. Má-li uživatel administrátorská práva (privilegovaný uživatel), musí dodržovat pokyny pro správce i uživatele.

3.1. POKYNY PRO SPRÁVCE POČÍTAČŮ

Počítače zaměstnanců, studentů a účastníků CŽV JU musí být nainstalovány a nakonfigurovány tak, aby byly splněny základní požadavky na jejich bezpečný provoz. Primárně se týkají klientských stanic pro práci s centralizovanými agendami JU (FIS, Mzdy, STAG a další), ale musí být aplikovány na všech počítačích všech součástí JU, tedy i na PC na katedrách a učebnách. Základní instalace - OS a nezbytný SW (viz

příloha *„ISMS-007-PC_Základní instalace SW na PC JU“)* provedou lokální správci počítačů nebo jejich zástupci. Ti zajistí, aby počítače všech uživatelů splňovaly následující požadavky:

1. Používat lze pouze operační systém, který umožňuje omezení uživatelských práv na PC - Windows 2000/XP/Vista/7, event. Linux či Mac OS X. Při instalaci musí být splněny licenční podmínky SW.
2. Pravidelně aktualizovat OS (mít nastavenu jeho automatickou aktualizaci) a další legálně používaný SW, tj. instalovat záplaty bezpečnostních děr.
3. Správně nastavit úrovně bezpečnosti používaného SW (MS Internet Explorer nebo Mozilla Firefox, poštovní klient, OS, firewall, MS Office, AV SW a další).
4. Uživatel PC musí mít přidělen pro přístup do sítě JU uživatelský účet s prvotním heslem - zajišťuje správce IDM. LS PC informuje uživatele při předání počítače, že je nutno si toto heslo neprodleně změnit, dále viz následující odstavec 3.2. b).
5. Běžný uživatel musí mít omezená uživatelská práva – zajistí LS PC (např. skupina Users ve Windows 2000/XP/Vista/7).
6. Nastavit OS PC tak, aby byl před zahájením práce na PC uživatel donucen se vždy přihlásit, heslo platilo jen po omezenou dobu (pro privilegované uživatele max. 6, pro běžného 12 měsíců), a poté si jej uživatel byl nucen změnit. Toto lze nastavit u PC v doméně řízené AD (Active Directory), kde je doba platnosti hesla určována pomocí skupinových politik (Group Policy).
7. U PC řízených AD nastavit historii hesla min. na 5, aby byl uživatel nucen si nastavit heslo nové.
8. Na PC musí být nainstalován firewall a nastavena jeho trvalá aktualizace.
9. Nainstalovaný firewall by měl povolit příchozí provoz jen z důvěryhodných počítačů a sítí a jen ten provoz, který je důležitý pro správnou činnost PC v síti JU, provozovaných aplikací nebo nástrojů pro administraci aplikací, PC nebo sítí (např. ping, traceroute apod).
10. Zařazení počítačů nebo sítí mezi důvěryhodné by mělo být restriktivní (důvěryhodných počítačů by mělo být co nejméně).
11. Na PC připojené do sítě JU musí být vždy spuštěn předepsaný antivirový SW s automatickou aktualizací virové databáze, který byl stanoven pro používání na JU – viz dokument *„ISMS-006_Antivirová ochrana počítačů JU“*. Za jeho instalaci a nastavení zodpovídá LS AVO, který se řídí pokyny HS AVO.
12. Nastavit automatické aktualizace u nainstalovaných aplikací, pokud je to možné.
13. Na učebnách JU a v knihovně nastavit na každý PC heslo pro BIOS, které zná jen správce, aby na PC nebylo možné měnit základní nastavení.
14. V případě přihlášení k PC řízeným AD pomocí čipu PKI přístupové karty nastavit chování PC tak, aby při vyjmutí této karty došlo k uzamčení počítače.

Tyto požadavky platí i pro počítače zaměstnanců, studentů a účastníků CŽV v majetku JU, s nimiž se připojují do univerzitní počítačové sítě a jsou umístěny mimo objekty JU.

3.2. POVINNOSTI UŽIVATELE

a) Používat počítač v rámci své pracovní náplně v souladu s výzkumným a vzdělávacím programem JU, nikoli ke komerčním účelům či v rozporu s autorským zákonem.

b) Po přidělení individuálního účtu, po prvním přihlášení do sítě JU a rovněž dále periodicky si změnit své prvotní přidělené heslo. To lze provést buď na portálu IDM, ev. přes ITportál-IDM, kde je možné nalézt informace ke správě uživatelského účtu, který se používá také pro přístup k některým IS, nebo postupovat podle interních předpisů dané součásti, existují-li. Bližší informace poskytne LS PC součásti. Nové heslo nesmí být kratší než dvanáct znaků a musí obsahovat min. jedno malé písmeno, jedno velké písmeno a jednu číslici. Heslo nesmí obsahovat tři po sobě následující znaky z atributů – titul, jméno, příjmení, uživatelské jméno a dále znaky s diakritikou ani mezeru, ale může obsahovat některé speciální znaky jako např. čárka, tečka, středník a pomlčka. Privilegovaní uživatelé by měli volit hesla delší. Heslo musí uživatel držet v tajnosti.

c) Odpovídá za škody vzniklé zneužitím svého uživatelského účtu, pokud je umožnil vlastním nedbalým zacházením s účtem nebo heslem.

d) V případě důvodného podezření, že někdo neoprávněně používá cizí účet, bezodkladně informovat LS či HS PC a MIB.

e) Dostane-li uživatel přidělen PC bez vědomí LS PC své součásti, je povinen mu to neprodleně oznámit a umožnit mu na tento počítač přístup, aby si založil lokální administrátorský účet pro případ nápravy event. kolize na tomto PC.

f) Je-li nutné PC z pracovních důvodů sdílet s dalšími uživateli, musí se každý uživatel přihlásit a pracovat pod vlastním uživatelským účtem a po skončení relace ukončit všechny aplikace a odhlásit se.

g) Při ukládání dat na PC z jiných zdrojů pečlivě zvažovat, zda jde o zdroj důvěryhodný a neotevírat žádné neznámé dokumenty, jejichž obsahem či původem si uživatel PC není jist.

h) Zálohovat vlastní data z PC na externí médium (CD, DVD, flash disk, externí disk) či server (informaci o této možnosti poskytne LS PC) pro případ nutnosti obnovy těchto dat z důvodu SW či HW havárie nebo infiltrace PC.

i) Dodržovat všechna ustanovení uvedená v kapitole 5 směrnice "*ISMS-006_Antivirová ochrana počítačů JU*", která s touto směrnicí úzce souvisí.

3.3. SPECIFIKA PRO UŽIVATELE IDENTIFIKAČNÍCH KARET S PKI ČIPY

Vybraným uživatelům JU bude pracovištěm IPS CIT vydána nová identifikační karta (IK) s PKI čipem, na níž bude uložen certifikát od fy Cesnet TCS s platností tři roky pro podepisování a schvalování dokumentů JU (např. faktur, cestovních příkazů, PDF souborů apod.).

Dále na ní může být uložen také digitální certifikát pro přihlašování do centrální domény AD od interní CA s platností jeden rok. To se zatím týká správců počítačů AD. K problematice IK s certifikáty je již vydána zvláštní směrnice *ISMS-009_Elektronický podpis a certifikáty* s podrobnějšími informacemi.

Držitelé těchto IK musí respektovat následující pokyny:

- uživatel musí dodržovat certifikační politiky a pravidla stanovená certifikačními autoritami, které vydaly certifikáty, jež uživatel používá – JU spolupracuje s CA Cesnet a využívá CA AD JU
- pokud uživatel vlastní certifikát k přihlášení do domény AD, musí jej k přihlašování do této domény přednostně použít (nikoliv uživatelské jméno a heslo)
- při odchodu od PC musí uživatel IK vyjmout ze snímače a uschovat ji, tj. nenechávat ji bez dozoru ve své kanceláři
- uživatel musí udržovat v tajnosti PIN ke své ID kartě.

3.4. CO UŽIVATEL NESMÍ

- Nesmí používat SW či HW prostředky pro odhalování či odposlech uživatelských hesel
- nesmí zasahovat do hardwarové konfigurace počítače a BIOSu
- nesmí přemísťovat PC nebo HW komponenty bez vědomí LS PC
- nesmí provádět zásahy do operačního systému, vyjma běžných uživatelských nastavení
- nesmí používat nelegálně nabyté programové vybavení
- nesmí porušovat autorský zákon pořizováním či šířením nelegálních kopií autorských děl (publikace, CD, DVD, SW apod.)
- nesmí využívat počítač JU k osobním komerčním účelům (poskytovat informace, programy či data za úplatu apod.)
- nesmí používat pro připojení k počítačové síti jinou síťovou adresu, než mu byla přidělena (automaticky nebo staticky)
- nesmí zpřístupnit svůj uživatelský účet jiným uživatelům
- nesmí otvírat neznámé stránky či e-maily, potvrzovat hlášení, u kterých si není jist, co způsobují
- nesmí používat PC k obtěžování či zastrašování jiných uživatelů či pro reklamní účely
- nesmí využívat počítač a infrastrukturu počítačové sítě k páchání trestných činů
- nesmí se pokoušet se neoprávněně získat vyšší přístupová práva, než mu byla přidělena
- nesmí porušovat zákon 101/2000 Sb. na ochranu osobních údajů, pokud s nimi při své činnosti přichází do styku.

3.5. POKYNY PRO STUDENTY A ÚČASTNÍKY CŽV NA UČEBNÁCH A V KNIHOVNĚ

Na učebnách a v knihovně jsou PC sdílené více uživateli. Vlastníkem PC je JU, která je poskytuje ke studijním účelům. Správce učebny, jehož jméno s telefonním kontaktem musí být viditelně v těchto

prostorách vyvěšeno, zodpovídá za instalovaný SW na těchto počítačích a spolu s LS AVO za nastavení antivirové ochrany.

Student a účastník CŽV musí dodržovat relevantní pravidla chování uživatele (viz předchozí kapitoly 3.2. a 3.4.) a kromě zásad uvedených v této směrnici i související směrnici "*ISMS-006_Antivirová ochrana počítačů JU"*, musí respektovat následující ustanovení:

- Musí se **vždy přihlásit pod svým uživatelským účtem** a po **skončení činnosti se opět odhlásit**, aby nemohl být jeho účet zneužit. Za chyby způsobené zcizením účtu zodpovídá jeho majitel.
- Před ukončením relace na PC (odhlášením) **uzavřít všechny spuštěné aplikace** včetně otevřených oken internetového prohlížeče.
- Nikdy **neukládat na PC své heslo pro přístup k jakékoli spouštěné aplikaci do PC**, bude-li to systém či aplikace umožňovat, zvláště pak ne u univerzitních IS (STAG, Odysea atd.). Např. nikdy v internetovém prohlížeči nevolit nabídku "Zapamatovat heslo" (např. „Má si Firefox zapamatovat heslo pro ….").
- V případě kolize, **podezření na infiltraci** či nefunkčnost PC o této skutečnosti neprodleně **informovat správce učebny**.

4. EVIDENCE POČÍTAČŮ

Každý LS PC musí vést evidenci provozovaných PC na své součásti. Dokud nebude na JU či její některé součásti k dispozici aplikace pro tyto účely, je nutné vést evidenci počítačů alespoň ve formě přílohy 2, s minimem údajů o PC, event. další informace o počítači a uživateli jsou uvedeny v Pasportu PC – viz kap. 5 níže. Používá-li LS PC jiný způsob evidence počítačů a jsou v ní obsaženy údaje z přílohy č. 2, je to považováno za vyhovující. Má-li některá součást JU jen malý počet PC, lze k této evidenci využít i složku *Aktiva IT* na portále *isms.jcu.cz*, kde každý PC je pak evidován jako jedno aktivum.

4.1. EVIDENCE DLE PŘÍLOHY 2

V příloze č. 2 této směrnice – viz soubor „*ISMS-007-P2_PC-Evidence*" - je formulář pro vedení evidence počítačů součásti. Evidovány musejí být i přenosné počítače a PC na učebnách.

LS PC:

- doplní do záhlaví dokumentu zkratku své součásti, své jméno a datum poslední aktualizace, kterou provádí průběžně dle změn počtu PC
- zaeviduje do tabulky všechny počítače své součásti podle předepsaných údajů (inventární číslo, označení budovy, číslo místnosti, příjmení a jméno uživatele, A/N podle kategorie uživatele-privilegovaný/ běžný). Ve sloupci Poznámka může uvést např. e-mail uživatele, odkaz na Pasport počítače, vyřazení PC apod.)
- v případě přenosných počítačů se ve sloupci *Místnost* uvede „NB" a jde-li o PC umístěný mimo JU, pak do sloupce *Budova* zapíše text „MIMO".

Je-li veden Pasport PC, pak jsou v něm uvedeny další podrobnější údaje.

4.2. VYŘAZENÍ POČÍTAČE

Při vyřazení počítače z provozu LS PC součásti JU provede následující kroky:

- do evidence PC do sloupce poznámka doplní datum vyřazení PC
- smaže pevné disky PC nejlépe jejich přeformátováním
- informuje zaměstnance pověřeného vyřazením PC z evidence majetku
- PC předá k likvidaci technikovi nebo postupuje podle pravidel likvidace své součásti.

4.3. AKTUALIZACE EVIDENCE POČÍTAČŮ

Evidenci počítačů je nutné udržovat v aktuálním stavu, tj. zaznamenávat do ní další počítače, nejlépe následně po jejich uvedení do provozu. Revize a aktualizace musí být provedena **nejméně jednou za půl roku**. Tyto činnosti **provádí a za ně zodpovídá LS PC**. Kontrolu provádí ITM součásti nebo vedoucí součásti (je-li ITM a LS PC tatáž osoba), případně jím pověřený zaměstnanec.

5. PASPORT POČÍTAČE

Počítač v majetku JU může mít svůj vlastní identifikační list – tzv. Pasport - se specifikací PC, informací o uživateli, který jej provozuje a s popisem HW a SW konfigurace. Pasport je povinný pouze u počítačů, které se vyskytují mimo prostory JU a uživatel, jemuž byl PC svěřen pracuje z domova formou Homeworkingu. V ostatních případech je volitelný. Nebude-li na JU či součásti provozována aplikace pro evidenci počítačů, která bude schopná pasport vygenerovat, měl by být vytvořen dle přílohy č. 4 této směrnice, a to jak v digitální, tak prvotně i v listinné podobě. Do pasportu je doporučeno zaznamenávat i volně dostupný SW – freeware či Free SW.

5.1. PC NOVĚ ZAVÁDĚNÉ DO PROVOZU

Každý počítač zaváděný do provozu na kterékoli součásti JU (týká se i přenosných PC) musí být předáván uživateli lokálním správcem PC vždy současně s identifikačním listem – tzv. Pasportem počítače – viz příloha č. 4 – „*ISMS-007-P4_PC-Pasport*“ pouze v případě práce v režimu Homeworking (dále viz směrnice *ISMS-010_Homeworking*). V ostatních případech je pouze doporučen. Tento pasport vytváří, předává a archivuje LS PC.

Základní instalace PC

Prvotní instalaci SW provádí na PC výhradně LS PC, který je zodpovědný za dodržení uvedených postupů. Uživatel nového PC je povinen jej kontaktovat pro prvotní instalaci, pokud by obdržel PC bez vědomí LS PC. Další informace k základní instalaci jsou uvedeny v kapitole 6 níže.

Postup vyplnění pasportu: (provede LS PC)

- záhlaví pasportu - uvést zkratku součásti JU
- identifikační údaje o PC – inventární číslo, výrobní číslo a model-název PC
- identifikační údaje o uživateli - doplnit příjmení a jméno uživatele včetně indikace administrátorských práv (A= má právo Admin, N= nemá, jde o běžného uživatele), e-mail a telefonní kontakt na uživatele
- HW počítače – uvést základní konfiguraci PC
- SW počítače – doplnit SW nainstalovaný na předávaném počítači, včetně OS a freeware včetně dalších požadovaných atributů (typ licence, doklad, datum instalace a příjmení autora instalace). Není-li uveden nabývací doklad, musí být možnost jej dohledat v ekonomickém oddělení součásti. Ten jediný je právoplatným podkladem pro legální používání SW.
- datum předání PC.

Předání pasportu – LS PC:

- LS PC vytiskne pasport oboustranně ve dvou vyhotoveních
- podepíše jej spolu s uživatelem
- jeden výtisk archivuje a jeden předá uživateli, který tím potvrzuje převzetí PC a dodržování uvedených pokynů
- zašle uživateli pasport v digitálním tvaru k budoucí aktualizaci – viz bod 5.4 níže.

5.2. PC JIŽ PROVOZOVANÉ

Uživatelé počítačů pracující z domova a nebo uživatelé součástí, které vedou pasporty PC tyto počítače jsou již používány, budou postupně kontaktováni lokálním správcem PC své součásti, který zmapuje jejich HW a SW konfiguraci a vyhotoví a předá pasport stejným způsobem, jak je popsáno v předchozí podkapitole 5.1.

Privilegovaní uživatelé se mohou dohodnout s LS PC své součásti na postupu vyhotovení pasportu, který bude také archivovat LS PC podepsaný v listinné i digitální podobě. Se souhlasem LS PC, mohou tito uživatelé vytvořit pasport sami a předat jej LS PC k podpisu a archivaci v digitální i listinné podobě. Konečný termín vyhotovení pasportů za všechny provozované počítače součásti JU stanoví ITM nebo LS PC po vydání této směrnice.

5.3. PC NA UČEBNÁCH

Je-li učebna vybavena počítači se shodnou SW a HW konfigurací, stačí vyhotovit jen jeden pasport za všechny PC a v identifikaci PC – sériovém čísle uvést jejich počet. Do evidence aktiv IT na portále ISMS do složky své součásti pak zaevidovat jedno aktivum s uvedením počtu PC a celkovou cenou. Nemá-li LS PC do složky Aktiva IT přístup, požádá svého ITM či BS, ev. MIB o přístup nebo vložení tohoto aktiva, není-li již v interní složce součásti zaevidováno. Tato položka musí být v aktivech uvedena vždy, bez ohledu na režim práce.

5.4. AKTUALIZACE PASPORTU

Pasport by měl být aktualizován při každé změně SW či HW konfigurace. Za tuto aktualizaci odpovídá uživatel, stejně jako za zaslání digitální kopie LS PC své součásti JU. Aktualizace musí být provedena nejméně jednou ročně s výjimkou, kdy nedošlo k žádné změně.

Provádí-li další instalace SW LS PC, je jeho povinností buď informovat uživatele o změně a potřebě jejího zápisu do pasportu nebo aktualizovat pasport PC uživatele a předat mu digitální kopii.

6. DOPORUČENÁ ZÁKLADNÍ INSTALACE SW NA PC

Na každém PC či NB v majetku JU je doporučeno nainstalovat software, který je uveden v příloze *„ISMS-007-P3_PC-Základní instalace SW* “. Tuto prvotní instalaci vždy zajistí LS PC součásti. Další SW instaluje LS PC dle potřeby běžného uživatele a nebo privilegovaný uživatel sám, vždy v souladu s licenčními podmínkami SW.

LS PC může tento seznam SW přizpůsobit potřebám součásti, ale musí přitom dodržet licenční podmínky každého jednotlivě instalovaného SW. Nejde-li o Freeware či Free SW, musí být instalovaný SW podložen platnou licencí s nabývacím dokladem o jejím zakoupení.

Při předání počítače uživateli, který pracuje z domova (režim Homeworking), doplní LS PC do pasportu každého počítače, včetně přenosných počítačů, nainstalovaný SW - viz příloha č. 4 *„ISMS-007-P4_PC-Pasport“*. Další postup související s pasportem PC je uveden v kapitole 5 výše.

7. OCHRANA CITLIVÝCH DAT

Data, která jsou uložena na PC nebo jeho záložním médiu mohou mít charakter důvěrných dat, tzn. mohou obsahovat údaje, které chceme chránit před zneužitím či odcizením. Jde např. o osobní data, PINy, přístupová hesla k bankovním či počítačovým účtům, přístupové klíče k trezorům, finanční informace, telefony atd. Nejvhodnější forma jejich ochrany je v tomto případě zašifrování pomocí vhodné volně dostupné či placené počítačové aplikace. Nepovolané osoby pak nemají k datům přístup bez znalosti hesla nastaveného při kryptování. Toto heslo je samozřejmě nezbytné uchovat v tajnosti.

Z velkého množství nabízených programů v oblasti kryptografie lze doporučit velmi spolehlivou a variabilní aplikaci TrueCrypt, kterou jako freeware nabízí firma TrueCrypt Foundation a je k dispozici i v české verzi. Umí vytvořit virtuální zašifrovaný disk uvnitř souboru nebo zašifrovat část paměťového média včetně USB paměti. Návod k použití a bližší informace o tomto programu jsou popsány v příloze 4 této směrnice - dokument “*ISMS-007-P5_PC-Zabezpečení citlivých dat šifrováním*“. Program TrueCrypt může být provozován na všech PC s OS Windows všech verzí, Linux i MAC OS X a může být spouštěn (s omezením určitých funkcí) i bez instalace.

C. ZÁVĚREČNÁ USTANOVENÍ

Kontrolou dodržování této směrnice je pověřen HS PC a ředitel CIT a ISMS nebo jím pověřená osoba. Porušování cílů a zásad definovaných v této a další návazné dokumentaci ISMS zaměstnancem, studentem či účastníkem CŽV JU poškozuje dobré jméno a zájmy univerzity a může být považováno za porušování pracovních či studijních povinností se všemi důsledky z toho vyplývajícími.

SEZNAM PŘÍLOH

Označení přílohy	Název přílohy
ISMS-007-P1	PC-Správci
ISMS-007-P2	PC-Evidence (pro LS PC)
ISMS-007-P3	PC-Základní instalace SW (pro LS PC)
ISMS-007-P4	PC-Pasport
ISMS-007-P5	PC-Zabezpečení citlivých dat šifrováním.

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
ISMS-001	Politika ISMS JU
ISMS-002	Celková bezpečnostní politika JU
ISMS-006	Antivirová ochrana počítačů JU
ISMS-009	Elektronický podpis a certifikáty
ISMS-010	Homeworking
R95_2007	Užívání PC, SW, NET (Opatření rektora)
R7_2004 / nové R168_2011	Opatření rektora k uplatnění a zavádění jednotného identifikačního a přístupového systému na Jihočeské univerzitě v Českých Budějovicích
R186_2011	Opatření rektorky – Homeworking