CIT – SOUHRN OPATŘENÍ K POSTUPU PŘI INCIDENTU / VÝPADKU

Výtah z Opatření ředitele CIT_01 – Postup pro krizovou komunikaci CIT. Při pochybnostech o závažnosti vždy zařaď incident do vyšší úrovně.

Úrovně závažnosti incidentů			
Úroveň	Kritérium – příklad	Co udělat	Komu hlásit a kam zapsat
1 (Nízká)	Lokální porucha bez dopadu na uživatele mimo CIT	**Bez zvláštní komunikace**, řeší se běžným provozem.	• info vedoucímu a dotčeným kolegům • **záznam do SD**
2 (Střední)	Výpadek jedné služby s dopadem na část uživatelů (např. Moodle, Verso, iFIS)	• **pošli info** přes https://vypadky.jcu.cz • **informuj vedení CIT**	• vypadky.jcu.cz (uživatelé, IT správci) • **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.	• **pošli info** přes https://vypadky.jcu.cz (dle potřeby všichni uživatelé JU). • **Informuj vedení CIT.** • **Při podezření na incident informuj i MKB.**	• vypadky.jcu.cz (uživatelé, IT správci) • **vedení CIT, MKB** • **záznam do SD**
4 (Kritická)	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	• **NIC NEMAŽ, NERESTARTUJ, NEPŘEINSTALOVÁVEJ!** • Informuj IHNED ředitele CIT či zástupce. • Zapisuj časovou osu (co, kdy, kdo zjistil/udělal). • **Mlč navenek – nekomunikuj s médii/veřejností.**	• **ředitel CIT /** koordinátor • **MKB / pověřenec** → NÚKIB/ÚOOÚ dle lhůty • **záznam do SD**

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

Neinformuj veřejnost ani média. Komunikace navenek jde výhradně přes oprávněné osoby dle čl. 3 odst. 6 (tiskový mluvčí JU, rektor JU a MKB).

Nepiš o incidentu na běžné univerzitní kanály (Teams, e-mail), pokud existuje podezření, že útočník má přístup k těmto systémům – použij záložní komunikaci.

Nemaž, nerestartuj, nepřeinstalovávej nic bez pokynu odpovědných osob (v případě podezření na cizí zavinění) - ničíš tím forenzní stopy.

Zapisuj si časovou osu (co jsi udělal/a, co jsi zjistil/a) - bude potřeba pro NÚKIB hlášení i pro krizový tým.

Mlč navenek, mluv dovnitř. Navenek mluví jen tiskový mluvčí (příp. rektor či MKB). Nepotvrzuj, nevyvracej, neposílej logy/screenshoty mimo bezpečné úložiště.

Informuj rychle a přesně nadřízeného.

Neuzavírej incident jako „vyřešený“ bez potvrzení odpovědných osob.

Primární komunikační kanály:

- **https://vypadky.jcu.cz (hlášení výpadků)**
- **https://servicedesk.jcu.cz (SD – záznam každého incidentu)**
- **Kontakty a telefony, příp. MS Teams → Příloha č. 1**

Záložní komunikační kanály:

- **mobilní komunikace – kontakty, osobní setkání - viz Příloha č. 1 - Kontaktní list**