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

ISMS - SYSTÉM ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI

Označení dokumentu:	**ISMS-012**
Název dokumentu:	**Bezpečnostní incidenty**
Typ dokumentu:	Interní dokument - typ B – směrnice
Určeno pro:	Všechny zaměstnance, studenty a účastníky CŽV JU, zvláště všechny specialisty ICT (LS PC, AVO a sítí), správce objektů a zabezpečených oblastí
Prvek normy ISO:	27001
Datum vydání:	12.8.2014
Datum účinnosti:	13.8.2014
Platnost do:	odvolání
Počet stran + příloh:	9 + 2
Verze:	1.0
Účel:	Klasifikace bezpečnostních incidentů, jejich hlášení a postupy při jejich výskytu.
Uložení:	Portál ISMS - https://isms.jcu.cz/
Ruší dokumenty:	-
Zpracovatel:	Ing. Jana Kolářová - MIB JU
Přezkoumal:	IT manažeři a správci ICT JU, vedoucí APS, HS sítě
Schválil:	RNDr. Josef Milota - ředitel ISMS a CIT

OBSAH

A. ÚVODNÍ USTANOVENÍ

CÍL PROCESU A ÚČEL

Cílem této směrnice je popsat typy bezpečnostních incidentů, jejich řešení a stanovit postupy s cílem zabránit opakování BI přijetím potřebných opatření a eliminovat jejich výskyt také osvětou uživatelů JU.

POJMY, DEFINICE A ZKRATKY

1. POJMY A DEFINICE

- **Bezpečnostní incident (BI) -** jedna nebo více nežádoucích a neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činnosti JU a ohrožení bezpečnosti informací.
- **Fórum bezpečnosti JU -** je nejvyšší orgán, který rozhoduje o otázkách informační bezpečnosti na půdě JU. Dále viz *ISMS-002_Celková bezpečnostní politika JU*, str.8.
- **HelpDesk -** technická podpora uživatelů (studentů, zaměstnanců a účastníků CŽV) JU, prostřednictvím níž mohou uplatňovat své požadavky. Na JU jde o portál https://rt.jcu.cz/ kam lze po přihlášení zadat požadavek k vyřešení (podrobněji uvedeno ve směrnici *ISMS-003_Provozní postupy* a jejích přílohách *ISMS-003-P5_HelpDesk-řešení požadavků* a *ISMS-003-P1_Klíčové IS)*.
- **Phishing** - druh internetového podvodu zaměřený na získání přístupových údajů uživatelů k účtům do IS, k e-mailům nebo do elektronického bankovnictví a jejich zneužití pro obohacení podvodníků.
- **Součást JU** - fakulta či ústav jako organizační jednotka JU.
- **Spam** – nevyžádané sdělení (nejčastěji e-mail) obvykle masově šířené Internetem, nejvíce využívané k rozesílání nežádoucí reklamy.
- **Správce zabezpečené oblasti** – obvykle bezpečnostní správce, správce sítě či správce ICT součásti JU pověřený vedoucím součásti JU či útvaru provozující zabezpečenou oblast, který odpovídá za její ochranu, přiděluje práva přístupu pro další osoby a řídí a eviduje vstup servisních organizací.
- **Uživatel JU** – zaměstnance, student či účastník CŽV JU.
- **Zabezpečená oblast** – stavebně ohraničený prostor uvnitř objektu, kde se zpracovávají nebo ukládají data, zejména pak citlivé či utajované informace. Jsou to technologické místnosti se zařízeními ICT zajišťující provoz IS, zálohování dat a dodávky elektrické energie, digitální telefonní a komunikační zařízení, síťové komponenty, prostory pro archivaci médií, učebny s ICT, případně jiná technologie.

2. ZKRATKY

- **BI** – viz **Bezpečnostní incident**
- **CIT –** Centrum informačních technologií – celoškolské pracoviště JU.
- **CŽV –** celoživotní vzdělávání.
- **HS –** hlavní správce ICT JU – vždy jeden na dané platformě (HS PC, HS AVO, HS sítě)
- **ICT** (Information and Communication Technologies) – Informační a komunikační technologie - zahrnují veškeré technologie používané pro komunikaci a práci s informacemi.
- **IPS** – Identifikační a přístupový systém – pracoviště CIT, které na JU provozuje a spravuje JIS a další IS.
- **IS** – Informační systém = systém pro sběr, udržování, zpracování a poskytování informací a dat pomocí počítačů.
- **ISMS** (Information Security Management System) – Systém řízení bezpečnosti informací.
- **IT** (Information technology) – Informační technologie - zjednodušeně řečeno počítače a vše co s nimi souvisí.
- **ITM** – IT manažer, který zajišťuje ICT služby své součásti (fakulty, ústavu).
- **JU** – Jihočeská univerzita v Českých Budějovicích.
- **LS PC, LS AVO, LS sítě** - lokální správce počítačů, antivirové ochrany a sítě na každé součásti JU.
- **MIB –** Manažer informační bezpečnosti JU.
- **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.
- **P2P** - (Peer-to-Peer) - klient-klient je označení typu počítačové sítě, ve které spolu komunikují (vyměňují si data) přímo jednotliví klienti-uživatelé sítě. Např. výměna hudby MP3 nebo filmů apod.
- **RT** (Request Tracker) – systém podpory řešení provozních problémů, viz pojem HelpDesk.

ODPOVĚDNOSTI A PRAVOMOCI

Manažer informační bezpečnosti JU

- Spravuje frontu „incidenty" v systému HelpDesk, kde jsou evidovány bezpečnostní incidenty (BI) za celou JU a kontroluje jejich řešení a implementaci opatření
- upozorňuje uživatele JU, kteří vyvolali BI na nutnost dodržování předpisů a požaduje od nich (případně dalších řešitelů BI) informaci o přijatých nápravných opatřeních
- předkládá Fóru bezpečnosti informace o závažných BI a jejich řešení.

Hlavní správce sítě JU (HS sítě)

- komunikuje s poskytovatelem připojení JU k Internetu – sdružením CESNET, od něhož dostává informace o BI uživatelů JU a jemuž hlásí síťové BI požadovanou formou
- zpracovává tato hlášení, vyhodnocuje je a upozorňuje viníky na nutnost změny a nápravu, současně o těchto BI informuje i MIB JU a vedoucího APS
- kontroluje chod sítě JU a archivuje hlášení o BI způsobených uživateli v síti JU.

Správce ICT součásti (LS PC, LS AVO, LS sítě, případně HS), bezpečnostní správce nebo ITM:

- řeší BI v rámci své součásti a stanovuje nápravná a preventivní opatření
- pomáhá uživatelům určit závažnost BI a spolupracuje s nimi při hlášení BI, případně sám zašle hlášení na incidenty@rt.jcu.cz
- setká-li se či je mu nahlášen BI typu:
  - porušení fyzické bezpečnosti, řeší jej co nejdříve se správcem objektu
  - narušení provozu lokální počítačové sítě – spolupracuje při řešení s HS sítě JU
  - jiný BI - řeší bezodkladně nápravu s přímým nadřízeným
- závažná či opakující se porušení bezpečnosti ICT vždy řeší přes HelpDesk, po analýze a vyřešení provede záznam o výsledku a přijatých protiopatřeních
- poučí uživatele své součásti - pokud BI zavinil - o nutnosti změny chování a nápravných opatřeních.

Zaměstnanec student nebo účastník CŽV JU (uživatel JU)

- je povinen nahlásit zjištěný či jím vyvolaný BI neprodleně po jeho zjištění - způsob hlášení viz kapitola 2 níže; neučiní-li tak, může být škoda způsobená nenahlášením incidentu po uživateli vymáhána
- musí poskytnout součinnost při řešení BI (odpojení PC od sítě, umožnění přístupu, předání potřebných informací, aplikace doporučeného řešení atd.)
- zjistí-li poruchy rozvodu energií či jakékoli narušení fyzické bezpečnosti kdekoli v objektech JU ihned informuje recepci nebo správce objektu/zabezpečené oblasti (seznam správců objektů JU viz příloha 2 – ISMS-011-P2 Zabezpečené oblasti a správci), případně lokálního správce ICT své součásti (viz https://isms.jcu.cz/kontakty)
- řídí se Opatřením rektora ke stanovení organizace požární ochrany
- vyvaruje se jakýchkoliv vědomých BI
- respektuje a dodržuje zákony ČR (zvláště Zákon 101/2000 Sb. O ochraně osobních údajů a Zákon č. 121/2000 Sb.- Autorský zákon), směrnice ISMS JU a opatření rektora, kvestora, děkana a ředitelů, které se vztahují k BI – viz oddíl C této směrnice
- je-li obětí BI, má právo na poskytnutí informací o průběhu řešení incidentu a jeho závěrech
- je si vědom toho, že nenahlášený BI je sám o sobě bezpečnostním incidentem
- bere na vědomí, že není anonymní, ale je tzv. „dohledatelný" a v případě, že se dopustí BI, je možné zjistit jeho identitu.

Další odpovědnosti jsou součástí dokumentu.

ZMĚNY OPROTI PŮVODNÍ VERZI

Toto je první verze 1.0 dokumentu.

B. POPIS

Stav, který nastane při narušení pravidel bezpečnostní politiky - směrnic ISMS či porušení některých právních předpisů a zákonů ČR – viz oddíl C. níže - nebo nastane dosud neznámá a nepředpokládaná situace ovlivňující informační bezpečnost, lze nazvat **bezpečnostní událostí**. Samotný vznik bezpečnostní události nemusí být ještě bezpečnostním incidentem (BI). Jím se může tato situace stát až po vyhodnocení bezpečnostní události. S tou přichází obvykle do prvního kontaktu běžný uživatel, který BI ne vždy umí poznat. Pak se může obrátit na lokální správce ICT (LS PC, AVO či sítě), bezpečnostního správce (BS) nebo IT manažera (ITM) dané součásti JU.

Bezpečnostní incident je tedy jedna nebo více nechtěných nebo neočekávaných indikovaných bezpečnostních událostí, jimiž jsou s vysokou pravděpodobností narušeny procesy, chod informačních systémů, provozu sítě či služeb JU při nerespektování pravidel definovaných k jejich ochraně a uvedených prioritně v základním dokumentu ISMS-002_Celková bezpečnostní politika – viz https://isms.jcu.cz/isms-dokumenty/interni-dokumenty-typ-b/isms-002_cbp a dalších směrnicích ISMS (seznam lze nalézt na https://isms.jcu.cz/isms-dokumenty/ISMS-000_Seznam%20smernic.pdf/view).

1. TYPY BEZPEČNOSTNÍCH INCIDENTŮ

Bezpečnostní incidenty lze rozdělit podle různých hledisek. BI určitého typu může vyvolat incidenty jiných typů.

1.1. LOGICKÉ TŘÍDĚNÍ

- narušení chodu informační služby (dostupnost)
- narušení oprávnění ke službě nebo k datům (důvěrnost)
- narušení integrity informace (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 způsobit další BI – např. svévolná změna konfigurace pracovní stanice, odstranění antivirového SW, použití elementárního hesla, nastavení přístupu bez hesla apod.

1.2. PODLE ZPŮSOBENÝCH ŠKOD

- **Lehké BI** – ty, které nezpůsobily žádnou finanční ztrátu, nemají negativní vliv na činnosti dalších služeb či uživatelů JU a lze je vyřešit za účasti lokálního správce ICT na úrovni fakulty/ústavu – viz kap. 6 níže.
- **Závažné BI** → takové BI, které mají vážné následky, negativně ovlivňují či přímo brání chodu IS, obvykle způsobují finanční ztráty a poškozují dobré jméno JU. Ty je nutné nahlásit - viz kap. 3 „Hlášení BI" níže. Řešení těchto typů BI vyhodnocuje Fórum bezpečnosti JU, které rozhoduje o případných sankcích.

2. PŘEHLED ZÁVAŽNÝCH BI

Poměrně snadno lze odhadnout porušení zákonů či podvodnou snahu o vylákání přístupových údajů k informačním a počítačovým systémům. Obtížněji lze odhalit neoprávněný přístup k počítačovému systému či útoky na systém, kdy může dojít k jeho zahlcení tak, že přestává reagovat na oprávněné požadavky. Takové neoprávněné aktivity, stejně jako další níže uvedené události, jsou považovány za závažné BI a je nezbytné je ohlásit.

Konkrétní příklady nejčastějších závažných BI:

- zcizení, ztráta pevných či přenosných elektronických přístrojů (PC, NB, PDA, média s citlivými daty)
- zcizení, ztráta firemní dokumentace ICT
- zcizení a ztráta dat, jejich neoprávněné přepsání nebo zničení
- pokusy o neoprávněné přihlášení do počítačové sítě nebo k IS
- zavirování PC s následkem šíření malware do/ze sítě JU
- Spam – pokud se opakuje a i přes upozornění iniciátora je nadále odesílán
- nedodržení smluvních ustanovení s třetími stranami, týkající se managementu bezpečnosti informací
- pokus nebo reálné fyzické uskutečnění neoprávněného přístupu do zabezpečených oblastí či prostor s ICT

- neoprávněné sdílení autorských děl v síti P2P (např. při použití software G3-Torrent, Torrent swapper…, MP3 Rocket atd.)
- poskytnutí informací třetím stranám bez příslušného oprávnění a zveřejnění či poskytnutí informací osobám mimo JU (např. osobních či citlivých dat o uživatelích JU, přístupových údajích apod.)
- zjištění porušení pravidel požární ochrany v souvislosti s prostředky ICT či zabezpečenými oblastmi
- útoky způsobující zahlcení systému, který pak buď neodpovídá anebo má extrémně dlouhou dobu odezvy
- nedodržení ustanovení pracovní smlouvy a jejich dodatků v souvislosti s negativním používáním prostředků ICT
- ztráta, zcizení nebo nefunkčnost pronajaté ICT v užívání JU
- interními audity zjištěné nedodržení stanovených postupů, které mohou vést k různým BI
- zamlčení zjištěného BI.

3. HLÁŠENÍ BI

V případě zjištění bezpečnostního incidentu je **každý zaměstnanec, student a účastník CŽV** povinen závažný BI ihned nahlásit a zajistit okamžitě informace o incidentu tak, aby s nimi nebylo možné neoprávněně manipulovat. Tím přispěje **k co nejrychlejšímu odstranění bezpečnostního incidentu** a jeho následků. Jedná se především o izolaci zdroje narušení nebo ohrožení (např. vypnutí či odpojení zařízení, které BI způsobuje, od sítě).
Lokální správce ICT pak může zablokovat uživatele nebo počítač v doméně, zakázat přístup. počítače nebo uživatele ke službě apod.
Toto je třeba provést pokud možno neprodleně po zajištění informací o závažném BI, 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.

3.1. CO O BI NAHLÁSIT

Jde o informace, které blíže určují bezpečnostní incident, aby bylo možné ihned zahájit jeho řešení a zabránit tak event. dalším škodám:

- kdy k BI došlo
- kde nastal (určit co nejpřesněji místo)
- kdo jej způsobil (konkrétní útočník či účastníci BI a informace vedoucí k jeho/jejich identifikaci)
- jak k BI došlo
- co bylo cílem útoku (je-li to zřejmé).

3.2. ZPŮSOBY HLÁŠENÍ BI

Dle charakteru BI má uživatel JU povinnost nahlásit zjištěný závažný BI jedním z následujících způsobů:

- zaslat hlášení o BI e-mailem na incidenty@rt.jcu.cz – s údaji uvedenými v příloze P2 této směrnice – viz *„ISMS-012-P2_BI-Hlášení“*
- může požádat o pomoc lokálního správce ICT své součásti (PC, AVO, sítě), bezpečnostního správce nebo IT manažera, případně hlavního správce JU – osobně, telefonicky, e-mailem
- za předpokladu, že BI narušuje pracovní činnost a povinnosti zaměstnance, který bezpečnostní incident zjistil, je navíc třeba neprodleně informovat i přímého nadřízeného.

Zamlčení bezpečnostního incidentu je samo o sobě bezpečnostním incidentem !

4. PŘÍJEM A POSTUP ŘEŠENÍ BI

Řešení BI je graficky znázorněno vývojovým diagramem v příloze č. 1 – viz *„ISMS-012-P1_BI-Řešení“*. Pokud není zcela jasné, zda jde o bezpečnostní incident, rozhoduje na základě poskytnutých informací lokální správce ICT, v případě potřeby ve spolupráci s manažerem informační bezpečnosti.

Postupně je třeba provést následující kroky:

1. Identifikovat, kde k BI došlo, lokalizovat zasažený objekt a zjistit účastníky BI – počítač, uživatele či jiné zdroje

2. co nejrychleji zabránit dalším škodám
3. analyzovat příčinu a navrhnout postup řešení BI
4. odstranit následky - zajistit náhradní chod služby, pokud byla narušena
5. určit závažnost a škody
6. přijmout konkrétní preventivní opatření, aby se BI neopakoval
7. je-li to vyžadováno, odpovědět na stížnost – např. poskytovateli sítě či služby
8. upozornit uživatele na změnu činností či chování – buď jen iniciátora a účastníky BI nebo obecně i další uživatele, a to dle charakteru BI
9. informovat správce ICT, pokud BI sám neřešil či nenahlásil
10. vytvořit záznam o incidentu
11. podle potřeby upravit pravidla a aktualizovat směrnice ISMS či Opatření vedoucích pracovníků
12. v případě finančních ztrát následkem BI vyvolat jednání disciplinární a škodní komise, ev. trestní šetření.

5. EVIDENCE BI

Aby bylo možné bezpečnostní incidenty analyzovat, odhalit jejich zdroj a reagovat na ně, je nutné shromáždit co nejvíce informací a vést jejich evidenci.

Co je vhodné evidovat:

- kdy k BI došlo
- kde nastal – určit místo
- kdo jej způsobil – konkrétní útočník či informace vedoucí k jeho identifikaci
- jak k BI došlo
- co bylo cílem útoku
- charakter narušení – úmysl, nedbalost, neznalost
- jaké opatření bylo překonáno – fyzické, logické, organizační, personální, atd.
- jaké aktivum ICT bylo narušeno – HW, SW, síť, data
- pravděpodobnost opakování.

Evidence závažných BI je součástí HelpDesku (fronta „incidenty“), kde kontrolu jejich řešení a splnění stanovených opatření provádí manažer informační bezpečnosti JU, který případně doplňuje nová pravidla a aktualizuje směrnice ISMS. Informuje o nich a jejich řešení Fórum bezpečnosti JU.

6. LEHKÉ BEZPEČNOSTNÍ INCIDENTY

Níže jsou uvedeny příklady BI a nestandardních situací, které obvykle vyřeší uživatel za pomoci lokálního správce PC, AVO nebo sítě, případně bezpečnostního správce či IT manažera své součásti. Ten v daném případě rozhodne, zda bude nutné se dále incidentem zabývat. Jde o tyto anomálie:

- odhalení nakaženého souboru antivirovým programem pokud nešíří viry na další PC nebo nestandardně se chovající počítač
- selhání přihlašovací procedury k PC na JU
- vyzrazení vlastního hesla účtu – uživatel JU si jej okamžitě musí změnit
- příjem nevyžádané pošty – spamu, pokud není spojen s další podvodnou činností – např. phishingem typu požadavku na zaslání přihlašovacích informací k účtu, žádostní o zaplacení finanční částky apod.
- odcizení přenosných médií (např. DVD, USB flash disků, přenosných disků atd.), pokud neobsahují nezašifrovaná citlivá data JU
- ztráta či zcizení uživatelské identifikační karty JU – řeší se bezodkladně osobně s pracovištěm IPS či HelpDesk
- rozdíly zjištěné při inventarizaci prostředků ICT – řeší zaměstnanec s přímým nadřízeným
- nedostupnost počítačové sítě anebo jednotlivých aplikací - uživatel pouze upozorní správce sítě (LS či HS) nebo správce aplikace.

7. MOŽNOSTI PŘEDCHÁZENÍ BI

Nejčastější příčinou bezpečnostních incidentů bývá lidský faktor, někdy dokonce neúmyslně zaviněný z nevědomosti. Následující výčet je výběr doporučení, které jsou uvedeny i v jiných směrnicích ISMS a na která by měl uživatel počítače dbát a stanovená pravidla dodržovat, aby co nejvíce eliminoval výskyt BI.

7.1. PRAVIDLA PRO VŠECHNY UŽIVATELE JU

- chránit hesla a klíče – nesdělovat, volit složitější a delší, častěji je měnit, zvláště při podezření jejich zcizení změnit okamžitě
- mít aktuální antivirový SW – nikdy jej nevypínat či neodstraňovat, průběžně aktualizovat, periodicky testovat stav disků a výměnných médií
- archivovat a šifrovat citlivá data – zvláště na výměnných médiích (flash, externí disky apod.) a tato chránit před zcizením
- znát operační systém a používat vhodné nástroje a utility – před zahájením práce se dobře seznámit s jejich funkcí a využívat všechny přednosti umožňující zvýšení bezpečnosti, např. e-mailový klient, webový prohlížeč, manipulace se soubory, ...
- uvědomit si možnost nebezpečí napadnutí systému zevnitř
- chránit své osobní a autentizační údaje – varovat se odpovídání na výzvy k jejich odeslání či sdělení jakoukoli formou, např. pod záminkou potřeby administrátorských změn atd.
- používat pouze legální software (podložený licencí nebo volně dostupný), který je potřeba pro pracovní nebo studijní činnost
- důsledně dodržovat stanovená pravidla ISMS
- dodržovat striktně autorský zákon – nestahovat dokumenty, videa, zvukové záznamy a jiná data jemu podléhající (musí být dodrženy smluvní či obchodní podmínky)
- chovat se rozumně, neodpovídat na různé výzvy zbrkle, ale pečlivě zvažovat své činnosti, zvláště je-li uživatel vyzýván ke sdělení interních dat a citlivých údajů či zaplacení určité částky → přílohy neotevírat a nikdy na to nereagovat!

7.2. DOPORUČENÍ PRO SPRÁVCE ICT A VEDENÍ JU

- dle možnosti vyloučit anonymní užívání sítě
- trvat na jednoznačné autentizaci uživatelů – každý uživatel má svůj vlastní účet a heslo
- logovat aktivity uživatelů (přístupy ke službám) a tyto logy archivovat pro možnost pozdější detekce zdroje BI
- provádět osvětu uživatelů o bezpečném chování při práci s ICT formou přednášek, e-learningových kurzů či školení.

C. ZÁVĚREČNÁ USTANOVENÍ

Kontrolou dodržování této směrnice jsou pověřeni IT manažeři součástí JU a všichni správci ICT součástí JU, případně zaměstnanci určení ředitelem ISMS JU, ředitelem součásti či děkanem fakulty. 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 nebo studijních povinností.

SEZNAM PŘÍLOH

Označení přílohy	Název přílohy
ISMS-012-P1	BI-Řešení (schéma)
ISMS-012-P2	BI-Hlášení

SOUVISEJÍCÍ DOKUMENTY (platné v době vydání směrnice)

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
ISO/IEC TR 18044/ ISO/IEC TR 18044	Řízení bezpečnostních incidentů (Information technology - Security techniques - Information security incident management)
Zákon 101/2000 Sb.	O ochraně osobních údajů a pozdější předpisy
Zákon č. 121/2000 Sb.,	Autorský zákon
Vyhláška č. 523/2005 Sb.	Vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi
R168/2011	Opatření rektora k uplatnění a zavádění jednotného identifikačního a přístupového systému na JU
R 202/2012	Opatření rektora JU ke stanovení organizace požární ochrany na JU
R 131/2009	Opatření rektora JU – Provozní řád REK a FF
R 95/2007	Opatření rektora - Užívání PC, SW, NET
ŘCIT 2/2007	Opatření ředitele CIT – Nakládání s daty získanými kamerovým systémem
ISMS-001	Politika ISMS JU
ISMS-002	Celková bezpečnostní politika JU
ISMS-003	Provozní postupy
ISMS-006	Antivirová ochrana počítačů JU
ISMS-007	Správa a bezpečnost provozu počítačů
ISMS-008	Správa a bezpečnost počítačové sítě JU
ISMS-010	Homeworking
ISMS-011	Politika fyzické bezpečnosti
Správci ICT (AVO,PC,sítě) + BS+ ITM -	https://isms.jcu.cz/kontakty