Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-023**
Název dokumentu:	**Politika řízení kontinuity činností**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Rozsah působnosti bezpečnostní politiky: • zavedení systému kontinuity činností (Business continuity management – BCM) • vedená dokumentace • zavedení a provozování systému BCM • strategie, testování, údržba, zdokonalování dle PDCA
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 6, 15
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	4 + 0
Verze:	1.1
Význam a benefity:	Mezi přínosy zavedení této sekce bezpečnostní politiky patří zejména • zvýšení odolnosti JU proti narušení provozu • snížení dopadů mimořádných událostí, havárií a krizových stavů • zajištění klíčových procesů i za krizového stavu • zvýšení důvěryhodnosti univerzity.
Uložení:	Sekce kyberbezpečnosti na Wiki JU
Ruší dokumenty:	-
Zpracovatel:	Manažer KB JU
Přezkoumal:	Výbor pro kybernetickou bezpečnost JU
Schválil:	Výbor pro kybernetickou bezpečnost JU

Informační vyhlášení

JU má zpracován plán kontinuity, který zohledňuje podstatná rizika, která by mohla nepříznivě ovlivnit IT systémy a služby (viz analýza rizik) a program testování Plánu kontinuity.

Politika kontinuity činností je náležitě oznámena a vztahuje na všechny příslušné zaměstnance, a případně na poskytovatele služeb. Je součástí školení dotčených zaměstnanců.

a) Práva a povinnosti zúčastněných osob

Osoby dotčené bezpečnostním incidentem mají své zapojení/spoluúčast do obnovy služeb definováno v dokumentech „Eskalační politika“ a „Incident handling“.

Osoby dotčené obnovením aktiva, podaktiva jsou definovány v seznamu aktiv a podpůrných aktiv.

Dále jsou do zúčastněných osob zahrnuty osoby a orgány zastávající bezpečnostní role.

Výše uvedené dokumenty určují úlohy a povinnosti osob dle typu scénáře incidentu (např. chyby, poruchy, kybernetické útoky):

- komunikaci a spolupráci s dalšími osobami, příslušnými zainteresovanými subjekty za účelem účinné reakce na incident a obnovy provozu po incidentu;
- poskytnutí včasných informací nadřízeným i podřízeným, spolupracujícím, majících také vliv na třetí strany (např. zákazníky, ostatní uživatele, příslušný orgán dohledu) podle potřeby a v souladu s platnými předpisy.

Není-li předem určen vedoucí řešení nápravy incidentu, je to manažer kybernetické bezpečnosti.

b) Cíle řízení kontinuity činností

Cílem plánů je efektivní (rychlost/náklady při dodržení integrity a důvěrnosti):

1. stanovení dostupnosti procesů a činností, funkcí, úloh a IT aktiv, které jsou těmito riziky ohroženy,
2. obnova klíčových/kritických IT služeb,
3. stanovení potřebné doby obnovy,
4. určení kritických bodů obnovy.

1. minimální úroveň poskytovaných služeb

JU má zpracován aktuální seznam „provozně kritických“ služeb (VISů a dalších), u nichž je veden seznam potřebných funkčních IT aktiv a podpůrných aktiv.

2. doba obnovení chodu

Určení kategorie služby „provozně kritická“ je dáno přípustnou kritickou lhůtou pro obnovení IT služby, zároveň s ohledem na potřebnou maximální dobu pro zprovoznění všech potřebných aktiv a podpůrných aktiv.

3. bod obnovení dat

Plán kontinuity činnosti je zaveden tak, aby na JU byla zajištěna, přiměřená reakce na případné scénáře selhání v rámci

- cílové doby obnovy (maximální doba, během níž musí být po incidentu obnoven systém nebo proces),
- a cílového bodu obnovy (maximální lhůta, během níž je přijatelná ztráta dat v případě incidentu na předem definované úrovni služeb).

c) Politika řízení kontinuity činností pro naplnění cílů kontinuity

Plány zahrnují potřebné lidské i materiální zdroje, interní i externí. Včetně způsobu jejich koordinace.

Plány by měly obsahovat i hlediska různých scénářů, včetně extrémních, ale věrohodných scénářů a scénářů kybernetických útoků, a posuzování potenciálních dopadů těchto scénářů. Na základě těchto scénářů by mělo být vyhodnoceno, jak je zajištěna kontinuita systémů a služeb IT, jakož i bezpečnost informací.

Plány jsou pravidelně kontrolovány a ověřovány, a jsou obsahem školení administrátorů, správců a jsou testovány.

d) Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik

JU vedle analýzy rizik, pravidelně posuzuje možná rizika z proběhlých bezpečnostních incidentů s ohledem na kontinuitu její činnosti.

Proběhlé bezpečnostní incidenty, vedle svého okamžitého dopadu na JU, mohou představovat vznik nového způsobu pro další navazující incident, který by mohl mít ještě větší dopady.

Potenciál proběhlých incidentů a schopnost detekce jejich eskalace jsou brány v úvahu při analýze rizik.

e) Určení a obsah potřebných plánů kontinuity a havarijních plánů

Pro efektivní řešení mimořádných událostí (nečekaná událost, kdy preventivní opatření selžou) s kritickým dopadem na univerzitu (viz analýza rizik, analýza dopadů) má JU veden „**Plán kontinuity**“ (plán pro zachování provozu klíčových IT služeb), (Business Continuity Plan – dále jen **BCP**).

Předpoklady a obsah pro stanovení BCP:

- podpora managementu
- stanovení cílů BCP
- přidělení odpovídajících zdrojů
- stanovení odpovědností a povinností
- posilování povědomí o významu BCP a školení.

Cíle BCP:

- v okamžiku havárie budou všichni zodpovědní pracovníci vědět, co mají dělat (kde hledat informace), koho kontaktovat, jaké služby a v jakém pořadí obnovovat.
- na základě předchozí analýzy jim bude umožněno soustředit se v okamžiku havárie na obnovu nejkritičtějších procesů či zachování aktiv.
- popsat, jak vytvořit takové postupy a prostředí, které umožní zajistit kontinuitu a obnovu klíčových procesů a činností JU v požadovaných časech a na předem stanovené minimální úrovni, v případě jejich narušení nebo ztráty.
- zajistit, aby v určitém čase od incidentu byl obnoven provoz na určité úrovni.

BCP jsou vedeny pro jednotlivé kritické činnosti JU a detailně popisují postupy k zajištění kontinuity provozu (v přechodném období) a k návratu do běžného provozu.

Součástí BCP jsou plány obnovy dílčích aktiv – "**Havarijní plány**" obnovy ICT (Disaster recovery plan – dále jen **DRP**).

Oblasti pro DRP:

- selhání IS – narušení obvyklého chodu JU až do té míry, kdy je potřeba náhradních služeb k zajištění chodu a snížení dopadů.
- výpadek napájení
- výpadek klimatizace v datacentru
- selhání datové sítě
- napadení hackerem
- výpadek internetu
- napadení virem
- zašifrování dat
- selhání hardwaru
- živelné pohromy, vyplavení nebo požár.

Na BCP a DRP může podrobněji navazovat "**Systém řízení kontinuity činností**" (Business continuity management system – **BCMS**), který prosazuje procesní přístup k implementaci, provozování, monitorování, přezkoumávání a zlepšování všech činností životního cyklu BCM.

f) Postupy pro realizaci opatření vydaných Úřadem

Regulační opatření vydává Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) na základě zhodnocení působení konkrétních hrozeb a jejich dopadů.

Opatření mají tři stupně: varování, ochranné opatření a reaktivní opatření.

Všechny tři stupně opatření je potřeba posuzovat v souvislostech analýzy rizik a podle stupně provést příslušné nebo povinné kroky.

Způsob plnění nebo doporučený postup realizace regulačního opatření je nedílnou součástí operativní části vyhlášení.

Postupy pro realizaci (opatření) ve vztahu k úřadu:

- Varování – mimo vyhodnocení dopadu v analýze rizik, není potřeba zpětná reakce
- Ochranné opatření obecné povahy – je rozšířeno o povinnost jej provést do určitého termínu
- Reaktivní opatření – je rozšířeno o povinnost reagovat úřadu prohlášením o jeho splnění.

Postupy pro realizaci (opatření) na JU:

Způsob plnění regulačních opatření obsahuje oblasti:

- Seznam dílčích opatření
- jejich časová posloupnost
- popis postupů k jejich realizaci
- vymezení odpovědnosti
- subjekty, které se budou na realizaci jednotlivých opatření podílet
- případné materiálně technické zabezpečení.

Každá oblast obsahuje konkrétní aktuální údaje: názvy, jména, místa, datumy atp. Postupy musí být zpracovány tak, aby umožnily bezproblémové zavedení potřebných regulačních opatření a jejich efektivní použití.

Historie revizí

Historie revizí je uvedena u souboru této politiky na Wiki JU.