SBÍRKA ROZHODNUTÍ A OPATŘENÍ ŘEDITELE CIT
JIHOČESKÉ UNIVERZITY V ČESKÝCH BUDĚJOVICÍCH

číslo: **CIT_01** datum: **1. 11. 2026**

Opatření ředitele CIT, kterým se stanoví postup pro krizovou komunikaci Centra informačních technologií při kybernetickém bezpečnostním incidentu a jiné mimořádné IT události

Článek 1
Úvodní ustanovení a účel opatření

1. Toto opatření upravuje postup Centra informačních technologií Jihočeské univerzity v Českých Budějovicích (dále jen „CIT“) při krizové komunikaci související s řešením kybernetického bezpečnostního incidentu nebo jiné mimořádné IT události (výpadku, poruchy, bezpečnostního incidentu apod.) na Jihočeské univerzitě v Českých Budějovicích (dále jen „JU“).
2. Toto opatření stanoví, co dělat v prvních minutách a hodinách po zjištění bezpečnostního incidentu, komu a jak incident hlásit, jakým způsobem komunikovat uvnitř JU i navenek, tak aby nedošlo k prozrazení citlivých informací, ztrátě důkazů nebo poškození dobrého jména JU. Toto opatření nenahrazuje technické postupy, ani povinnosti vyplývající z jiných vnitřních předpisů JU, upravuje výhradně otázky komunikace v době krize.
3. Opatření je závazné pro všechny zaměstnance CIT a spolupracující útvary JU uvedené v čl. 3 a v čl. 8 tohoto opatření.
4. CIT při plnění povinností podle tohoto opatření vychází zejména z těchto právních předpisů a vnitřních norem JU (vždy v jejich aktuálně účinném znění):
   a) zákon č. 264/2025 Sb., o kybernetické bezpečnosti, a jeho prováděcí právní předpisy (dále jen „ZoKB“),
   b) zákon č. 110/2019 Sb., o zpracování osobních údajů,
   c) zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách),
   d) zákon č. 480/2004 Sb., o některých službách informační společnosti,
   e) zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), je-li dotčen obsah zveřejňovaných sdělení,
   f) Statut Jihočeské univerzity v Českých Budějovicích,
   g) opatření rektora č. R 634, kterým se vydává Organizační řád Rektorátu JU (vymezení působnosti CIT a jeho ředitele),
   h) opatření rektora č. R 632, k posilování odolnosti vůči nelegitimnímu ovlivňování na JU (hlášení bezpečnostních incidentů, čl. 6),
   i) zákon č. 262/2006 Sb., zákoník práce.
5. Vysvětlení použitých zkratek a pojmů je uvedeno v Příloze č. 7.

Článek 2
Základní postup v případě detekce krize

1. Sběr ověřených faktů, první reakce a zhodnocení závažnosti – viz článek 4, tab. 1.
2. Svolání řešitelského či krizového týmu (v případě úrovně 4 dle tab. 1). Jednotlivé role v týmu jsou uvedeny v tab. 2 v článku 8, konkrétní kontakty pak v příloze č. 1 – Kontaktní list. Svolání týmu je provedeno fyzicky či přes níže uvedené kanály. Rozhodnutí o úrovni transparentnosti a nutnosti případné vnější komunikace (v případě úrovně 4 - viz tab. 1).
3. Postup dle úrovně závažnosti incidentu (rozlišení v tab. 1 níže) a jednotlivé postupy níže.
4. Zahájení případné komunikace vůči cílovým skupinám.
5. Návrat do předkrizového režimu, vyhodnocení a nápravy.
6. Zaměstnanec CIT, který incident zjistí, a koordinátor krizového týmu postupují v prvních 30 minutách podle kontrolního seznamu v Příloze č. 3. Provedené kroky se v seznamu odškrtávají a zapisuje se čas jejich provedení.
7. Stručný souhrn tohoto opatření pro rychlou orientaci správců CIT je uveden v Příloze č. 6. Je určen k vytištění a nenahrazuje text opatření.

Článek 3
Odpovědnost a koordinace

1. Za koordinaci krizové komunikace při incidentu odpovídá ředitel CIT, případně jím pověřený zástupce (vedoucí USII, USKZ nebo USIS – viz Příloha č. 1 - Kontaktní list).
2. Postup podle tohoto opatření aktivuje ředitel CIT nebo jeho zástupce neprodleně po potvrzení incidentu, a to podle úrovně jeho závažnosti dle čl. 4.
3. Koordinátor krizového týmu, kterým je ředitel CIT nebo jeho zástupce, svolává krizový komunikační tým, řídí rozhodování, schvaluje obsah sdělení a je jediným styčným bodem mezi technickým (řešitelským) týmem a komunikačním týmem.
4. O strategii vnější komunikace u incidentů úrovně 4 rozhoduje rektor JU, případně vystupuje společně s tiskovým mluvčím JU (viz Příloha č. 1 - Kontaktní list).
5. Právní posouzení (GDPR, ohlašovací povinnosti, právní rizika sdělovaných informací) zajišťuje Útvar právní Rektorátu JU ve spolupráci s pověřencem pro ochranu osobních údajů (dále jen „pověřenec“) a s manažerem kybernetické bezpečnosti JU (dále též jen „MKB“) (viz Příloha č. 1 - Kontaktní list).
6. Navenek jménem JU komunikuje výhradně tiskový mluvčí JU, rektor JU a MKB dle platné legislativy; ostatní osoby se řídí zásadami podle čl. 5 až 10 tohoto opatření.

Článek 4
Rozdělení události dle úrovně závažnosti

1. Incidenty se pro účely tohoto opatření dělí podle závažnosti a dopadu do čtyř úrovní podle tabulky č. 1. Při pochybnostech o zařazení se incident zařazuje vždy do vyšší uvažované úrovně.
2. Úroveň závažnosti určuje, zda komunikace zůstává pouze vnitřní, nebo je nutné zapojit i vnější komunikaci – krizový komunikační tým, MKB a tiskového mluvčího JU.
3. Pro účely tohoto opatření se rozumí:
    a. vnitřní komunikací komunikace určená zaměstnancům, studentům a dalším uživatelům IT služeb JU, správcům IT součástí, vedení JU a členům krizového komunikačního týmu, včetně informování přes aplikaci vypadky.jcu.cz a záznamů v ServiceDesku;
    b. vnější komunikací komunikace určená subjektům mimo JU, zejména médiím a veřejnosti, a plnění ohlašovacích povinností vůči orgánům veřejné moci (NÚKIB, ÚOOÚ).

Tabulka 1 - Stanovení úrovní (závažnosti) incidentů a případné aktivace krizového komunikačního týmu.

Úrovně závažnosti incidentů		
Úroveň	Kritérium	Rozsah komunikace
1 (Nízká)	Lokální porucha bez dopadu na uživatele mimo CIT (řeší se běžným provozem)	**Bez zvláštní komunikace;** případně informace vedoucímu a dotčeným kolegům; záznam do SD
2 (Střední)	Výpadek jedné služby s dopadem na část uživatelů (např. Moodle, Verso, iFIS)	**Vnitřní komunikace** – dotčení uživatelé, správci IT součástí a vedení CIT; záznam do SD.
3 (Vysoká)	Výpadek klíčové služby (AD, síť, M365, IS/STAG, výpadek web. stránek) s dopadem na celou univerzitu, nebo podezření na bezpečnostní incident či únik dat.	**Vnitřní komunikace –** dotčení uživatelé, správci IT součástí a vedení CIT, v případě potřeby všichni uživatelé JU; při podezření na bezpečnostní incident též MKB; záznam do SD
4 (Kritická)	Např. ransomware závažnějšího rozsahu, závažný DoS/DDoS útok, potvrzený únik dat většího rozsahu, závažný incident nahlašovaný NÚKIB/ÚOOÚ a zásah orgánů činných v trestním řízení, které výrazně omezí služby univerzity	**Plná aktivace** – krizový tým, výbor KB, vedení univerzity, právník, tiskový mluvčí, informování NÚKIB/ÚOOÚ dle zákonné lhůty – MKB / pověřenec; záznam do SD.

Postup aktivuje ředitel CIT nebo jeho zástupce ihned po potvrzení incidentu. Úroveň závažnosti určuje, zda komunikace zůstává pouze vnitřní, nebo se zapojuje i vnější komunikace – krizový tým, MKB a tiskový mluvčí.

Článek 5
Postupy komunikace dle jednotlivých úrovní závažnosti 1-3 (dle tab. 1)

(1) Nízká úroveň

Příklad: lokální porucha bez dopadu na uživatele mimo CIT, řešená běžným provozem.

1. Bez zvláštní komunikace;
2. případně informace vedoucímu a dotčeným kolegům/správcům;
3. záznam do ServiceDesku.

(2) Střední úroveň

Příklad: výpadek jedné služby s dopadem na část uživatelů (např. Moodle, Verso, iFIS).

1. Informace dotčeným uživatelům;
2. https://vypadky.jcu.cz – IT správci, uživatelé IS;
3. vedení CIT;
4. záznam do ServiceDesku.

(3) Vysoká úroveň

Příklad: výpadek klíčové služby (AD, síť, M365, IS/STAG), výpadek webových stránek s dopadem na celou univerzitu, nebo podezření na bezpečnostní incident.

1. Vnitřní komunikace, v případě potřeby všichni uživatelé JU;
2. https://vypadky.jcu.cz – IT správci, uživatelé IS;
3. vedení CIT;
4. při podezření na bezpečnostní incident informovat MKB (a pověřence, jde-li o osobní údaje);
5. záznam do ServiceDesku.

Článek 6

Základní pravidla a chování pro incidenty úrovně 4 (kritická)

Příklady
• Ransomware závažnějšího rozsahu; • potvrzený únik dat většího rozsahu; • závažný incident nahlašovaný na NÚKIB/ÚOOÚ; • zásah orgánů činných v trestním řízení, které výrazně omezí služby univerzity.

Následující zásady platí prioritně pro incidenty klasifikované jako úroveň 4 a musí je znát každý zaměstnanec CIT bez ohledu na svou pracovní pozici:

1. **Neinformuj veřejnost ani média.** Komunikace navenek jde výhradně přes oprávněné osoby dle čl. 3 odst. 6 (tiskový mluvčí JU, rektor JU a MKB).
2. **Nepiš o incidentu na běžné univerzitní kanály** (Teams, e-mail), pokud existuje podezření, že útočník má přístup k těmto systémům – použij záložní komunikaci (viz Příloha č. 2).
3. **Nemaž, nerestartuj, nepřeinstalovávej** – nic bez pokynu odpovědných osob (v případě podezření na cizí zavinění) - ničíš tím forenzní stopy.
4. **Zapisuj si časovou osu** (co jsi udělal/a, co jsi zjistil/a) - bude potřeba pro NÚKIB hlášení i pro krizový tým.
5. **Mlč navenek, mluv dovnitř**
    - Informuj rychle a přesně nadřízeného.
    - Nekomunikovat s médii, studenty ani veřejností žádným způsobem – to mohou jen oprávněné osoby dle čl. 3 odst. 6 (tiskový mluvčí JU, rektor JU a MKB).
    - Nepotvrzovat ani nevyvracet detaily incidentu mimo krizový tým.
    - Neposílat logy/screenshoty mimo určené bezpečné úložiště a kanály komunikace.
    - Neuzavírat incident jako „vyřešený" bez potvrzení odpovědných osob.

Článek 7
Postupy komunikace pro incidenty úrovně 4 (dle tab. 1)

Podoba komunikace
Vnitřní komunikace • Výbor KB; • **krizový tým** (ředitel CIT, vedení univerzity, právník, tiskový mluvčí); • vnitřní komunikace, vedení CIT a v případě potřeby všichni uživatelé JU - https://vypadky.jcu.cz; • záznam do ServiceDesku. **Vnější komunikace** • Dle právních předpisů oznámení incidentu NÚKIB, resp. ÚOOÚ atd. dle zákonné lhůty – Manažer kybernetické bezpečnosti JU, pověřenec; • navenek jménem JU komunikuje výhradně tiskový mluvčí JU, rektor JU a MKB dle platné legislativy; ostatní osoby se řídí zásadami podle čl. 5 až 10 tohoto opatření.

Obsah vnější krizové komunikace

- JU musí vždy hovořit jedním hlasem – **navenek informuje pouze tiskový mluvčí** či rektor.
- Co se navenek nesmí sdělovat:
    - Technické detaily zranitelnosti nebo způsobu útoku (dokud nejsou uzavřené – riziko zneužití);
    - nepotvrzený rozsah úniku dat nebo konkrétní jména dotčených osob;
    - odhady příčiny incidentu, dokud nejsou ověřené technickým týmem;
    - cokoli, co může ovlivnit případné trestní řízení nebo forenzní šetření.

Postup úrovně závažnosti 4:

1. Informovat vedoucí pracovníky – ředitel CIT, vedoucí USII, USKZ a USIS (viz Příloha č. 1), MKB.
2. Informovat pracovníky, kteří budou při řešení incidentu přímo zasahovat.
3. Informovat ostatní dotčené pracovníky a uživatele JU (https://vypadky.jcu.cz).
4. Koordinátor krizového týmu předá tiskovému mluvčímu a rektorovi ověřené shrnutí situace.
5. Tiskový mluvčí (viz Příloha č. 1 - Kontaktní list) případně vydá v případě dotazů z vnějšku o incidentu úrovně 4 tzv. Holding Statement (vzor v Příloze č. 5) – potvrzení, že JU o problému ví a řeší ho, i když ještě nejsou známy všechny detaily.
6. Další aktualizace se vydávají při zásadní změně stavu, nikdy dříve, než jsou informace ověřené.
7. Po vyřešení incidentu se vydá závěrečné shrnutí a poučení (je-li relevantní pro veřejnost).

Článek 8
Krizový komunikační tým a kontakty

Krizový komunikační tým tvoří zejména tyto role:

- **Vedoucí týmu (koordinace)** – ředitel CIT, jeho zástupce: svolává tým, řídí rozhodování, schvaluje obsah sdělení, je jediným styčným bodem mezi technickým a komunikačním týmem;
- **rektor JU** – schvaluje strategii komunikace u incidentů úrovně 4, případně vystupuje spolu s tiskovým mluvčím;
- **právník, pověřenec, MKB** – posuzují dopad incidentu z hlediska ochrany osobních údajů nebo ZoKB, posuzují právní/technická rizika sdělovaných informací, pověřenec a MKB plní ohlašovací povinnosti;
- **odborníci** – odborní pracovníci CIT, případně externí poradci;
- **tiskový mluvčí JU** – primární oficiální hlas navenek vůči médiím, veřejnosti a na sociálních sítích.

Tabulka 2 – Členové krizového komunikačního týmu.

Členové krizového komunikačního týmu	
Působnost	**Osoba**
Koordinace týmu	**CIT ředitel**
	Zástup: CIT USII – vedoucí
	Zástup: CIT USKZ – vedoucí
	Zástup: CIT USIS – vedoucí
Kybernetická bezpečnost	**Manažer kybernetické bezpečnosti**
Vedení	**Rektor JU**
Styk s veřejností	**Tiskový mluvčí JU**
	Zástup: Útvar marketingu – vedoucí
Právní stránka	**Útvar právní Rektorátu – vedoucí**
	Zástup: Útvar právní Rektorátu, pověřenec
Dopad na ochranu osobních údajů	**Pověřenec**
	Zástup: Útvar právní Rektorátu JU

Konkrétní kontakty jsou uvedeny v příloze číslo 1 – Kontaktní list krizového komunikačního týmu.

Článek 9
Náhradní řešení pro krizové situace

Pro případ přerušení lokální konektivity (wifi, internetové připojení):

1. Zapnout mobilní data, Bluetooth i WiFi, u tabletů vypnout případný režim „Letadlo“;
2. vypnout režimy nerušit a jejich případné automatické zapínání, jinak si dát výjimky pro členy týmu;
3. připravené nabité mobilní zařízení, případně mít k dispozici powerbanku a nabíječku.

Pro rozsáhlý výpadek elektřiny:

1. Pro nouzový vstup na pracoviště bez karet, bez elektřiny jsou určeny fyzické univerzální klíče pro přístup do vchodových dveří CIT, do serveroven, krizové místnosti, záložní krizové místnosti. Tyto klíče jsou na recepci v přízemí budovy Rektorátu a případně také u vedoucího Útvaru správy a údržby budov Rektorátu.

Článek 10
Kanály pro vnitřní komunikaci a obsah komunikace

1. Primárními kanály pro vnitřní komunikaci jsou:
    a. Aplikace pro rozesílání informací o výpadcích a odstávkách: https://vypadky.jcu.cz.
    b. Záznam vždy v ServiceDesku na adrese https://servicedesk.jcu.cz, v případě nedostupnosti v listinné podobě a do ServiceDesku bude vložena po jeho zprovoznění.
    c. Kontakty a telefony (viz Příloha č. 1), příp. MS Teams
2. Každé sdělení o incidentu určené pro vnitřní komunikaci (zejména zpráva zveřejněná na vypadky.jcu.cz a e-mail či jiné oznámení uživatelům a správcům IT součástí) musí obsahovat čtyři body: co se stalo, jaký je dopad, co se dělá pro nápravu, a co se očekává od příjemce (např. nehlásit duplicitně poruchu, nepoužívat postižený systém, kam se obracet s dotazy). Vzory sdělení pro vnitřní komunikaci jsou uvedeny v Příloze č. 4.
3. Nejsou-li primární kanály dostupné (např. při podezření na kompromitaci nebo při výpadku sítě), použijí se záložní kanály uvedené v příloze č. 2.

Článek 11
Závěrečná ustanovení

1. Toto opatření nabývá platnosti a účinnosti dne 1. 11. 2026.
2. Přílohy tohoto opatření se aktualizují bez nutnosti vydání nového opatření, vždy se zaznamenáním data verze přílohy.

Bc. Eduard Krlín
ředitel

Eduard Krlín
Digitálně podepsal Eduard Krlín
Datum: 2026.10.30 08:20:36 +01'00'

Centrum informačních technologií
Jihočeská univerzita v Českých Budějovicích

Zpracoval: Robert Kroupa, Centrum informačních technologií JU

Rozdělovník: vedení JU, pracovníci CIT JU, Rada ICT, MKB, tiskový mluvčí JU, Útvar právní JU, pověřenec

Přílohy:

Příloha č. 1 – Kontaktní list krizového komunikačního týmu CIT

Příloha č. 2 – Záložní komunikační kanály pro vnitřní komunikaci

Příloha č. 3 – Kontrolní seznam prvních 30 minut

Příloha č. 4 – Vzory sdělení CIT

Příloha č. 5 – Vzor možné podoby tiskového prohlášení (tzv. Holding Statement)

Příloha č. 6 – Souhrn tohoto opatření

Příloha č. 7 – Vysvětlivky některých pojmů