**Příloha č. 10**

# Incident Management

# OBSAH

# ČÁST I. ÚVODNÍ USTANOVENÍ

## Kapitola 1 DEFINICE POJMŮ

**Bezpečnostní incident**: událost v IS, která způsobila narušení důvěrnosti, integrity, dostupnosti nebo neodmítnutelnosti informace v důsledku selhání bezpečnostních opatření nebo porušení bezpečnostní politiky.

**Bezpečnostní událost:** událost v IS, která může způsobit narušení důvěrnosti, integrity, dostupnosti nebo neodmítnutelnosti informace.

**HelpDesk:** kontaktní místo pro uživatele informačního systému MD**,** určené pro předávání informací o incidentech, požadavcích na úpravy aplikací a podobně.

**Incident:** jakákoli odchylka od popsaného stavu, resp. výpadek služby.

**Informační systém (IS):** informační infrastruktura, soustava aplikací, organizačních opatření, procedur a souvisejících služeb pro tvorbu, získávání, zpracování, ukládání a prezentaci informací.

**Informační aktivum:** jakákoli informace nebo prostředek pro práci s ní, který má pro MD nějakou hodnotu.

## Kapitola 2 ROZSAH PŮSOBNOSTI

Tato příloha Bezpečnostní politiky informací MD (dále jen BPI MD) popisuje pravidla, zásady a principy pro řízení incidentů IS MD. Řídí se jí všichni zaměstnanci MD. Externí subjekty jsou zavázány k plnění této přílohy smluvně.

Bezpečnostní incidenty jsou řešeny a řízeny stejně jako jiné incidenty s tím, že jejich specifika jsou uvedena ČÁSTI IV. („Bezpečnostní incident a jeho specifika“) této přílohy BPI MD.

# ČÁST II. ROLE, ODPOVĚDNOSTI A PRAVOMOCI

**Ředitel Odboru ICT** zajišťuje fungování systému pro evidenci průběhu řešení incidentů (HelpDesk MD).

**Manažer KB**:

- řídí řešení bezpečnostních incidentů,
- dohlíží na implementaci případných opatření,
- vede evidenci všech bezpečnostních incidentů.

**Správce IS** dozoruje řešení incidentů.

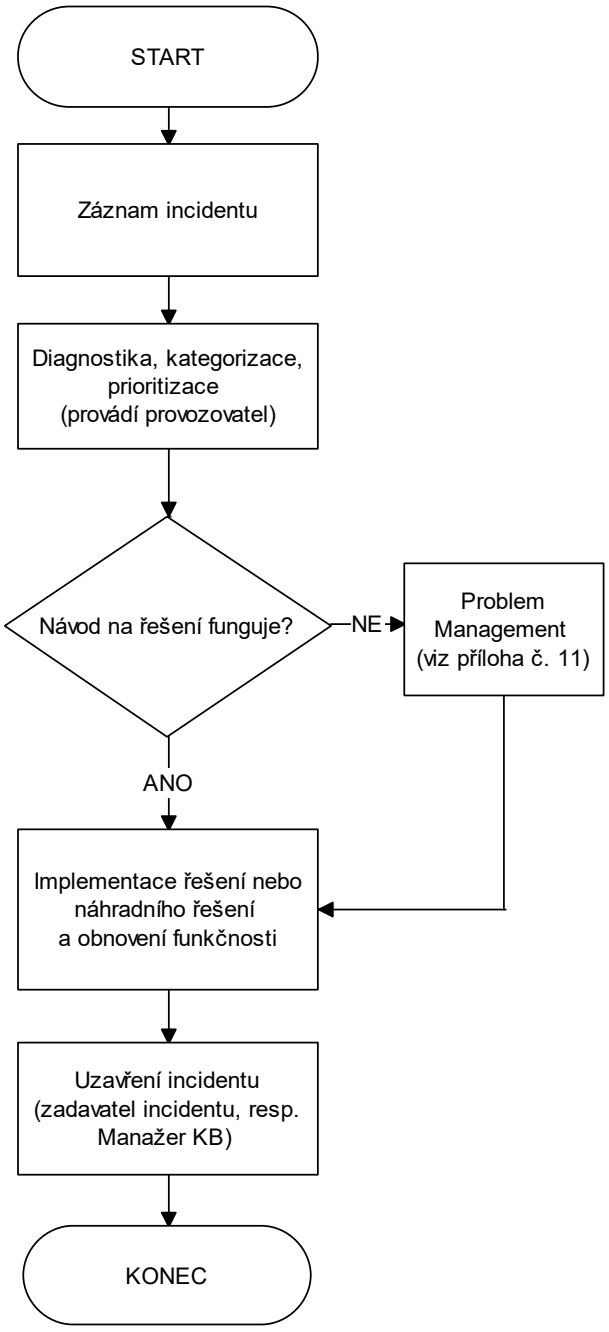
**Provozovatel IS:**

- hlásí incidenty definovaným způsobem MD,
- řeší incidenty ve své působnosti,
- vede evidenci všech bezpečnostních incidentů v rámci své působnosti.

# ČÁST III. SCHÉMA INCIDENT MANAGEMENTU

Proces Incident Managementu musí respektovat následující schéma.

Obrázek 1: Schéma Incident Managementu




Pravidla:

1. Každý uživatel a administrátor IS musí mít definované jedno místo, kam hlásí incidenty.
2. V rámci zjednodušení terminologie se od počátku hovoří o „incidentu“, ačkoli se na začátku jedná o „událost podezřelou z incidentu|“ a v průběhu řešení (zejména pak v průběhu diagnostiky) se může ukázat, že se o incident nejedná.
3. Prvotní kategorizace, zda se jedná o bezpečnostní incident, je v odpovědnosti řešitele incidentu, který provádí jeho diagnostiku. Ten si může vyžádat součinnost ostatních dodavatelů, podílejících se na provozu daného IS, Manažera KB atd. Tuto kategorizaci je nutné brát jako návrh. Konečné potvrzení že se jedná o bezpečnostní incident je na správci daného IS.
4. Manažer KB musí mít přístup ke všem incidentům, aby mohl z metodického pohledu kontrolovat jejich správnou kategorizaci.

Poznámka:

V popisu nejsou podrobněji řešeny jednotlivé úrovně řešení incidentu (1. úroveň a další expertní úrovně). Bezpečnostní politika nastavuje základní pravidla, zásady a principy, kterými se proces řízení incidentů musí řídit. Rozpracování řízení incidentů do většího detailu je věcí implementace tohoto procesu v rámci jednotlivých IS.

# ČÁST IV. BEZPEČNOSTNÍ INCIDENT A JEHO SPECIFIKA

Požadavky na proces Incident Management z pohledu bezpečnosti informací:

- incident se stává bezpečnostním incidentem ve fázi diagnostiky – pokud nahlášený incident splňuje definici bezpečnostního incidentu, je povinností diagnostikujícího pracovníka tento označit za bezpečnostní,
- Manažer KB hlásí bezpečnostní incident Národnímu úřadu pro kybernetickou a informační bezpečnost podle jím stanovených pravidel.

- řešení všech bezpečnostních incidentů řídí Manažer KB (v jeho pravomoci je překvalifikování bezpečnostního incidentu na bezpečnostní událost),
- vyřešení bezpečnostního incidentu potvrzuje také Manažer KB.

Diagnostikující pracovník provozovatele musí při kategorizaci bezpečnostních incidentů vycházet z:

- hodnoty a důležitosti incidentem dotčených informačních aktiv,
- dopadů na poskytované IT služby, resp. případných dalších dopadů (bezpečnost informací, zastavení procesů atd.),
- předpokládaných škod.

Kategorie bezpečnostních incidentů:

- **méně závažný** (provozní), při kterém je méně významně narušena bezpečnost IT služeb (potažmo informací) – může **být řešen s nižší prioritou**, **vhodnými prostředky** musí být **omezeno** jeho další šíření a musejí být minimalizovány vzniklé i potenciální škody,
- **závažný**, při kterém je narušena bezpečnost IT služeb (potažmo informací) - **musí být řešen neprodleně**, **vhodnými prostředky** musí být zabráněno jeho dalšímu šíření a musejí být minimalizovány vzniklé i potenciální škody,
- **velmi závažný**, při kterém je přímo a významně narušena bezpečnost IT služeb (potažmo informací) - **musí být řešen neprodleně**, **všemi dostupnými prostředky** musí být zabráněno jeho dalšímu šíření a musejí být minimalizovány vzniklé i potenciální škody.

Řešení všech bezpečnostních incidentů musí být provozovatelem IS zdokumentováno.

# ČÁST V. PŘECHODNÁ USTANOVENÍ

Do doby zajištění technických prostředků a podmínek pro centrální řízení zejména bezpečnostních incidentů je nutné postupovat v co největší možné míře souladu s touto přílohou BPI MD.