Jihočeská univerzita
v Českých Budějovicích
University of South Bohemia
in České Budějovice

ISMS - SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

Označení dokumentu:	**ISMS-008**
Název dokumentu:	**Správa a bezpečnost počítačové sítě JU**
Typ dokumentu:	Interní dokument - typ B – směrnice
Určeno pro:	všechny zaměstnance, studenty a účastníky CŽV JU
Prvek normy ISO:	27001
Datum vydání:	22.4.2013
Datum účinnosti:	22.4.2013
Platnost do:	odvolání
Počet stran + příloh:	13 + 2
Verze:	1.0
Účel:	Zásady a stanovení bezpečnostních požadavků na provoz počítačové sítě JU
Uložení:	Portál ISMS - https://isms.jcu.cz/
Ruší dokumenty:	-
Zpracovatel:	Ing. Jana Kolářová - MIB JU, Bc. Petr Šimek - HS sítě JU
Přezkoumal:	IT manažeři a správci sítě součástí JU, HS PC, vedoucí středisek CIT
Schválil:	RNDr. Josef Milota - ředitel ISMS a CIT

OBSAH

A. ÚVODNÍ USTANOVENÍ

CÍL PROCESU A ÚČEL

Cílem tohoto dokumentu je stanovit pravidla a opatření platná pro všechny subjekty počítačové sítě JU, aby byla tato síť co nejlépe zabezpečena a nebyl narušován její provoz.

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. Bližší informace o běžných typech a postupech – viz interní směrnice ISMS-006_ Antivirová ochrana počítačů JU .
- **Eduroam** - je akademický roamingový systém poskytující síťovou konektivitu pro své uživatele v připojených organizacích. Přístup je založen na zabezpečené autentizaci v domácí instituci - VŠ, AV a další vzdělávací ústavy. Správcem eduroam v ČR je Sdružení CESNET, z. s. p. o. Česká eduroam je součástí evropské konfederace národních eduroam.
- **Firewall** (FW) - je síťové zařízení se speciálním SW sloužící k řízení a zabezpečování provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně řečeno - definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Cílem je ochrana vlastní počítačové sítě nebo počítače samotného, v závislosti na typu FW. Vstupní a výstupní kanály sítě nebo počítače jsou softwarem monitorovány a FW některé z nich povoluje a jiné zakazuje - dle nastavení správce/uživatele. Nehlídaným portem může vniknout do počítače malware. Firewall je také součástí OS Windows, je standardně zapnut a je doporučené jej provozovat (kontrola: Ovládací panely-> Brána Windows firewall). Navíc většina antivirových firem dodává (volitelně) AV SW i s firewallem.
- **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). Obecně platí, že čím je heslo delší, tím hůře je odhalitelné.
- **Hoax** – poplašná zpráva, která varuje před neexistujícím nebezpečným virem, problémem či fakty, které se nezakládají na pravdě, s výzvou k dalšímu rozesílání.
- **Infiltrace PC** – jakýkoli neoprávněný vstup do počítačového systému.
- **Internet** - je celosvětový systém navzájem propojených počítačových sítí, ve kterých mezi sebou počítače komunikují pomocí rodiny protokolů TCP/IP. Cílem všech uživatelů Internetu je bezproblémová komunikace - výměna dat.
- **Intranet** – firemní počítačová síť, která používá stejné technologie (protokoly) jako Internet. Na rozdíl od něj je však Intranet privátní („soukromý"), tj. jeho využívání je omezeno na určitý okruh uživatelů např. firmy, školy, různé instituce apod.
- **IP adresa** - číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol). V současné době je nejrozšířenější verze IPv4, která používá 32bitové adresy, např. 192.168.0.1. Z důvodu nedostatku IP adres bude nahrazen protokolem IPv6, který používá 128bitové IP adresy.
- **Malware** (Malicious software) - souhrnný výraz pro jakýkoliv škodlivý program. Tento pojem zahrnuje počítačové viry, adware, spyware, červy, trojské koně a několik dalších. Seznam nejnovějšího malware lze nalézt např. na http://www.hoax.cz/malware/.
- **Počítačová síť** - (anglicky computer network) je souhrnné označení pro technické prostředky, které realizují spojení a výměnu informací mezi počítači. Umožňují tedy uživatelům komunikaci podle určitých pravidel, za účelem sdílení využívání společných zdrojů nebo výměny zpráv.
- **Ping** (Packet InterNet Groper) – program, který umožňuje prověřit funkčnost spojení přes protokol TCP/IP mezi dvěma síťovými rozhraními (PC, síťová zařízení) v počítačové síti.
- **Server** – obvykle výkonnější počítač, který poskytuje uživatelům nějaké služby, které určují druh serveru, jako např. souborový, tiskový, databázový, www, aplikační, mailový server apod.
- **Spam** – nevyžádané sdělení, obvykle e-mailová zpráva.
- **Software** (SW) – programové vybavení počítače.
- **Správce počítačů** – zaměstnanec JU pověřený údržbou operačních systémů a dalšího software na osobních počítačích (PC nebo NB) JU. Každá součást má jednoho či více správců počítačů.
- **Uživatel** – je zaměstnanec, student nebo účastník CŽV JU, který sdílí počítačovou síť. **Běžný uživatel** nemá administrátorská práva.

- **Virus** - v oblasti počítačové bezpečnosti označuje program, který se dokáže sám šířit bez vědomí uživatele.

2. ZKRATKY

- **AD** (Active Directory) - je implementace adresářových služeb LDAP pro PC s Windows, nástroj pro správu uživatelů, skupin, počítačů a sítí.
- **APS** (Akademické počítačové středisko) – pracoviště CIT, které zajišťuje správu, provoz a rozvoj páteřní počítačové sítě a jejích komponent + další činnosti.
- **AV SW** – antivirový software, který chrání počítačový systém proti případnému útoku, odhaluje a odstraňuje počítačové viry infiltrované do počítače. Aby splňoval svoji funkci, musí být antivirový program aktuální a musí být zajištěna pravidelná aktualizace databáze virů.
- **AVO –** antivirová ochrana počítače pomocí nainstalovaného AV SW.
- **BS –** bezpečnostní správce součásti JU (funkce popsaná v dokumentu *ISMS-002_Celková bezpečnostní politika JU)*.
- **CESNET** (Czech Education and Scientific NETwork) - sdružení CESNET, z. s. p. o. založené vysokými školami a Akademií věd České republiky v roce 1996. Jeho hlavním cílem je provozovat a rozvíjet páteřní akademickou počítačovou síť ČR. Zaměřuje se na výzkum a vývoj informačních a komunikačních technologií, budování a rozvoj e-infrastruktury určené pro výzkum a vzdělávání. Současná generace této sítě nabízí na páteřních trasách přenosové rychlosti v řádu desítek gigabitů za sekundu.
- **CIT** (Centrum informačních technologií) - celoškolské pracoviště JU, které zabezpečuje správu a rozvoj centralizovaných informačních systémů a informační infrastruktury na JU.
- **CŽV** – Celoživotní vzdělávání.
- **DHCP server (**Dynamic Host Configuration Protocol) - používá se pro automatickou konfiguraci počítačů připojených do počítačové sítě, přiděluje počítačům pomocí DHCP protokolu potřebné atributy, zejména IP adresu. Její platnost je omezená, a proto je na počítači spuštěn DHCP klient, který ji prodlužuje.
- **DNS -** (Domain Name system) - hierarchický systém doménových jmen (jmen počítačů) realizovaný servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jde o distribuovanou databázi síťových informací.
- **HS sítě –** hlavní správce páteřní počítačové sítě JU, který informuje a metodicky řídí lokální správce sítí jednotlivých součástí JU.
- **HTTP(S)** (Hyper Text Transfer Protocol Secure) - je nejpoužívanější protokol pro přenos hypertextových dokumentů ve formátu HTML. Verze HTTPS umožňuje posílat data šifrovaná a tím i lépe zabezpečená proti odposlouchávání a podvržení dat. Umí též ověřit identitu protistrany.
- **HW** (HardWare) - technické prostředky ICT.
- **ICT** (Information and Communication Technologies) – Informační a komunikační technologie - zahrnují veškeré technologie používané pro komunikaci a práci s informacemi.
- **IDM** (IDentity Management) – správa uživatelských účtů, tj. aplikace, která udržuje informace o všech uživatelích JU, jež mají přístup k některým IS a do sítě JU.
- **IP** (Internet Protocol) - je základní protokol pracující na síťové vrstvě, používaný v počítačových sítích a Internetu. Protokol IP poskytuje datagramovou službu celé rodině protokolů TCP/IP. Sám o sobě neposkytuje záruky na přenos dat a rozlišuje pomocí IP adresy pouze jednotlivá síťová rozhraní.
- **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 – obor, který zahrnuje návrh, vývoj, využívání, zavádění, podporu a řízení IS a zpracování digitálních informací. Především jde o HW a SW počítačů.
- **ITM** – IT manažer/ka, který/á zajišťuje IT služby své součásti.
- **JU** – Jihočeská univerzita v Českých Budějovicích.
- **KaM** (Koleje a menzy) – celoškolské pracoviště JU poskytující ubytování, stravování a konferenční prostory.
- **LAN** (Local Access Network) – lokální počítačová síť, v tomto dokumentu LAN součásti JU.
- **LDAP** (Lightweight Directory Access Protocol) - protokol pro ukládání a přístup k datům na adresářovém serveru. Slouží k autentizaci uživatelů.
- **LS sítě –** lokální správce sítě na každé součásti JU (fakulty, ústavy).
- **MIB –** Manažer informační bezpečnosti JU.
- **MS (**MicroSoft) - zkratka firmy Microsoft, který obvykle předchází názvu SW produktu.
- **OS** – operační systém počítače - Windows, Linux, UNIX, Mac, atd.
- **PC** (Personal Computer) – osobní počítač uživatele.

- **SIS** (Středisko informačních systémů) – pracoviště CIT -– spravuje většinu centrálních IS.
- **SLS sítě** – Studentský lokální správce sítě součásti KaM na koleji, kde je ubytován.
- **SW** (SoftWare) - programové vybavení počítače.
- **TCP/IP -** je hlavním protokolem celosvětové sítě Internet. Jde o komunikační protokol - množinu pravidel, které určují syntaxi a význam jednotlivých zpráv při komunikaci.
- **VPN** (Virtual Private Network) – virtuální privátní síť - prostředek k propojení několika počítačů prostřednictvím veřejné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě. Při navazování spojení je totožnost obou stran ověřována a po autentizaci je veškerá komunikace šifrována. Proto lze toto připojení považovat za bezpečné.
- **WiFi** (Wireless Fidelity) - standard pro bezdrátovou lokální počítačovou síť, která je určená k připojení mobilních zařízení (např. PDA, notebooky, tablety, chytré telefony apod.) k Internetu. Využívá volného frekvenčního pásma, proto je ideální pro budování levné, ale výkonné sítě bez nutnosti pokládky kabelů.
- **WWW** (World Wide Web) - ve volném překladu „Celosvětová pavučina“, je označení pro aplikace internetového protokolu http, neboli soustava propojených hypertextových dokumentů.

ODPOVĚDNOSTI A PRAVOMOCI

- **Hlavní správce sítě JU** (HS sítě)

  a) Spravuje páteřní síť JU
  b) definuje a aktualizuje obecně závaznou metodiku správy sítě na JU
  c) přiděluje rozsahy IP adres správcům lokálních sítí součástí (LS sítě) a předává jim pravomoci je spravovat
  d) nastavuje programově ovladatelné switche, které tvoří rozhraní mezi páteřní sítí JU a LAN budovy součásti JU
  e) metodicky řídí činnost LS sítě jednotlivých součástí – vydává metodické pokyny pro LS sítě
  f) kontroluje dodržování pravidel provozu a předpisů pro správu sítě JU
  g) je oprávněn monitorovat a testovat provoz sítě JU a zjistí-li bezpečnostní incident, neprodleně informuje MIB a LS sítě součásti JU, kde incident nastal
  h) spolupracuje s HS AVO, HS PC a MIB při řešení závažné infiltrace počítačů, o níž je informován nebo ji sám zjistí
  i) řídí řešení výjimečných situací na síti JU
  j) eviduje a aktualizuje aktiva ICT páteřní sítě na portálu isms.jcu.cz
  k) plánuje rozvoj a modernizaci sítě a koncových zařízení.

- **Lokální správce sítě** (LS sítě) - správce ICT součásti JU (pracovník součásti, jehož funkce se mohou kumulovat – např. BS, ITM, LS AVO či PC) pověřený správou LAN své součásti. Vykonává tyto činnosti:

  a) připojuje zařízení k síti a přiděluje IP adresy z rozsahu přiděleném HS sítě JU
  b) vede evidenci o přidělených IP adresách v DNS
  c) kontroluje dodržování předpisů pro správu sítě na své součásti
  d) rezervuje IP adresy pro dané uživatele LAN a vede vlastní podrobnější evidenci s atributy uživatele (např. místo, skupina,….)
  e) řídí se pokyny hlavního správce sítě JU či jeho zástupce
  f) v případě výskytu bezpečnostního incidentu ve své LAN informuje MIB o přijetí nápravných opatření, jež zabrání jeho opakování
  g) instaluje a konfiguruje komponenty sítě podle instrukcí výrobce a v souladu s pokyny HS sítě JU a s touto směrnicí, případně v souladu s platnou metodikou vydanou v rámci své součásti, která nesmí být v rozporu s dalšími směrnicemi ISMS JU
  h) informuje uživatele své součásti o důležitých změnách souvisejících s používáním sítě.

- **Uživatel** - zaměstnanec, student nebo účastník CŽV JU, který využívá počítačovou síť JU ke své pracovní činnosti nebo studiu a musí respektovat následující ustanovení:

a) dodržuje pravidla vyplývající z této směrnice a směrnic souvisejících, včetně interních předpisů své součásti
b) řídí se pokyny svého lokálního správce sítě nebo HS sítě
c) využívá PC připojené do sítě JU v rámci své pracovní náplně a v souladu s výzkumným a vzdělávacím posláním JU
d) je povinen dodržovat pravidla, která platí na prostředcích jiných sítí, k nimž získá přístup prostřednictvím sítě JU
e) plně zodpovídá za negativní dopady způsobené zneužitím svého uživatelského účtu, pokud je způsobil vlastním nedbalým zacházením s účtem a heslem, které musí udržovat v tajnosti
f) uživatel nesmi umožnit přístup do sítě JU prostřednictvím svého připojeného zařízení nebo programového vybaveni dalším zařízením nebo osobám.

Další odpovědnosti jsou součástí textu.

ZMĚNY OPROTI PŮVODNÍ VERZI

Toto je první verze 1.0 dokumentu.

B. POPIS

1. POČÍTAČOVÁ SÍŤ JU

Počítačová síť JU je hierarchického typu s hvězdicovou strukturou. Nejvyšší úroveň tvoří páteřní síť, na níž jsou napojeny logické sítě jednotlivých součástí JU (fakult a ústavů) propojené optickými kabely metropolitní sítě.

1.1. POSKYTOVATEL PŘIPOJENÍ

Poskytovatelem připojení JU k Internetu je sdružení CESNET, z.s.p.o. (Czech Education and Scientific NETwork), jehož hlavním cílem je provozovat a rozvíjet páteřní akademickou počítačovou síť ČR. Nabízí řadu služeb jako např. eduroam (připojení k síti v navštívené organizaci), podporu vývojového prostředí, datová úložiště, video a web konference, IP telefonii, zprostředkování certifikátů, monitorování sítě a další. Podrobnější informace o tomto sdružení lze nalézt na portálu http://www.cesnet.cz/ .

1.2. PÁTEŘNÍ SÍŤ JU

Konektivita páteřní sítě JU na výzkumnou síť CESNET je realizována routerem – centrálním prvkem sítě JU. Páteřní síť včetně všech jejích komponent je spravována hlavním správcem sítě (HS sítě). Jednotlivé univerzitní budovy, které se nacházejí i mimo hlavní areál JU, jsou propojeny v metropolitní síti převážně optickými kabely. Součástí páteřní sítě jsou i pronajaté přenosové linky třetích stran, které připojují vzdálenější budovy JU, např. Vodňany a Nové Hrady. Pro vyšší bezpečnost je síť JU chráněna centrálním firewallem – viz níže kapitola 1.4.

1.3. LOKÁLNÍ SÍTĚ SOUČÁSTÍ JU

Lokální síť fakulty či ústavu (LAN) pokrývá obvykle jednu či více budov a umožňuje připojení svých uživatelů k univerzitní síti a využívání služeb a IS JU, jakož i přístup k Internetu. Fakulty, jejichž objekty nejsou součástí metropolitní sítě, jsou připojeny pronajatými linkami od třetích stran – např. budovy FROV Vodňany, Nové Hrady. Správcem LAN je lokální správce sítě (LS sítě) – viz 2.2 níže – který přiděluje IP adresy novým uživatelům.

1.4. PRVKY ZABEZPEČENÍ SÍTĚ

Součástí zabezpečení Intranetu JU jsou firewally (FW) instalované na několika úrovních. Jde o síťová zařízení se speciálním SW sloužícím k řízení a zabezpečování provozu mezi sítí JU a Internetem, s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně řečeno – FW definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Cílem je ochrana vlastní počítačové sítě JU nebo počítače samotného, v závislosti na typu FW. Vstupní a výstupní kanály sítě nebo počítače jsou softwarem monitorovány a FW některé z nich povoluje a jiné zakazuje - dle nastavení uživatele. Nehlídaným portem může vniknout do počítače malware.

1.4.1. Centrální firewall

- Omezuje přístupy ke službám segmentů sítě JU
- diferencuje přístupy do segmentů součástí JU
- neuplatňuje se v provozu LAN součástí
- spravuje jej HS sítě.

1.4.2. Speciální firewall JU

- Slouží pro zabezpečení ekonomických agend
- odděluje segment sítě s důležitými centrálními agendami od Intranetu JU
- řídí přístup pro externí správce k jednotlivým agendám
- spravuje ho APS CIT.

1.4.3. Firewally na serverech

FW instalovaný na serveru zvyšuje bezpečnost jeho provozu omezením přístupů v závislosti na službě/službách, které poskytuje. Instalaci a konfiguraci FW zajišťuje správce serveru. Z bezpečnostních důvodů je doporučeno firewall na serverech provozovat.

1.4.4. Firewall na PC

Chrání vlastní počítač proti případnému průniku malware. Součástí OS Windows je FW, který je standardně zapnut a je nutné jej provozovat (kontrola: Ovládací panely-> Brána Windows firewall).

Na PC je možno nainstalovat i další FW, který např. volitelně nabízí většina antivirových firem jako součást AV SW. Při předání počítače zaměstnanci JU zodpovídá za nastavení FW a antivirového SW lokální správce PC součásti JU. Je-li uživatel PC privilegovaný (má administrátorská práva), přebírá tuto zodpovědnost po převzetí počítače.

1.4.5. Centrální router

Centrální router je aktivní síťové zařízení, které procesem zvaným routování (směrování) přeposílá datové pakety protokolu IP směrem k jejich cíli.
Zajišťuje připojení na výzkumnou síť CESNET a směruje pakety adresátovi co nejefektivnější cestou. Správu tohoto routeru zajišťuje HS sítě JU.

1.4.6. Další aktivní prvky sítě

V počítačové síti JU jsou zapojeny různé další aktivní komponenty, které slouží potřebám vzájemného propojování uvnitř intranetu a aktivně působí na přenášené signály. Jde např. o switche, huby, repeatery, routery a další. Všechny síťové prvky musejí být buď pod kontrolou nebo fyzicky chráněny (v závislosti na jejich důležitosti) – viz směrnice JU *„ISMS-011_Politika fyzické bezpečnosti“.*

2. PERSONÁLNÍ ZAJIŠTĚNÍ SPRÁVY SÍTĚ JU

2.1. HLAVNÍ SPRÁVCE SÍTĚ (HS sítě)

HS PC je zaměstnanec JU určený ředitelem CIT, který může metodicky řídit lokální správce sítě jednotlivých součástí JU a vydává dle potřeby doplňující metodické pokyny, které budou ukládány na portál ISMS do složky Net-MP-HS a budou k dispozici ITM, BS a dalším lokálním správcům sítě. Odpovědnosti a další pravomoci HS sítě jsou popsány v oddíle A. HS sítě JU má svého zástupce.

2.2. LOKÁLNÍ SPRÁVCE SÍTĚ (LS sítě)

LS sítě je určen IT manažerem nebo vedoucím dané součásti JU pro činnosti spojené se správou LAN v rozsahu své působnosti. Nejde o samostatnou katalogovou funkci, ale bývá obvykle kumulovaná s dalšími činnostmi v oblasti ICT. Může se jednat o BS, správce AVO či PC nebo přímo ITM. Jeho odpovědnosti a pravomoci jsou popsány v oddíle A. Měl by mít svého zástupce.

Seznam všech správců sítě JU (HS i LS) je uveden v příloze P1 této směrnice – viz "*ISMS-008-P1_Síť-Správci JU*" a bude dle potřeby aktualizován. Je také interně dostupný všem uživatelům JU po přihlášení na portálu ISMS ve složce Kontakty.

2.3. STUDENTSKÝ LOKÁLNÍ SPRÁVCE SÍTĚ (SLS SÍTĚ)

SLS je funkce zřízená pouze na součásti KaM, a to pro každou budovu s ubytovací kapacitou. Tito správci jsou jmenováni ředitelem KaM z řad studentů, ubytováni v budově, kterou spravují a mohou se vzájemně zastupovat. Jsou metodicky vedeni LS sítě KaM. Mají také právo odpojit uživatele při porušení pravidel kolejní počítačové sítě. Struktura řízení sítě KaM a povinnosti SLS jsou popsány na Kolejní počítačové sítě.

3. BEZPEČNOSTNÍ POŽADAVKY NA PROVOZ SÍTĚ JU

3.1. POKYNY PRO SPRÁVCE SÍTĚ

Není-li lokální správce sítě a LS PC konkrétní součásti JU totožný, může některé dále uvedené síťové činnosti provádět LS PC při instalaci a přípravě PC uživatele JU.

Pro bezpečný provoz své LAN by měl LS sítě zajistit na své součásti následující požadavky:

1. Sdělit uživateli pro přístup do sítě JU jeho unikátní účet s prvotním heslem jemu známé konstrukce a informovat jej, aby si heslo po prvním přihlášení změnil, není-li vynucení změny možné předem programově zajistit.
2. Nebude po uživateli vyžadovat sdělení či zadání hesla bez předchozího požadavku uživatele na technickou podporu a bez ověření jeho identity pomocí dodatečných údajů.
3. Nastavit na PC uživatele automatické aktualizace a úrovně bezpečnosti internetových prohlížečů (MSI Explorer, Mozilla Firefox, ev. Opera) a poštovního klienta (MS Outlook, Thunderbird) – dle dispozic LS sítě.

4. Předat uživateli sítě přístupové informace k jeho schránce elektronické pošty (mailboxu) a sdělit její případná omezení (velikost zprávy, rozsah odesílaných příloh – běžně obvykle 4 MB)
5. Běžný uživatel musí mít omezená uživatelská práva, která mu nastaví LS PC (např. skupina Users ve Windows 2000/XP/Vista/7/8).
6. Na PC musí být nainstalován firewall a musí být aktivní. Je doporučeno 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.). Je-li PC součástí centrální domény AD, je toto nastaveno automaticky.
7. Zařazení počítačů nebo sítí mezi důvěryhodné by mělo být co nejvíce restriktivní (důvěryhodných počítačů by mělo být co nejméně).

Tyto požadavky platí i pro počítače zaměstnanců, studentů a účastníků CŽV JU, s nimiž se připojují do univerzitní počítačové sítě.

3.2. POKYNY PRO UŽIVATELE SÍTĚ

- **Založení uživatelského účtu**
  Účet pro přístup uživatele do sítě JU a k různým informačním systémům (IS) se zakládá automaticky na základě záznamu personálního útvaru v IS personální agendy či záznamu studijního oddělení součásti JU ve studijním systému, příp. záznamem, jež provádí pověřené pracoviště součásti v IS pro evidenci studentů CŽV a je mu přiřazeno prvotní standardní heslo. Jakmile uživatel získá tyto přístupové informace, je povinen si prvotní heslo změnit na portálu https://idm.jcu.cz na své vlastní **originální heslo** (viz pojem **heslo** v oddílu **Pojmy** výše), zapamatovat si jej a nikomu jej nesdělovat (ani správci) a dále toto heslo periodicky měnit. V případě pochybností, že bylo někým odhaleno, je nutno si jej neprodleně změnit na jiné, aby nebylo možné přístupové informace zneužít.

  Žádný správce ICT JU nikdy nebude po uživateli vyžadovat sdělení či zadání hesla bez předchozího požadavku uživatele na technickou podporu a bez ověření jeho identity pomocí dodatečných údajů!

- **Zrušení uživatelského účtu**
  Po skončení zaměstnaneckého poměru nebo studia, případně jeho přerušení, dochází automaticky k zablokování uživatelského účtu a není tedy možné se dále k síti JU připojovat a využívat dříve povolené IS. Pokud uživatel s takovým účtem později obnoví zaměstnanecký poměr nebo studium, jeho účet bude odblokován a může jej začít používat s naposledy nastaveným heslem.

- **Co běžný uživatel NESMÍ**
  - Používat v síti JU nepovolené či nedostatečně zabezpečené zařízení (např. počítač nebo chytrý telefon bez nainstalovaného antivirového SW,...). V případě porušení toto pravidla, je uživatel plně zodpovědný za negativní důsledky vzniklé použitím takového nezabezpečeného zařízení.
  - Pracovat pod jiným než svým vlastním uživatelským účtem. Výjimka je povolena jen v případě hostujících lektorů bez pracovně právního vztahu k JU, a to pouze s povolením vedoucího příslušné katedry.
  - Modifikovat síťový SW tak, aby obcházel či narušoval nastavené bezpečnostní aspekty.
  - Používat počítač v síti JU bez aktivního a aktualizovaného antivirového SW a bránit mu v provádění automatických aktualizací.
  - Používat v síti zavirovaný PC.
  - V případě použití vlastního PC nesmí nastavovat na počítači fixní IP adresu (standardně musí využívat DHCP), např. připojení na kolejích.
  - Narušovat práci ostatních uživatelů sítě ani chod a výkonnost sítě jako celku nadměrným zatěžováním ICT prostředků, např. bezdůvodným přenášením velkého objemu dat, či jakýmkoli jiným způsobem.
  - Pokoušet se získat jiná přístupová práva či privilegovaný stav v počítačové síti, který mu nebyl přidělen odpovědným pracovníkem, případně získá-li je např. vinou HW či SW chyby nebo nedbalostí jiného uživatele, je povinen tuto skutečnost neprodleně oznámit lokálnímu nebo hlavnímu správci sítě a manažeru informační bezpečnosti.
  - Přistupovat nebo se pokoušet o přístup do oblastí, pro které nemá oprávnění.
  - Provádět změny konfigurací zařízení sítě a dalších prostředků připojených do sítě JU či zaměňovat jednotlivé komponenty způsobem, který by mohl negativně ovlivnit provoz počítačové sítě. Jakékoli zásahy do konfigurace je třeba předem projednat s HS sítě či LS sítě součásti JU.
  - Získávat nebo šířit nelegální SW. Na počítačích v majetku JU nesmí být nelegální SW používán!

- Provádět činnost, která by mohla ohrozit provozuschopnost sítě.
- Vystavovat na serverech materiály, jejichž obsah je v rozporu se zákony, je nemravný anebo má charakter politické, náboženské či jiné podobné agitace K šíření informací tohoto typu nesmí využívat ani e-mail či různé konference.
- Používat SW nebo HW prostředky pro monitorování činnosti jiných uživatelů nebo serverů. Testovat a monitorovat síť mohou výhradně HS a LS sítě.
- Rozesílat nevyžádanou poštu – tzv. SPAM.
- Šířit poplašné zprávy – tzv. hoax.
- Využívat síť JU ke komerčním účelům.
- Stahovat neznámé soubory z Internetu (zejména s příponou ".EXE"), které mohou být zdrojem malware.
- Otevírat e-mailové zprávy od neznámých adresátů nebo zprávy s podezřelým obsahem, obzvláště nespouštět přílohy těchto zpráv, ale takový e-mail smazat.
- Reagovat na e-mail, který by požadoval sdělení hesel, PINů či osobních údajů.

- **Doporučení**
  - Zkontrolujte, že máte na PC, z něhož přistupujete do Internetu, aktivní firewall, který minimalizuje rizika neoprávněného přístupu k Vašemu PC.
  - Mějte na paměti, že běžná zpráva elektronické pošty je v podstatě otevřená listovní zásilka.
  - Dbejte na zadání správných adres příjemců, aby z tohoto důvodu nedocházelo zbytečně k chybovým zprávám.
  - Uvědomte si, že Vaše činnost na síti není anonymní a že lze dohledat původce nelegální činnosti.
  - Buďte extrémně opatrní a zvažujte, kam zadáváte své přihlašovací údaje, aby nedošlo k jejich zneužití.

4. ZPŮSOBY PŘIPOJENÍ DO SÍTĚ JU

4.1. PEVNÉ PŘIPOJENÍ

PC uživatele-zaměstnance je v budovách JU připojováno do interní sítě JU strukturovanou kabeláží s přidělenou IP adresou v rozsahu segmentu sítě. Tímto způsobem se připojují i další síťová zařízení jako např. tiskárna, scanner apod. Je-li zařízení ze zásuvky odpojeno, doporučuje se, aby LS sítě odpojil zásuvku z aktivního prvku sítě.

4.2. BEZDRÁTOVÉ PŘIPOJENÍ (WIFI)

Bezdrátová síť JU má přístupové body v různých lokalitách a studenti, zaměstnanci i účastníci CŽV JU ji mohou využívat z přenosných počítačů, PDA či mobilních telefonů. Podmínkou přístupu je předchozí vytvoření nového uživatelského účtu FreeRadius ve tvaru ***username@jcu.cz***, kde *username* je název přiděleného univerzitního uživatelského účtu. Vlastní účet (jméno a heslo) může uživatel získat nastavením FreeRadius hesla v informačním systému **IDM** volbou „Změna hesla FreeRadius", podle návodu na wifi.jcu.cz.

4.2.1. EDUROAM

Eduroam je akademická celoevropská konfederace poskytující bezdrátovou síťovou konektivitu pro uživatele z připojených institucí. Přístup uživatelů je založen na zabezpečené autentizaci v domácí instituci.

JU je součástí České eduroam, jejímž správcem je sdružení CESNET, z. s. p. o. Uživatelé JU přistupují do Eduroam pomocí svého FreeRadius účtu a hesla – viz 4.2. Další informace jsou na www.eduroam.cz a eduroam.jcu.cz.

4.3. VPN

Vzdálený přístup k některým službám, informačním systémům či aplikacím JU (např. knihovní databáze), u nichž je podmínkou přistupovat z IP adresy JU, vyžaduje připojení přes VPN (Virtual Private Network) koncentrátor. Jde o bezpečné šifrované spojení, po jehož navázání uživatel získá vnitřní IP adresu JU. Vzdálený počítač je třeba nakonfigurovat podle návodu na http://vpn.jcu.cz/, kde jsou příklady podle typů operačního systému Windows.

Předpoklady použití připojení přes VPN koncentrátor:

- mít vytvořený uživatelský účet FreeRadius obdobně jako u předchozích dvou způsobů připojení, tj. Wi-Fi nebo Eduroam – viz 4.2. a 4.3. výše
- vzdálený počítač mít připojen k Internetu
- při konfiguraci síťového připojení na PC uvést adresu VPN koncentrátoru „vpn-access.jcu.cz" a nastavit firewall tak, aby propouštěl port 1723/TCP a také IP protokol GRE (47), který je službou VPN využíván.

4.4. KOLEJE

Studenti a zaměstnanci ubytovaní na kolejích JU mohou využívat - za splnění určitých podmínek popsaných na http://kam.jcu.cz/ - pevné připojení do sítě JU z kolejí K1-K5 a hostelu Bobík ze svého vlastního počítače s nastaveným automatickým přidělování IP adres přes DHCP. Předpokladem je předchozí vyplnění a schválení žádosti a zaplacení měsíčního poplatku. Studenti musejí při své práci dodržovat mimo jiné také pravidla popsaná v dokumentu Organizace správy a zásady pro užívání studentské kolejní počítačové sítě. Poruší-li bezpečnostní opatření a dopouštějí-li se bezpečnostních incidentů (např. nelegální stahování filmů či jiné zakázané aktivity), správce KaM v součinnosti s HS sítě JU má právo je po předchozím varování odpojit od sítě JU.

Na každé koleji existuje ještě studentský LS sítě (SLS), který spravuje síť v budově, v níž je ubytován. Vyřizuje žádosti studentů a zajišťuje jejich fyzické připojení – více viz odst. 2.3.

Studentská počítačová síť je provozována odděleně od lokální počítačové sítě KaM a odpovědnost za její připojení k páteřní síti JU má pracoviště APS CIT. Nastavení centrálního firewallu je pro koleje striktnější než pro ostatní součásti.

5. VYUŽITÍ SLUŽEB SÍTĚ JU

Nejběžnější způsoby využití počítačové sítě JU jsou elektronická pošta, webové portály, přístupy k informačním systémům JU, časová synchronizace počítačů a IP telefonie.

Každá služba má svého správce, který je zodpovědný za její provoz.

5.1. ELEKTRONICKÁ POŠTA (E-MAIL)

Veškerá elektronická pošta JU prochází antispamovým a antivirovým filtrem. Odhalené nevyžádané zprávy jsou předem odfiltrovány a uživatelé JU dostávají prostřednictvím jednotlivých LAN většinou jen zprávy, které jim náležejí. Další filtraci poštovních zpráv si mohou uživatelé JU nastavit sami nebo za pomoci LS PC na svých počítačích v e-mail klientech (MS Outlook, Thunderbird, atd.).

5.1.1. INDIVIDUÁLNÍ E-MAIL

Každý uživatel JU má přidělen univerzitní účet elektronické pošty shodný s názvem jeho prvotního účtu (viz 3.2. Založení uživatelského účtu), doplněný o doménu, a to obvykle ve tvaru ***username@součást.jcu.cz*** , kde ***username*** je název jeho uživatelského účtu a ***součást*** je zkratka fakulty (např. ef, prf, pf,...). Někteří uživatelé mohou mít tento účet bez zkratky ***součást***i, tedy jen s doménou *jcu.cz*.

Mimoto si může uživatel nastavit vlastní soukromou e-mail adresu. Pokud si tuto sekundární adresu uživatel nastaví, musí uvést správnou aktivní adresu a v případě její neplatnosti provést změnu též na JU v IDM:

K provozování e-mailu mohou mít jednotlivé součásti své vlastní doplňující předpisy, které nesmí být v rozporu s touto směrnicí.

5.1.2. HROMADNÝ E-MAIL

Tato služba je realizována vesměs prostřednictvím distribučních serverů v Office 365, které jsou pro základní skupiny uživatelů generovány automaticky. Fakulty mohou mít navíc své lokální hromadné adresy. Tyto maily jsou určeny jen vybraným pracovníkům, které jmenuje děkan nebo ředitel součásti JU (tzv. E-poštmistrům a Zadavatelům). Lze ji využít pro zaslání zprávy od Zadavatele vybrané cílové skupině adresátů JU, a to jak zaměstnancům, tak i studentům a účastníkům CŽV. Ve všech kategoriích lze volit podle potřeby různé množiny adresátů, např.:

- všichni zaměstnanci/studenti/účastníci CŽV
- zaměstnanci zvolené fakulty/ústavu/katedry nebo studenti fakulty
- zaměstnanci podle funkcí či útvarů (vedoucí pracovníci, technici, specialisté, atd.)
- studenti podle formy (prezenční, distanční, kombi) a typu studia (Bc, Mgr., doktorské apod.)
- a další různé kombinace.

Vlastní odeslání hromadného e-mailu zajišťuje E-poštmistr té součásti JU, která chce tuto službu využít.

Mailové adresy jsou čerpány z IDM (jednotná správa uživatelů na JU). Podrobnější popis je uveden na webu ISMS ve složce Postupy.

5.2. WWW PORTÁLY

Každý webový portál JU musí mít svého správce, jehož jméno a kontakt na něj musí být na portálu uveden.

Oprávnění uživatelů pro přístup k portálu nebo k jeho jednotlivým složkám a uživatelské role přiděluje správce portálu (tzv. webmaster), případně jimi pověřené a proškolené osoby. Autentizace probíhá u většiny webů přes LDAP, výjimečně jinou technologií. V případě lokálních účtů vytváří uživatelské jméno a heslo správce portálu.

Přihlášení k webovým portálům by mělo probíhat pomocí zabezpečeného spojení protokolem HTTPS. Vygenerování, instalaci a aktualizaci certifikátů pro webový portál provádí jeho správce.

5.3. PŘÍSTUPY K INFORMAČNÍM SYSTÉMŮM A APLIKACÍM

Informační systémy (IS) JU lze využívat jednak prostřednictvím Intranetu – tedy z vnitřní sítě JU, ale také z vnějšího prostředí za předpokladu, že má uživatel k požadovanému IS přístup (vlastní účet a heslo).

Přístup oprávněných uživatelů z externích sítí je možný pouze pomocí programu se šifrovaným přenosem svých autentizačních údajů a dat (např. přes VPN koncentrátor, SSH, HTTPS). Uživatel je povinen zajistit, aby jeho heslo nebylo přenášeno z vnější sítě v otevřené (nešifrované) formě. K některým IS JU není vzdálený přístup bez VPN koncentrátoru (viz 4.3) možný.

Výjimkou je IDM, k němuž lze přistupovat pouze z vnitřní sítě JU, nikoli vzdáleně.

5.4. IP TELEFONIE

Službu IP telefonie mohou využívat jen vybraní zaměstnanci JU. Není určena pro studenty či účastníky CŽV JU. Její správu zajišťují pracoviště SIS a APS CIT JU.

5.5. ČASOVÁ SYNCHRONIZACE POMOCÍ NTP

Všechny prvky sítě JU jsou synchronizovány pomocí NTP serverů, které nám poskytuje sdružení CESNET. Z nich jsou dále synchronizovány servery a počítače zaměstnanců JU. Pro časovou synchronizaci je doporučeno použít server virgo.jcu.cz.

6. MONITOROVÁNÍ SÍTĚ

Provoz aktivit ve vnitřní síti JU je pravidelně monitorován správci sítě, kteří kontrolují její funkčnost. Testování a monitorování páteřní sítě JU je pouze v kompetenci HS sítě. Ten v případě potřeby provádí změny či zásahy a upozorňuje LS sítě a MIB na případné bezpečnostní incidenty.

Každý, kdo používá počítačové prostředky v síti JU, vyjadřuje souhlas s takovým monitorováním. Pokud monitorování odhalí nepovolenou aktivitu, může být záznam poskytnut jako podklad pro vyšetřování, disciplinární nebo trestní řízení. Jinak jsou záznamy získané monitorováním důvěrné.

C. ZÁVĚREČNÁ USTANOVENÍ

Kontrolou dodržování této směrnice je pověřen ředitel CIT a ISMS, vedoucí součástí JU nebo jimi pověřené osoby, IT manažeři a správci sítě JU. 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-008-P1	Síť-Správci JU
ISMS-008-P2	Seznam E-poštmistrů JU

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-007	Správa a bezpečnost provozu počítačů JU
ISMS-009	Elektronický podpis a certifikáty
R95_2007	Užívání PC, SW, NET (Opatření rektora)

* indikace uvedených dokumentů JU jsou platné v době vydání této směrnice, později mohou být změněny.