Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-002**
Název dokumentu:	**Celková bezpečnostní politika JU**
Typ dokumentu:	Interní dokument - typ B – politika
Určeno pro:	Všechny zaměstnance, studenty a účastníky CŽV JU
Prvek normy ISO:	27001
Datum vydání:	14.4.2009
Datum účinnosti:	14.4.2009
Platnost do:	odvolání
Počet stran + příloh:	19 + 1
Verze:	7.0 - aktualizace 5/2018
Účel:	Souhrn základních bezpečnostních požadavků na řešení informační bezpečnosti na úrovni fyzické, personální, administrativní, počítačové a komunikační i bezpečnosti vývojového prostředí za účelem ochrany hmotných a nehmotných aktiv JU.
Uložení:	Portál ISMS - https://isms.jcu.cz/
Ruší dokumenty:	verzi 6.0
Zpracovatel:	Doc. Milan Berka – Netprosys, s.r.o., Ing. Jana Kolářová – manažerka informační bezpečnosti JU - APS CIT
Přezkoumal:	IT manažeři všech součástí JU
Schválil:	Vedení JU

OBSAH

A. ÚVODNÍ USTANOVENÍ

CÍL PROCESU A ÚČEL

Celková bezpečnostní politika (CBP) se zabývá ochranou hmotných a nehmotných aktiv Jihočeské univerzity s důrazem na aktiva ICT. Je základním dokumentem pro oblast informační bezpečnosti na JU.

Tato směrnice je závazná pro všechny zaměstnance, studenty a účastníky CŽV JU, jakož v definované míře i pro pracovníky třetích stran, kteří přicházejí do styku s informacemi a jinými aktivy JU. Ti by měli být poučeni o těch zásadách, které se jejich činnosti na JU týkají.

POJMY, DEFINICE A ZKRATKY

1. POJMY A DEFINICE

- **Aktiva JU** – cokoli, co má pro JU nějakou hodnotu.
- **Analýza rizik (AR)** – proces identifikování bezpečnostních rizik stanovující jejich závažnost a identifikující oblasti, které vyžadují ochranná opatření.
- **Bezpečnostní incident** – jedna nebo více nežádoucích a neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činnosti JU a ohrožení bezpečnosti informací.
- **Bezpečnost informací** – všechny aspekty související s definováním, dosažením a udržováním důvěrnosti, integrity, dostupnosti, individuální zodpovědnosti, autenticity a spolehlivosti informací.
- **Bezpečnostní protiopatření** – postup nebo mechanismus, který snižuje riziko.
- **Expirace** - vypršení lhůty platnosti, rezervace, záruky, v ICT např. lhůty platnosti hesla, účtu, ochrany dat apod.
- **Hrozba** – potenciální příčina nežádoucího incidentu, který může mít za následek poškození systému nebo organizace.
- **Informační aktiva JU** – SW, HW, interní informační systémy a jejich data, správci a služby IT
- **Legální SW** – SW, při jehož použití nejsou porušena žádná autorská práva (obvykle s řádnou licencí nebo např. Free SW se zdrojovým kódem, případně Freeware).
- **Management rizik** – celkový proces identifikování, kontrolování a eliminování nebo minimalizování nepředvídaných událostí, které mohou ohrozit aktiva.
- **Mimořádná situace** – stav, kdy bezprostředně hrozí, že dojde k neoprávněnému nakládání s aktivy JU nebo neoprávněnému přístupu do zabezpečené oblasti.
- **Nepovolaná osoba** – fyzická osoba, která není určena pro vstup do zabezpečených oblastí.
- **Objekt** – budova, ve které se nacházejí zabezpečené oblasti.
- **Oprávněná osoba** – fyzická osoba, která je oprávněna přistupovat do zabezpečených oblastí z pověření vedení JU.
- **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.
- **Provozní postupy** – dokument ***ISMS-003_Provozní postupy*** blíže specifikující pravidla bezpečnosti v určitých oblastech IT na JU.
- **Portál ISMS** – https://isms.jcu.cz = portál JU, kde jsou uloženy dokumenty a informace související se Systémem řízení informační bezpečnosti na JU.
- **Riziko** – potenciální možnost, že daná hrozba využije zranitelnosti aktiv nebo skupiny aktiv a způsobí tak jejich ztrátu nebo zničení.
- **Schválené programové vybavení** – SW, jehož nákup byl schválen vedoucím součásti nebo pracovníkem pověřeným touto činností.
- **Spolehlivost** – vlastnost zajišťující konzistentní zamýšlené chování a jeho výsledky.
- **Systém kontroly vstupu** – systém obsahující konstrukční a organizační opatření včetně těch, která se týkají zařízení pro řízení vstupů.
- **Zabezpečená oblast** – stavebně ohraničený prostor uvnitř objektu, kde se zpracovávají nebo ukládají aktiva JU.
- **Zbytkové riziko** – riziko, které zůstává po implementaci ochranných opatření.
- **Zranitelnost** – zahrnuje slabé místo aktiva nebo skupiny aktiv, které může být využito hrozbou.

2. ZKRATKY

- **APS** – Akademické počítačové středisko – oddělení pracoviště CIT.
- **APV** – Aplikační programové vybavení.
- **AR** – Analýza rizik.

- **AVO** – Antivirová ochrana.
- **BI** – viz pojem **Bezpečnostní incident** výše.
- **BS –** Bezpečnostní správce IT součásti.
- **CBP –** Celková bezpečnostní politika JU.
- **CIT –** Centrum informačních technologií – celoškolské pracoviště JU.
- **CŽV –** celoživotní vzdělávání.
- **DB** – Databáze = systém pro ukládání dat a jejich následné zpracování.
- **FB –** Fórum bezpečnosti IT JU.
- **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 určité kategorie činností IT na JU (AVO, PC, sítě).
- **HW** (HardWare) = technické prostředky ICT.
- **IB –** Informační bezpečnost.
- **ICT** (Information and Communication Technologies) – Informační a komunikační technologie - zahrnují veškeré technologie používané pro komunikaci a práci s informacemi.
- **IDM** (IDentity Management) - udržuje informace o všech osobách, které mají přístup do sítě JU.
- **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 součásti JU.
- **LS –** Lokální správce určité kategorie činností IT na součásti JU (AVO, PC, síť).
- **MIB –** Manažer informační bezpečnosti JU.
- **NTP** (Network Time protokol) - protokol používaný na serverech pro synchronizaci času na počítačích připojených k síti.
- **OS** – Operační systém neboli základní programové vybavení počítače.
- **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.
- **SSH a SSL** – protokoly pro zabezpečení komunikace mezi počítačem a serverem formou šifrování dat.
- **SW** (SoftWare) - programové vybavení počítače.
- **VPN** (Virtual Private Network) – virtuální privátní síť.

ODPOVĚDNOSTI A PRAVOMOCI

Všichni zaměstnanci, studenti a účastníci CŽV jsou povinni dodržovat cíle a zásady definované v tomto dokumentu, řídit se jimi podle své role a dodržovat konkrétní opatření a postupy vycházející z cílů a zásad CBP v souladu s dalšími předpisy a opatřeními JU publikovanými vedením JU např. formou Rozhodnutí či Opatření rektora JU, ředitele CIT nebo dalších vedoucích pracovníků. Všechna ujednání zavedená tímto a navazujícími dokumenty jsou přiměřeně závazná též pro zaměstnance třetích stran, kteří se nějakým způsobem podílejí na provozu JU.

Další pravomoci a odpovědnosti jsou součástí dokumentu.

ZMĚNY OPROTI PŘEDCHÁZEJÍCÍM VERZÍM

Toto je pátá verze 5.0 dokumentu ISMS „Celková bezpečnostní politika JU“.

Změny oproti verzi 1.0, 2.0, 3.0, 4.0, 5.0 i 6.0
- nové organizační schéma dle právě aktuálního stavu
- doplnění funkcí správců AVO, PC a sítě dle právě aktuálního stavu
- doplněna nová kategorie, kromě studentů a zaměstnanců - účastník CŽV
- doplnění souvisejících dokumentů
- nová organizační struktura JU (Opatření rektora R375/2018)
- doplněny informace o platnosti nařízení EU 2016/679 (GDPR)

B. POPIS

1. CHARAKTERISTIKY CBP

1.1. CÍLE A ROZSAH BEZPEČNOSTNÍ POLITIKY

CBP se zabývá ochranou všech hmotných a nehmotných aktiv JU. Součástí CBP je tedy i bezpečnost informací a nakládání s nimi. V tomto smyslu je CBP vyjádřením **Politiky informační bezpečnosti**, což je v souladu s normou ČSN ISO/IEC 27001.

CBP stanovuje:

- globální bezpečnostní cíle ve vztahu k aktivům JU
- základní bezpečnostní principy přístupu k aktivům
- popis struktury a funkci bezpečnostního managementu JU.

CBP vyjadřuje stanovisko vedení JU reprezentované jejím rektorem a akademickým senátem v oblasti zajištění bezpečnosti a maximální ochrany fyzických, personálních a jiných aktiv, včetně interních informačních systémů s veškerými informačními aktivy.

Vedení JU chápe bezpečnost jako zcela prioritní a stanovuje mezi jednotlivými částmi systému rozdíl v tom, co je či není potřeba chránit. Obecně platí, že veškerá aktiva je třeba chránit na maximální úrovni s vynaložením odpovídajících časových a finančních prostředků.

1.2. ŘÍZENÍ DOKUMENTU CBP A NÁVAZNÉ DOKUMENTACE

Tento dokument musí být vždy schválen Fórem bezpečnosti JU, dán na vědomí zaměstnancům a studentům umístěním na interní server – viz Portál ISMS - a upozorněním na jeho vyvěšení či změnu.

Dokumenty navazující na CBP schvaluje ředitel CIT.

CBP se aktualizuje minimálně 1x za dva roky nebo dle okamžité potřeby v případě změny bezpečnostních rizik či jiných pravidel. Každý dokument je identifikován titulním listem, který obsahuje evidenční číslo a název dokumentu, jeho platnost, komu je určen, jméno autora a další údaje. Forma i obsah dokumentů se řídí směrnicí ***ISMS-004_Řízení dokumentace ISMS***.

Aktuální dokumenty jsou dostupné na portálu ISMS. Tištěné dokumenty jsou platné obecně pouze v okamžiku jejich vytištění.

1.3. VŠEOBECNÝ PRINCIP

Základním bezpečnostním principem je, že každý zaměstnanec univerzity má přístup jenom k těm prostředkům a aktivům, které nezbytně potřebuje pro výkon své práce a k žádným jiným. Každý zaměstnanec, podle své role a oprávnění, může modifikovat a vkládat do systémů jen ty informace, za které následně nese osobní odpovědnost.

1.4. ZÁVAZEK VEDENÍ

Vedení JU si je vědomo potřeby řešit bezpečnost informací v rámci své organizace a v této souvislosti vyčlenilo zdroje, vytvořilo organizační strukturu řízení informační bezpečnosti a stanovilo základní pravidla pro tuto činnost.

1.5. OBSAH ČINNOSTI JU

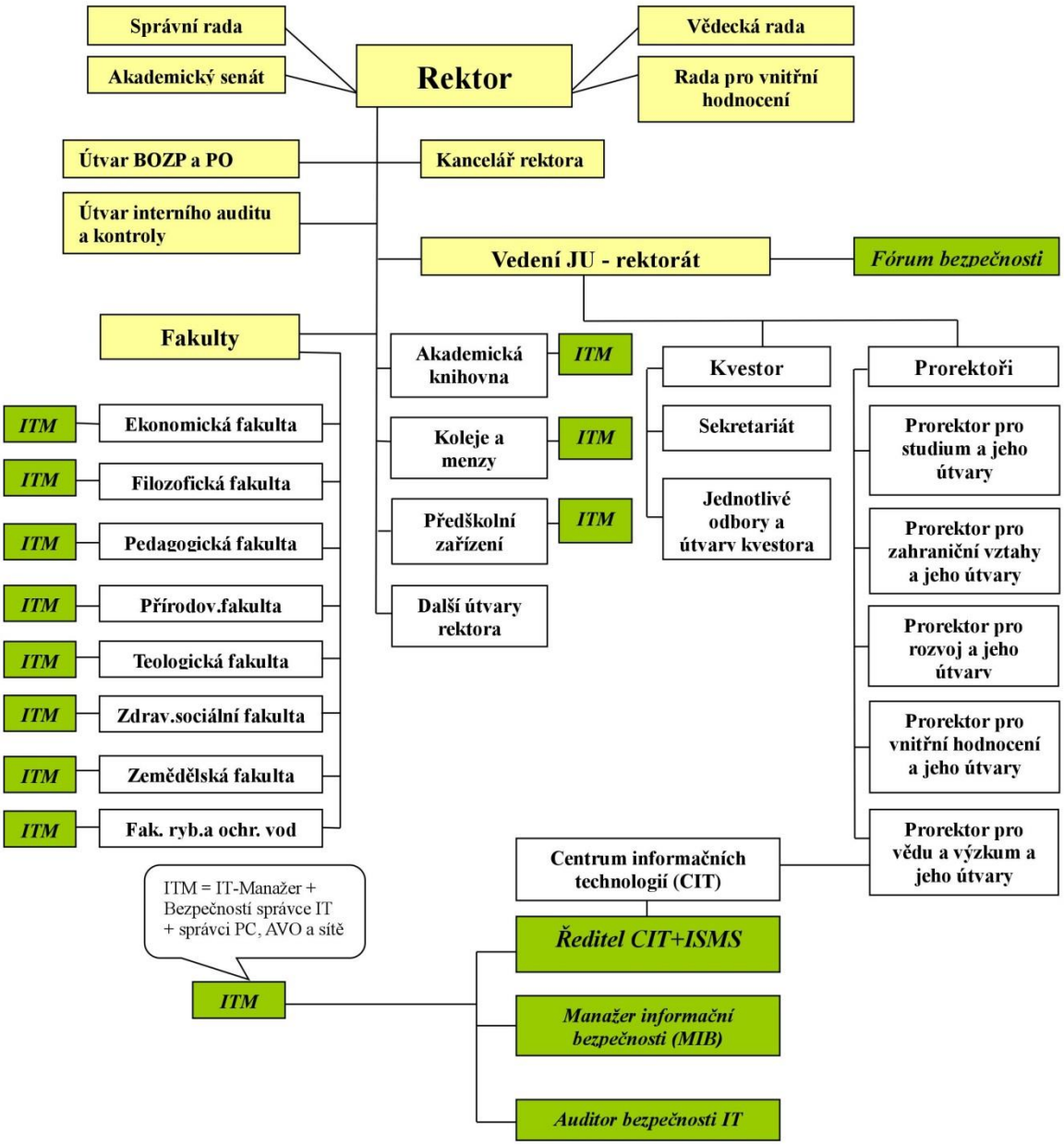
JU je vysokou školou podle vysokoškolského zákona. Uskutečňuje akreditované studijní programy a programy celoživotního vzdělávání. Typ vysokoškolské vzdělávací činnosti je určen typem uskutečňovaných akreditovaných studijních programů. Typy studijních programů jsou bakalářský, magisterský a doktorský. JU je právnickou osobou.

2. ORGANIZAČNÍ STRUKTURA A ŘÍZENÍ BEZPEČNOSTI

Následující organizační schéma JU zobrazuje útvary vedení a jednotlivé součásti se zvýrazněnými subjekty informační bezpečnosti, které jsou odlišeny kurzívou a podbarveny zeleně.

Organizační schéma Jihočeské univerzity v Českých Budějovicích

s ohledem na subjekty informační bezpečnosti



2.1. FÓRUM BEZPEČNOSTI

Fórum bezpečnosti ICT je nejvyšším orgánem, který rozhoduje o otázkách informační bezpečnosti na půdě JU. Výsledkem jeho práce je vždy návrh, zavedení nebo zlepšení bezpečnostních opatření, která se předkládají rektorovi JU nebo jeho zástupci. Ten buď návrh přijme, zamítne nebo vrátí zpět Fóru bezpečnosti k přepracování, přičemž musí vždy uvést důvody svého rozhodnutí. Na základě schválené politiky ISMS získává CIT oprávnění a povinnost řídit veškeré činnosti, které s informační bezpečností souvisejí.

Závěry a dokončení implementačních kroků ISMS, stejně tak i závažné problémy, předkládá ředitel CIT nebo manažer informační bezpečnosti Fóru bezpečnosti.

FB zasedá minimálně 1x za rok či podle potřeby. Vedením zasedání je pověřen prorektor – zástupce vedení JU. Fóru bezpečnosti jsou předkládány návrhy na zlepšení bezpečnostních opatření, návrhy aktualizací bezpečnostních politik a další náměty jednotlivých členů.
Veškeré projednávané otázky na zasedání FB jsou následně archivovány formou zápisu. Závažná rozhodnutí FB jsou buď prezentována na portále ISMS nebo sdělena příslušným pracovníkům e-mailem, včetně stanovených termínů a odpovědností.

Role Fóra bezpečnosti:

- schvaluje a podporuje implementaci systému řízení bezpečnosti
- přezkoumává a zdokonaluje bezpečnostní politiky a veškeré odpovědnosti
- sleduje významné změny informačních aktiv
- vyhodnocuje zprávy o závažných bezpečnostních incidentech, které předkládá ředitel CIT nebo manažer informační bezpečnosti JU
- zajišťuje soulad s informační bezpečnostní politikou
- schvaluje hodnocení bezpečnostních rizik a bezpečnostní klasifikace
- stanovuje hranice řízení bezpečnosti
- propaguje význam bezpečnosti informací na univerzitě.

Členy FB jsou:

- prorektor - zástupce vedení JU
- ředitel CIT a ISMS JU
- manažer informační bezpečnosti
- event. další zástupci součástí JU určení ředitelem CIT.

2.2. ŘEDITEL CIT A ISMS

Úloha ředitele CIT spočívá v následujících činnostech:

- koordinuje zavádění ISMS
- dohlíží na dodržování Celkové bezpečnostní politiky, navazujících předpisů a bezpečnostních politik
- vybírá dodavatele bezpečnostních řešení dle kritérií a komunikace s nimi
- doporučuje bezpečnostní opatření Fóru bezpečnosti
- ve spolupráci s Fórem bezpečnosti řeší důsledky závažných bezpečnostních incidentů
- zodpovídá za administrativní, personální, technickou a objektovou bezpečnost
- schvaluje dokumentaci ISMS.

2.3. MANAŽER INFORMAČNÍ BEZPEČNOSTI (MIB)

Zajišťuje tyto činnosti:

- připravuje a předkládá ke schválení návrhy pro tvorbu dokumentů ISMS a podklady pro analýzu rizik
- vyjadřuje se k bezpečnostním politikám v různých oblastech ICT, které jsou systémově podřízeny CBP a k opatřením v oblastech správy a vývoje IS
- řídí dokumentaci ISMS a její prezentaci na portále ISMS
- kontroluje realizaci bezpečnostních politik a navrhuje opatření vedoucí k nápravě
- eviduje a navrhuje řešení bezpečnostních incidentů v oblasti ICT
- řídí kontrolní činnost ISMS
- navrhuje plány školení bezpečnosti ICT, bezpečnostních auditů, testů a dává podněty k tvorbě havarijních plánů IS
- řídí audity ISMS pro přípravu na eventuelní certifikaci bezpečnosti.

2.4. IT MANAŽEŘI JEDNOTLIVÝCH SOUČÁSTÍ JU (ITM)

Spolupracují na realizaci pravidel informační bezpečnostní politiky své součásti následujícím způsobem:

- vyjadřují se k obecně platným bezpečnostním politikám a dokumentům ISMS, které jim předkládá ředitel ISMS nebo MIB
- komunikují s MIB při zavádění bezpečnostních pracovních postupů
- odpovídají za implementaci a realizaci bezpečnostních postupů a pravidel
- zodpovídají za administrativní, personální, technickou a objektovou bezpečnost
- kontrolují dodržování pokynů z jednotlivých směrnic ISMS
- zodpovídají za evidenci informačních aktiv
- zřídí funkci ***Bezpečnostní správce IT*** *(BS)*, jíž mohou pověřit jiného zaměstnance svého útvaru (např. správce serveru či sítě) zajišťováním informační bezpečnosti. BS pak spolupracuje s MIB a realizuje bezpečnostní pokyny ISMS uvnitř své součásti.

2.5. BEZPEČNOSTNÍ SPRÁVCE IT SOUČÁSTI JU (BS)

Tato funkce se zřizuje na každé součásti JU a zastává ji buď IT manažer dané součásti, a nebo pověří jejím vykonáváním jiného zaměstnance svého útvaru, nejčastěji správce sítě, serveru či jiné ICT. BS plní uvnitř své součásti tyto úkoly:

- implementuje bezpečnostní postupy a pravidla v souladu s dokumentací ISMS, případně v souladu s dříve vydanými platnými Opatřeními vedoucích pracovníků JU (rektora, ředitele CIT apod.), které dosud dokumentace ISMS neřeší
- vede evidenci informačních aktiv
- komunikuje s MIB při tvorbě a zavádění bezpečnostních pracovních postupů
- kontroluje dodržování pokynů z jednotlivých směrnic ISMS.

Po zřízení funkce BS nebo změně osoby, která tuto funkci zastává, informují IT manažeři MIB, kdo jmenovitě z jejich součásti je funkcí BS pověřen, a to včetně kontaktních údajů (telefon,e-mail,kancelář-adresa, číslo).

2.6. INTERNÍ AUDITOR INFORMAČNÍ BEZPEČNOSTI

Měl by být nezávislý na všech ostatních pracovnících bezpečnostního managementu mimo ředitele CIT, kterému je podřízen.
Jeho náplní práce je:

- kontrola dodržování bezpečnostních politik a směrnic ISMS podle vlastního uvážení nebo pokynů MIB
- předkládání podnětů k revizi CBP a systémových bezpečnostních politik IS
- kontrola způsobů řešení bezpečnostních incidentů
- zajišťování bezpečnostních a penetračních testů a jejich kontrola
- úschova protokolů o prováděných kontrolách a testech.

2.7. HLAVNÍ SPRÁVCI (HS)

Jsou zaměstnanci JU určení ředitelem CIT, kteří mají pravomoci metodicky řídit lokální správce (LS) jednotlivých součástí a vydávají pro ně dle potřeby doplňující metodické pokyny. Ty ukládají na portál ISMS do složky „*MP HS*“ a informují o nich LS e-mailem. Na JU existují tito HS:

- **HS AVO** – správa antivirové ochrany
- **HS PC** – správa osobních počítačů
- **HS NET** – správa univerzitní sítě.

Jejich odpovědnosti a pravomoci jsou popsány ve směrnicích podle jejich působnosti:

- ***ISMS-006_Antivirová ochrana počítačů JU***
- ***ISMS-007_Správa a bezpečnost provozu počítačů JU***
- ***ISMS-008_Správa a bezpečnost počítačové sítě JU.***

Nemusí se jednat o samostatnou pracovní pozici, ale funkce může být spojená se správou počítačů na CIT. Hlavní správci musí mít svého zástupce.

2.8. LOKÁLNÍ SPRÁVCI (LS)

Jsou zaměstnanci součástí JU, určení IT manažerem nebo vedoucím dané součásti, pro činnosti spojené s oblastí jejich působnosti. Nejde o samostatnou katalogovou funkci, ale bývá obvykle kumulovaná s dalšími činnostmi v oblasti ICT. Může se jednat o BS, správce PC či sítě nebo samotného ITM.

Na jednotlivých součástech JU jsou tito LS:
- **LS AVO** – správce antivirové ochrany součásti JU
- **LS PC** – správce osobních počítačů součásti JU
- **LS NET** – správce počítačové sítě součásti JU.

Odpovědnosti a pravomoci LS jsou popsány ve stejných směrnicích jako HS podle jejich působnosti – viz předchozí kapitola 2.7. Lokální správce by měl mít svého zástupce.

Jména a kontakty hlavních i lokálních správců jsou uloženy na portálu ISMS ve složce Kontakty.

2.9. VŠICHNI ZAMĚSTNANCI, STUDENTI A ÚČASTNÍCI CŽV
Aktivně se seznamují s bezpečnostní politikou JU a směrnicemi ISMS a účastní se případných přednášek či školení bezpečnosti ICT. Hlásí všechna narušení bezpečnosti a zásad bezpečnostní politiky, na která narazí při své práci manažeru informační bezpečnosti nebo řediteli CIT a svému LS. Bezpečnostní incident oznámí zaměstnanci také svému přímému nadřízenému.

2.10. DODAVATELÉ BEZPEČNOSTNÍCH ŘEŠENÍ
Dodavatelem bezpečnostních řešení je třetí strana, která na základě smluvního vztahu s organizací zajišťuje dodávky bezpečnostních projektů a prostředků dle požadavků CIT nebo Fóra bezpečnosti IT JU.

Dodavatel bezpečnostních řešení:
- odpovídá za poradenství poskytované CIT nebo Fóru bezpečnosti tak, aby veškeré jím doporučené strategie, konkrétní bezpečnostní opatření a cíle byly dostatečné k naplnění Celkové bezpečnostní politiky, odpovídaly obecným požadavkům na bezpečnost v dané oblasti, zabránily bezpečnostním incidentům a krizovým situacím a rovněž byly efektivní
- odpovídá za dodávku bezpečnostních prostředků a implementaci bezpečnostních projektů ve sjednaný čas a kvalitě
- ručí za trvalé zachování mlčenlivosti všech svých pracovníků i po ukončení smluvního vztahu s JU.

2.11. KOORDINACE BEZPEČNOSTI INFORMACÍ
Odpovědnosti za bezpečnost informací a řízení ISMS byly vyjmenovány výše. Celkově za ISMS odpovídá **Fórum bezpečnosti**, jako nejvyšší bezpečnostní orgán ICT na JU.

2.12. SCHVALOVÁNÍ PROSTŘEDKŮ NA BEZPEČNOST INFORMACÍ
Prostředky na bezpečnost informací schvaluje ve své kompetenci **ředitel CIT** a **kvestorka JU**. Děje se tak na návrh odpovědných orgánů a osob vyjmenovaných výše.

2.13. DOHODY O OCHRANĚ DŮVĚRNÝCH INFORMACÍ
Dohody obsahující požadavky na ochranu důvěrnosti nebo povinnosti zachovávat mlčenlivost se přezkoumávají jednou ročně. Přezkoumává je auditor nebo manažer informační bezpečnosti spolu s právním útvarem. Doložka o ochraně informací týkající se dodržování Nařízení EU 2016/679 (GDPR), dále Opatření rektora R378/2018 a R379/2018 a zákona č. 101/2000 Sb. O ochraně osobních údajů je součástí uzavíraných pracovních smluv a zaměstnanec má k dispozici její kopii.

2.14. BEZPEČNOSTNÍ POŽADAVKY V DOHODÁCH SE TŘETÍ STRANOU
Dohody uzavřené se třetí stranou, která přistupuje, zpracovává nebo šíří informace či spravuje prostředky pro jejich zpracování (případně dodává produkty nebo poskytuje služby k zařízení pro zpracování informací), musí pokrývat veškeré relevantní bezpečností požadavky. Předtím, než je externím subjektům povolen přístup k informacím a prostředkům pro zpracování, musí být identifikována rizika a implementována vhodná opatření na jejich pokrytí. Má-li třetí strana přístup k interním informacím, je nutné s ní uzavřít ***Smlouvu o mlčenlivosti, ochraně informací a zákazu jejich zneužití*** (viz příloha 1).

2.15. BEZPEČNOSTNÍ INCIDENTY (BI)

Vymezení obsahu incidentu

Bezpečnostním incidentem v oblasti IT se rozumí:

- narušení chodu informační služby (dostupnost)
- narušení oprávnění ke službě nebo k datům (důvěrnost)
- narušení integrity informací (integrita)
- ohrožení sítě nebo služby, které může vést k narušení chodu služby, narušení oprávnění ke službě či informaci nebo k narušení integrity informací

- porušení předpisů a směrnic, které mohou vést k bezpečnostním incidentům.

Hlášení incidentu
V případě bezpečnostního incidentu je každý zaměstnanec, student nebo účastník CŽV JU povinen zajistit okamžitě informace o incidentu tak, aby s nimi nebylo možné neoprávněně manipulovat. Narušuje-li BI pracovní činnost, neprodleně informovat svého nadřízeného a předat tyto informace manažeru informační bezpečnosti. Jde především o předmět BI, zdroj a cíl narušení, záznamy (LOGy) o narušení, účastníky BI apod.

Zaměstnanec je současně povinen, podle svých možností, přispět k okamžitému odstranění bezpečnostního incidentu a jeho následků. Jedná se především o izolaci zdroje narušení nebo ohrožení. Takovou izolací může být vypnutí zařízení, odpojení zařízení od sítí, odstranění uživatele nebo počítače z domény, zakázání přístupu počítače nebo uživatele ke službě nebo službám. Toto je třeba provést pokud možno neprodleně po zjištění informací o bezpečnostním incidentu, které byly popsány výše. Pokud je incident takového charakteru, že v jeho průběhu dochází k významným ekonomickým nebo morálním ztrátám JU, je prvořadou povinností zaměstnance zabránit těmto ztrátám. Dále je třeba zajistit náhradní chod služby, pokud je to možné apod., obvykle ve spolupráci s IT manažerem, lokálním správcem či správcem služby.

Zamlčení bezpečnostního incidentu je samo o sobě bezpečnostním incidentem.

Problematika bezpečnostních incidentů na JU je řešena samostatnou interní směrnicí ISMS ***Bezpečnostní incidenty***.

2.16. KLASIFIKACE A ŘÍZENÍ AKTIV

Tuto oblast řeší dokument ISMS ***Metodika aktiv*** a dokumentace k analýze rizik (AR), kterou předala externí firma po provedení AR u některých součástí JU. Zdrojem pro stanovení adekvátní ochrany prostředků IT a pro výpočty AR je seznam důležitých aktiv IT v následujícím členění.

Klasifikace aktiv
Aktiva lze členit různým způsobem a podle různých kritérií. Podrobnější informace o aktivech a jejich atributech jsou obsaženy v dokumentu ISMS ***Metodika aktiv***. Následná klasifikace vychází z účelu a funkce aktiv IT:

- **HW** - servery, PC, NB, tiskárny, aktivní síťové prvky (FW, routery, modemy,...), externí disky, UPS, klimatizace, telefonní ústředny + další IT
- **SW** - OS, DB, APV, krabicový SW, utility a další základní a aplikační SW
- **data v digitální formě** - data IS, DB s uživatelskými daty, dokumentace v elektronické podobě, záložní kopie, konfigurační a autorizační soubory, atd.
- **personální aktiva** - správci, operátoři a služby externích dodavatelů (jejich know-how).

Klasifikace aktiv se provádí při jejich vzniku nebo modifikaci.

Z jiného hlediska jsou nejdůležitějšími aktivy JU:

- utajované skutečnosti
- údaje o studentech (osobní data)
- údaje o zaměstnancích (osobní data, mzdová data)
- ekonomická data o organizaci
- HW zabezpečující síťové služby.

Dalšími citlivými aktivy jsou:

- ostatní data o zaměstnancích a studentech
- ostatní údaje o provozu JU
- HW IS
- SW IS.

Evidence aktiv
Všechna důležitá aktiva všech součástí JU musí být evidována a seznam udržován aktuální. Datová aktiva (aktiva v elektronické formě) týkající se převážně ICT (dále informační aktiva či aktiva IT) tvoří nejvýznamnější část aktiv JU. Jde např. o IS, servery, síťové prvky či jiná technologická zařízení, o nichž je třeba mít přehled a odpovídajícím způsobem je chránit, neboť jejich havárie by mohla mít velmi negativní dopad na provoz celé JU.

Některé typy aktiv IT jsou spojeny s existencí dalších povinných dokumentů – jde především o IS a HW. Proto bylo rozhodnuto o centralizované evidenci aktiv IT celé JU. Pro tyto účely byl vyhrazen prostor se složkou „Aktiva IT“ na webu JU https://isms.jcu.cz/, kde je rovněž k dispozici dokumentace ISMS. Složka Aktiva IT je členěna podle součástí JU a je přístupná pouze vybraným pracovníkům IT. Za aktuální stav evidence informačních aktiv je zodpovědný IT manažer dané součásti. Vedení evidence aktiv IT je v kompetenci bezpečnostního správce součásti, správců počítačů a IS.

Vlastníci aktiv
Všechna aktiva musejí mít určeného vlastníka, který je zodpovědný za toto aktivum dle pokynů pro vlastníky aktiv obsažených v ***Metodice aktiv***. Přidělením odpovědnosti k jednotlivým informačním aktivům je pověřen pracovník určený vedoucím součásti JU, jíž aktivum náleží, obvykle ITM nebo BS. Vlastníci jsou uvedeni v evidenci aktiv.

Přípustné použití aktiv
Pravidla pro přípustné použití informací a aktiv jsou uvedena v ***Metodice aktiv***.

2.17. KLASIFIKACE INFORMACÍ

Informace jsou klasifikovány s ohledem na jejich citlivost a kritičnost. V ISMS JU se rozlišují následující typy:

- **veřejná informace - typ A**
- **interní informace - typ B**
- **důvěrná informace - typ C**

Veřejné informace jsou takové informace, které nejsou označeny. Klasifikační označení je „A“ a je možné jej vypustit. Lze je šířit i mimo organizaci, což může být omezeno pouze na subjekty, kterých se tyto informace týkají.

Interní informace jsou označeny písmenem „B“. Jsou přístupné pouze zaměstnancům a studentům JU, není možné je posílat, přenášet a distribuovat mimo JU.
S informacemi takto označenými je možné komunikovat a využívat je v rámci organizace bez rozlišení osob.

Důvěrné informace jsou označeny písmenem „C“ a není možné je jakkoliv šířit. Jde o informace řízené speciálním způsobem. Jsou k dispozici uživatelům dle distribučního seznamu nebo seznamu přístupových práv v informačních systémech či na portálech JU. Seznámení s tímto typem informací se provádí buď prostřednictvím podpisu distribučního seznamu, potvrzením o přečtení na portále ISMS nebo logem v informačním systému dle uživatele. Takovéto informace není možné šířit mimo stanovený okruh osob.

Životní cyklus informace se řídí:

- Zákonem o utajovaných skutečnostech č. 148/1998 Sb.,
- Zákonem o elektronických komunikacích a vyhláškou 336/2005 Sb.
- Zákonem o účetnictví
- Zákonem o archivnictví č.449/2004 Sb.
- Vysokoškolským zákonem
- Vnitřním předpisem JU, pokud je vydán a týká se informací nepodléhajících výše uvedeným zákonům a vyhláškám.

2.18. OZNAČOVÁNÍ A NAKLÁDÁNÍ S INFORMACEMI

Všechny informace - s výjimkou „veřejných = typ „A“ - musejí být označeny dle své klasifikace, a to v elektronické i písemné podobě. Šířit informace je možné jen na okruh osob uvedený v jejich klasifikaci.
Označení důvěrné informace musí být uvedeno na titulní straně dokumentu nebo na obrazovce informačního systému, který informaci obsahuje. Pokud strana obsahuje více různých typů informací, je označena vždy jako informace nejvíce chráněná, která se na dané stránce nebo v dokumentu objevuje.

Kopírování dokumentů, provozování elektronické pošty, faxování a tisk materiálů jsou možné pouze pro potřeby definovaných skupin uživatelů. Nelze šířit jakýmikoliv prostředky informace mimo skupiny osob, které mají přístup k informaci na základě její klasifikace. Je-li potřeba informaci tohoto typu rozšířit mimo původní okruh osob, je nutné nejprve změnit klasifikaci této informace. To může provést její vlastník. Vlastníkem je osoba, která uvedený dokument schvaluje.

Každý zaměstnanec má možnost si při operacích s dokumenty a záznamy ISMS ověřit typ dokumentu. Běžně je tento typ uveden jednak na titulní straně dokumentu a též v zápatí každé strany dokumentu vytvořeného na JU.

2.19. ŘÍZENÍ DOKUMENTACE ISMS

Tvorba, distribuce, vedení, evidence a změny dokumentace ISMS jsou řízeny interní směrnicí ***ISMS-004_Řízení dokumentace ISMS***. Dokumentace je vedena v elektronické podobě, je uložena na portálu ISMS - https://isms.jcu.cz/isms-dokumenty. Podle typu dokumentů je přístupná všem zaměstnancům a studentům JU (typ B) nebo jen vybraným zaměstnancům (typ C), případně veřejnosti (typ A). Podmínkou pro zpřístupnění dokumentů typu B a C je přihlášení na portále ISMS. K tomu použije uživatel jméno a heslo přidělené správcem LDAP či IDM nebo častěji heslo své vlastní, pokud si jej změnil (povinnost uživatele).
Před zveřejněním musí být každý dokument přezkoumán a poté schválen ředitelem CIT. Za vypracovaný dokument odpovídá autor dokumentu, za řízení dokumentace MIB.

2.20. NEJVĚTŠÍ HROZBY

Jsou uvedeny v dokumentaci z Analýzy rizik (AR) zvolené součásti JU. Jejich charakteristiky se mohou během času měnit. AR byla provedena na REK, TF a ZSF v rámci I. a II. etapy ISMS realizované v roce 2007 a 2008. Dokumentace z AR obsahuje evidenci aktiv, evidenci a klasifikaci hrozeb, evidenci a klasifikaci zranitelností a následné výpočty rizik s různými protiopatřeními. Výsledky AR jsou shrnuty v dokumentech ***Analýza rizik.*** Kompletní dokumentace k AR předaná zpracovatelem, je uložena u MIB a u zástupců výše jmenovaných součástí v digitální podobě.

Dle rozhodnutí Fóra bezpečnosti může být analýza rizik v budoucnu provedena i u dalších součástí JU. V tomto případě bude takový záměr zahrnut do plánu dalších aktivit v rámci ISMS JU.

2.21. NEJDŮLEŽITĚJŠÍ PROTIOPATŘENÍ

Nejdůležitější protiopatření plynou z analýzy rizik. Jedná se o personální, technická, organizační a administrativní opatření. Většinou jsou realizována prostřednictvím dalších bezpečnostních politik ISMS či jiných návazných dokumentů.

2.22. PERSONÁLNÍ BEZPEČNOST

Je podrobněji popsána v dokumentu ***Politika personální bezpečnosti*.**

2.23. FYZICKÁ BEZPEČNOST

Je popsána v dokumentu **ISMS-011_Politika fyzické bezpečnosti .**

2.24. ŘÍZENÍ KOMUNIKACE A PROVOZU

Další postupy jsou popsány ve směrnici ***ISMS-003_Provozní postupy***, **ISMS-003_Provozní postupy,** event. v dalších navazujících směrnicích ISMS.

2.25. ŘÍZENÍ ZMĚN

Změny ve vybavení a prostředcích pro zpracování informací musejí být řízeny tak, jak je popsáno ve směrnici ***ISMS-003_Provozní postupy***. Postup odpovídá algoritmu životního cyklu. Plánování, realizace nákupu nebo dodávky, testování, zařazení do produkčního prostředí, ověřování funkčnosti a bezpečnosti, likvidace informací nebo zařízení či jiného aktiva.

2.26. ODDĚLENÍ POVINNOSTÍ

Pro snížení příležitostí k neoprávněné modifikaci nebo zneužití aktiv musí být odděleny jednotlivé povinnosti a odpovědnosti, pokud je to možné. Zásadně nemůže být sjednocována výkonná a kontrolní funkce pro dané aktivum.

2.27. ODDĚLENÍ VÝVOJE A TESTOVÁNÍ SW OD PROVOZU

Procesy testování a vývoje SW musí být odděleny od procesů provozních. Vývoj provádějí jiní pracovníci než ti, kteří zajišťují provoz systémů a nevyužívají k němu provozní systémy. Před nasazením do produkčního prostředí se definují a provedou akceptační testy (pokud je to možné), a to včetně záznamu, který obsahuje:

- popis testu
- předpokládané chování systému
- skutečný výsledek testu.

Záznamy o akceptačních testech se uchovávají jeden rok.
Test obsahuje doporučení, zda systém zařadit do produkčního prostředí či nikoliv.

2.28. DODÁVKY SLUŽEB

Úroveň služeb týkajících se bezpečnosti informací poskytovaných třetí stranou musí být v souladu se smluvními podmínkami. Toto zajišťuje zaměstnanec pověřený kontrolou příslušných dodávek.

2.29. MONITOROVÁNÍ A PŘEZKOUMÁVÁNÍ SLUŽEB TŘETÍCH STRAN

Služby, zprávy a záznamy poskytované třetí stranou musejí být monitorovány a pravidelně přezkoumávány, audity jsou opakovány dle potřeby. Audit zajišťuje MIB. Ke každému auditu existuje plán auditu, záznam o auditu s doporučeními preventivních a nápravných opatření. Kontrolu záznamů provádí **manažer informační bezpečnosti** a informuje o tom **Fórum bezpečnosti**. Audity provádí auditor bezpečnosti, a to buď interní nebo externí. Auditor musí být k této činnosti pověřen odpovědným pracovníkem.

2.30. ŘÍZENÍ ZMĚN SLUŽEB POSKYTOVANÝCH TŘETÍMI STRANAMI

Změny v poskytování služeb, včetně udržování a zlepšování existujících bezpečnostních politik, směrnic a bezpečnostních opatření, musejí být řízeny s ohledem na kritičnost systémů a procesů, které jsou součástí opakovaného hodnocení rizik. Za řízení změn je odpovědný ředitel CIT.

2.31. ŘÍZENÍ KAPACIT

Pro zajištění požadovaného výkonu informačního systému a sítí, s ohledem na budoucí kapacitní požadavky, musí být monitorováno, nastaveno a projektováno využití zdrojů.
Lidské zdroje jsou řízeny odpovídajícími vedoucími pracovníky.

2.32. IMPLEMENTACE INFORMAČNÍCH SYSTÉMŮ (IS)

Pro implementaci nových IS na JU, jejich aktualizaci, zavádění nových verzí, testování IS v průběhu vývoje a před spuštěním jejich ostrého provozu, jakož i pro ochranu informací, s nimiž IS pracují, jsou stanovena pravidla ve směrnici ***ISMS-003_Provozní postupy***.

2.33. OPATŘENÍ NA OCHRANU PROTI ŠKODLIVÝM PROGRAMŮM

Na ochranu proti škodlivým programům a nepovoleným kódům jsou ve směrnici ***ISMS-006_Antivirová ochrana počítačů JU*** uvedena opatření na jejich detekci, prevenci a nápravu. Musí být instalován antivirový a antispamový SW. SW musí být aktualizován a testován. Za realizaci postupů odpovídá IT manažer součásti JU, pokud nepověří vedoucí součásti touto činností jiného zaměstnance.

2.34. ZÁLOHOVÁNÍ A OBNOVA INFORMACÍ

Zálohování důležitých informací je kritické pro provoz IS JU. Chybějící záloha může v případě havárie IS ohrozit funkčnost některých důležitých procesů JU. Záložní kopie dat a programového vybavení musí být pořizovány v pravidelných intervalech a ukládány na bezpečné místo pro případ budoucího použití. Podrobnější pokyny budou vydány v samostatném dokumentu ISMS ***Zálohování, archivace a obnova dat***. Každý IS by měl mít vyhotoven samostatný pracovní postup s uvedením konkrétních kroků zálohy a obnovy dat, SW či celého serveru, na němž je IS provozován, případně může být tento postup součástí Havarijních plánů IS.
Za zálohování dat je odpovědný vlastník informačního aktiva nebo jím pověřený správce.

2.35. SÍŤOVÁ OPATŘENÍ A SLUŽBY

Pro zajištění ochrany před možnými hrozbami, pro zaručení bezpečnosti systémů a aplikací využívajících sítě a pro zajištění bezpečnosti informací při přenosu, musí být počítačové sítě spravovány a kontrolovány.
Síťové služby mohou být využívány pouze autentizovanými uživateli. O využití síťových služeb musí být veden protokol, provoz a identifikace zařízení v síti musejí být monitorovány.
Do poskytování síťových služeb musí být zahrnuty bezpečnostní prvky (i v případech poskytování formou outsourcingu).

2.36. SPRÁVA POČÍTAČOVÝCH MÉDIÍ

Pro zabránění neautorizovanému přístupu nebo zneužití informací musí být stanovena pravidla pro manipulaci s počítačovými médii, jejich ukládání, včetně instrukcí k likvidaci vyřazených médií. Další pokyny jsou uvedeny ve směrnici ***ISMS-003_Provozní postupy***.

2.37. PŘEDÁVÁNÍ INFORMACÍ A PROGRAMŮ

Předání interních nebo důvěrných informací nebo programů jiným organizacím musí být založeno na písemné dohodě uzavřené mezi JU a externími subjekty, obsahující doložku o ochraně informací. Součástí doložky musejí být i sankce, které odpovídají hodnocení aktiv z analýzy rizik, byla-li provedena.

2.38. BEZPEČNOST MÉDIÍ PŘI PŘEPRAVĚ

Média obsahující interní nebo důvěrné informace musejí být během přepravy mimo JU chráněna šifrováním proti neoprávněnému přístupu, zneužití nebo modifikaci. Média musejí být označena. Média s interními a důvěrnými informacemi nesmějí být při přepravě ponechána bez dozoru.

2.39. ELEKTRONICKÉ ZASÍLÁNÍ ZPRÁV

Elektronicky přenášené důvěrné informace musejí být mimo zabezpečenou síť chráněny šifrováním.

On-line transakce

Musí být zajištěna ochrana informací přenášených při on-line transakcích tak, aby byl zajištěn úplný přenos informací a zamezilo se špatnému směrování, neoprávněné změně práv, neoprávněnému prozrazení, duplikaci nebo opakování zpráv.

2.40. VEŘEJNĚ PŘÍSTUPNÉ INFORMACE

Informace publikované na veřejně přístupných systémech jsou chráněny proti neoprávněné modifikaci.

2.41. ZAZNAMENÁVÁNÍ UDÁLOSTÍ

Auditní záznamy, obsahující chybová hlášení a jiné bezpečnostně významné události, musejí být pořizovány a uchovávány po stanovené období tak, aby se daly použít pro budoucí vyšetřování a pro účely monitorování řízení přístupu, nejméně po dobu šesti měsíců. Pokud se jedná o osobní údaje, musejí být po uplynutí této doby smazány nebo anonymizovány. Z hlediska klasifikace se jedná o informace typu „C“, tj. důvěrné. Proto musejí být tyto záznamy také odpovídajícím způsobem chráněny.

2.42. ADMINISTRÁTORSKÝ A PROVOZNÍ DENÍK

Aktivity správců systémů, sítí a IS musejí být zaznamenávány v tzv. **provozním deníku** (PD) serveru, IS, FW či jiného důležitého aktiva IT. PD je veden správcem daného aktiva a měl by obsahovat SW či HW změny a záznamy o selhání systému či jiných haváriích, aby bylo možné analyzovat chyby a stanovit opatření k nápravě. Lze jej vést různou formou - např. systém LOGu, elektronický textový soubor nebo sešit, ale měl by být z hlediska bezpečnosti vždy fyzicky uložen mimo server. K tomuto účelu je vyhrazeno místo na ***portále ISMS*** ve složce ***Aktiva IT,*** členěné podle součástí JU, kde jsou aktiva, k nimž se provozní deníky vztahují, evidována. Tam musejí být PD ukládány a aktualizovány v elektronické podobě. Přístup do dané složky mají pouze ITM, BS součásti a autoři PD (obvykle správci), jejich zástupci a případně nadřízení. Za obsah a aktuálnost PD zodpovídá jeho správce. Provozní deník je dokument typu „C“, a tomu odpovídá jeho ochrana.

2.43. SYNCHRONIZACE ČASU

Hodiny všech důležitých systémů pro zpracování informací musejí být synchronizovány se zdrojem přesného času přes jednotný NTP server určený střediskem APS CIT. Správce systému je povinen tuto synchronizaci zajistit. Další pravidla synchronizace času jsou uvedena ve směrnici ***ISMS-003_Provozní postupy.***

3. ŘÍZENÍ PŘÍSTUPU

3.1. ŘÍZENÍ PŘÍSTUPU K SYSTÉMŮM

Identifikace terminálu, autentizace uživatele a další informace týkající se přístupu k systémům jsou uvedeny ve směrnici ***ISMS-003_Provozní postupy***.

Řízení privilegovaného přístupu

Přidělování a používání privilegií musí být omezeno a řízeno. Privilegovaný přístup k systémům mají pouze správci. Každý uživatel se k systému musí hlásit pod svým uživatelským účtem. Teprve následně se může přepnout do privilegovaného režimu, má-li k tomu oprávnění. O přihlášení a přepnutí musí existovat záznam.

3.2. SPRÁVA A POUŽÍVÁNÍ UŽIVATELSKÝCH HESEL

Hesla musejí splňovat komplexní požadavky na bezpečnost. Při výběru a používání hesel musí být po uživatelích požadováno, aby dodržovali stanovené bezpečnostní postupy uvedené v ***Provozních postupech*** a směrnici ***ISMS-007_Správa a bezpečnost provozu počítačů***. Za kontrolu odpovídají správci ICT a správci jednotlivých IS a domény. Systém správy hesel musí být interaktivní a musí zajišťovat použití kvalitních hesel.

3.3. PŘEZKOUMÁNÍ PŘÍSTUPOVÝCH PRÁV UŽIVATELŮ

Správce domény a IS musí nejméně jednou ročně provádět formální přezkoumání přístupových práv uživatelů. Musí být proveden test na sílu hesel, kontrolována expirace hesel a musí být přezkoumána oprávněnost existence účtu a výše oprávnění.

3.4. NEOBSLUHOVANÁ UŽIVATELSKÁ ZAŘÍZENÍ

Uživatelé a správci musí zajistit přiměřenou ochranu neobsluhovaných zařízení – PC, servery, firewall, a další. Takovou ochranou je např. aktivace spořiče obrazovky PC zabezpečená heslem uživatele. Spořič musí být nastaven tak, aby se aktivoval nejpozději po 20 minutách nečinnosti uživatele.

3.5. ZÁSADA PRÁZDNÉHO STOLU A PRÁZDNÉ OBRAZOVKY MONITORU

Po skončení práce nesmí zůstat na pracovním stole žádné dokumenty typu „C“, tj. důvěrné (typy viz kapitola tohoto dokumentu *Klasifikace informací* a směrnice ***Řízení dokumentace***) nebo vyměnitelná média s nešifrovanými důvěrnými interními informacemi. Totéž platí pro monitory počítačů. Stejně je třeba postupovat v případě, kdy se uživatel vzdálí ze svého pracoviště tak, že je mimo dohled.

3.6. VYUŽÍVÁNÍ SÍŤOVÝCH SLUŽEB

Uživatelé mohou mít přímý přístup pouze k těm síťovým službám, pro jejichž použití jsou oprávněni.

3.7. AUTENTIZACE UŽIVATELE EXTERNÍHO PŘIPOJENÍ

Přístup vzdálených uživatelů musí být autentizován. Pro vzdálený přístup se využívá technologie IP VPN. Pokyny jsou uvedeny ve směrnici ***ISMS-007_Správa a bezpečnost počítačové sítě JU***.

3.8. IDENTIFIKACE ZAŘÍZENÍ V SÍTÍCH

Při autentizaci připojení musí být použita automatická identifikace zařízení. U zařízení zahrnutých v doméně se toto provádí prostřednictvím doménového ovladače.

3.9. OCHRANA PORTŮ PRO VZDÁLENOU DIAGNOSTIKU A KONFIGURACI

Fyzický i logický přístup k diagnostickým a konfiguračním portům musí být bezpečně řízen. Přístup na privilegované porty mají pouze administrátoři a specializované programy, které slouží k daným účelům.

3.10. PRINCIP ODDĚLENÍ V SÍTÍCH

Skupiny informačních služeb, uživatelů a informačních systémů musí být v sítích odděleny. Jedná se především o personální a mzdové agendy, o studijní agendy a zaměstnanecké a studentské sítě.

3.11. BEZPEČNÉ POSTUPY PŘIHLÁŠENÍ

Přístup k operačnímu systému musí být řízen a dle možnosti musí využívat bezpečné protokoly např. SSH, SSL apod., nebo např. relace s jednorázovými hesly. Další informace jsou ve směrnici ***ISMS-003_Provozní postupy***.

3.12. IDENTIFIKACE A AUTENTIZACE UŽIVATELŮ

Všichni uživatelé musejí mít pro výhradní použití jedinečný identifikátor (uživatelské ID) a musí být také zvolen vhodný způsob autentizace k ověření jejich identity. Ve výjimečných případech je možné použít hromadný identifikátor, ale pak musí být dohledatelná konkrétní osoba, která jej využila, např. pomocí protokolu, kde je evidována práce s tímto účtem.

3.13. POUŽITÍ SYSTÉMOVÝCH NÁSTROJŮ

Použití systémových nástrojů, které jsou schopné překonat systémové nebo aplikační kontroly musí být omezeno a přísně kontrolováno. Takové nástroje je možné využít např. pro zjištění zranitelností sítí nebo systémů. Používat je může buď administrátor nebo auditor.

3.14. ČASOVÉ OMEZENÍ RELACE

Neaktivní relace se musí po stanovené době nečinnosti ukončit, umožňuje-li to použité programové vybavení. V tomto případě se jedná o omezení relace na straně serveru.

3.15. OMEZENÍ PŘÍSTUPU K IS

Uživatelé informačních systémů, včetně pracovníků podpory, musejí mít přístup k informacím a funkcím IS omezen v souladu s definovanými pravidly řízení přístupu.

3.16. MOBILNÍ VÝPOČETNÍ ZAŘÍZENÍ A SDĚLOVACÍ TECHNIKA

Při použití mobilních výpočetních a komunikačních zařízení – týká se především přihlašování, šifrování a ochrany proti škodlivým kódům - musejí být dodržena pravidla popsaná ve směrnici ***ISMS-003_Provozní postupy***.

4. VÝVOJ A ÚDRŽBA INFORMAČNÍCH SYSTÉMŮ

4.1. ANALÝZA A SPECIFIKACE BEZPEČNOSTNÍCH POŽADAVKŮ
Při vývoji nových informačních systémů nebo rozšíření existujících IS je potřeba zahrnout také požadavky na bezpečnostní opatření.

4.2. KONTROLA VSTUPNÍCH DAT
Vstupní data aplikací musí být zadavatelem kontrolována z hlediska správnosti a adekvátnosti.

4.3. KONTROLA VNITŘNÍHO ZPRACOVÁNÍ
U jednotlivých aplikací musí být stanoveny bezpečnostní požadavky na zajištění autentizace a integrity zpráv a dle potřeby určena a zavedena vhodná opatření.
Pro detekci poškození nebo modifikace informací vzniklého chybami při zpracování nebo úmyslnými zásahy by mělo být při instalaci aplikace zváženo začlenění kontroly platnosti dat.

4.4. KONTROLA VÝSTUPNÍCH DAT
Výstupní data aplikací musí být uživateli kontrolována z hlediska platnosti.

4.5. POUŽITÍ KRYPTOGRAFICKÝCH OPATŘENÍ
Pravidla pro používání kryptografických opatření budou stanovena buď doplněním do směrnice ***ISMS-003_Provozní postupy*** nebo samostatnou směrnicí.

Správa klíčů
Používání kryptografických technik je podporováno systémem jejich správy:
- při šifrováni důležitých dat je použito nejméně dvou klíčů
- každý uživatel a správce musí mít zálohu svého klíče
- veřejné klíče jsou v organizaci centrálně spravovány na serveru certifikační autority, existuje-li
- zálohy klíčů uživatelů a správců jsou bezpečně uchovány u IT manažera součásti nebo osoby stanovené vedoucím součásti.

4.6. PROGRAMOVÉ VYBAVENÍ PRO VÝVOJ IS
K vývoji IS je povoleno používat pouze schválené programového vybavení.

4.7. ŘÍZENÍ PŘÍSTUPU KE ZDROJOVÝM KÓDŮM
V případě vývoje IS přímo na JU musí být zavedeno řízení přístupu ke knihovně zdrojových kódů. Tam mají přístup pouze pracovníci, kteří řeší vývoj daného IS, event. správce vývojového serveru nebo jeho zástupce, nejsou-li členy vývojového týmu.

4.8. POSTUPY ŘÍZENÍ ZMĚN IS
Podstatné změny IS mající vliv na bezpečnost provozu musí být řízeny a zaznamenávány. Odpovědným je vždy příslušný správce tohoto typu aktiva. Řízení změny probíhá dle standardního postupu:

- žádost o změnu – podává správce IS řediteli CIT nebo manažeru IB
- schválení žádosti včetně posouzení bezpečnostních aspektů změny
- realizace změny
- akceptační testy - dle rozhodnutí ředitele CIT
- implementace změny do provozního prostředí.

Další informace k řízení změn IS jsou uvedeny ve směrnici ***ISMS-003_Provozní postupy.***

4.9. TECHNICKÉ PŘEZKOUMÁNÍ APLIKACÍ PO ZMĚNÁCH OPERAČNÍHO SYSTÉMU
V případě změny operačního systému musí být administrátorem přezkoumány a otestovány kritické aplikace, aby bylo zajištěno, že změny nemají nepříznivý dopad na provoz nebo bezpečnost IS. O změně i o přezkoumání změny se provede záznam do provozního deníku IS.

4.10. ÚNIK INFORMACÍ
Musí být zabráněno úniku informací. Použité prostředky jsou např. prostředky ochrany proti škodlivému kódu, šifrování interních a důvěrných dat, prověrka fyzických osob, smluvní zabezpečení informací. V případě úniku dat se postupuje dle interní směrnice ***Bezpečnostní incidenty***.

4.11. IS VYVÍJENÉ EXTERNÍM DODAVATELEM

IS, který má být v prostředí JU implementován a je vyvíjený externím dodavatelem, musí být monitorován. Programové vybavení musí být následně zprovozněno v testovacím prostředí. Teprve po provedení akceptačních testů a po schválení ředitelem CIT může být IS instalován do provozního prostředí JU.

4.12. ŘÍZENÍ, SPRÁVA A KONTROLA TECHNICKÝCH ZRANITELNOSTÍ

Bezpečnostní auditor zajišťuje v případě potřeby provedení penetračních testů za účelem získání informace o existenci technické zranitelnosti v provozovaném informačním systému a vyhodnocení úrovně ohrožení. Na základě testů navrhuje příslušná opatření na pokrytí souvisejících rizik.

4.13. HAVARIJNÍ PLÁNOVÁNÍ

Obnova provozu důležitých komponent IS, které mohou ovlivnit plnění provozních funkcí JU se řídí tzv. Plány kontinuity, havarijními plány a plány obnovy, které by měly být zpracovány jako samostatná dokumentace každého IS. Havarijní plány jsou prověřovány a je kontrolována jejich účinnost minimálně jedenkrát ročně. Jsou stanoveny mechanizmy změn v těchto plánech.
Mimo havarijní plány existují i evakuační plány, které jsou zpracovány pro jednotlivé lokality JU, pokud se nacházejí v záplavových oblastech. Evakuační plány jsou k dispozici u pracovníka zodpovědného za požární ochranu objektů JU.

5. SOULAD S POŽADAVKY

5.1. URČENÍ RELEVANTNÍ LEGISLATIVY

Pro každý informační systém musí být jeho správcem jednoznačně definovány, zdokumentovány a udržovány aktuální veškeré relevantní zákonné a smluvní požadavky a způsob, jakým jsou dodržovány.

5.2. ZÁKON NA OCHRANU DUŠEVNÍHO VLASTNICTVÍ

Pro zajištění souladu se zákonnými a smluvními požadavky na použití materiálů a aplikačního programového vybavení, které mohou být chráněny zákony na ochranu duševního vlastnictví, je povoleno užívání pouze legálního programového vybavení.

5.3. OCHRANA ZÁZNAMŮ ORGANIZACE

Důležité záznamy musí být chráněny proti ztrátě, zničení a padělání.

5.4. OCHRANA OSOBNÍCH ÚDAJŮ A SOUKROMÍ

Ochrana osobních údajů a soukromí musí být zajištěna v souladu s odpovídající legislativou – viz Nařízení EU 2016/679 (GDPR), představující právní rámec ochrany osobních údajů, dále viz zákon č. 101/2000 Sb. o ochraně osobních údajů s dalšími souvisejícími předpisy. Nařízení EU 2016/679 je zákonu č.101/2000 sb. vždy nadřízeno. Dále viz Opatření rektora R378 a R379 (všechny výše uvedené normy viz níže „Související dokumenty“). Pokud je to relevantní, je nutno respektovat i smlouvy s jinými subjekty. Jedná se především o data studentů a zaměstnanců JU.

5.5. PREVENCE ZNEUŽITÍ PROSTŘEDKŮ PRO ZPRACOVÁNÍ INFORMACÍ

Je zakázáno používat prostředky pro zpracování informací jiným než autorizovaným způsobem.

5.6. SHODA S BEZPEČNOSTNÍMI POLITIKAMI A SMĚRNICEMI

Vedoucí zaměstnanci musejí zajistit, aby všechny bezpečnostní postupy v rozsahu jejich odpovědnosti byly prováděny správně, v souladu s bezpečnostními politikami, směrnicemi ISMS a Opatřeními rektora či Opatřeními jiných vedoucích zaměstnanců.

5.7. AUDIT INFORMAČNÍCH SYSTÉMŮ

Informační systémy by měly být auditorem bezpečnosti kontrolovány, zda jsou v souladu s bezpečnostními opatřeními JU. Audity a činnosti zahrnující kontrolu provozních systémů musejí být vždy včas naplánovány, aby se minimalizovalo riziko narušení činností JU. K nástrojům určeným pro audit IS má přístup pouze auditor bezpečnosti a manažer informační bezpečnosti, aby se předešlo jejich možnému zneužití nebo ohrožení provozu IS.

C. ZÁVĚREČNÁ USTANOVENÍ

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

SEZNAM PŘÍLOH

Označení přílohy	Název přílohy
ISMS-002-P1	Smlouva o mlčenlivosti, ochraně informací a zákazu jejich zneužití

SOUVISEJÍCÍ DOKUMENTY

Označení dokumentu	Název dokumentu
ČSN ISO/IEC 27001	Systém řízení bezpečnosti informací (ISMS)
ČSN ISO/IEC 17799	Soubor postupů pro bezpečnost informací
ČSN ISO/IEC TR 13335	Směrnice pro řízení bezpečnosti IT
Zákon č. 101/2000 Sb.	Zákon o ochraně osobních údajů
Zákon č.127/2005 Sb.	Zákon o elektronických komunikacích
Zákon č.480/2004 Sb.	Zákon o některých službách informační společnosti
Zákon č.111/1998 Sb.	Zákon o vysokých školách
ISMS-001	Politika ISMS JU
ISMS-004	Řízení dokumentace ISMS
ISMS-006	Antivirová ochrana počítačů JU
ISMS-007	Správa a bezpečnost provozu počítačů
R95_2007	Užívání PC, SW, NET (Opatření rektora)
R375_2018	Organizační struktura JU a Rektorátu JU
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)