Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-002**
Název dokumentu:	**Politika řízení aktiv**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Tato politika se vztahuje na: • všechny zaměstnance JU, • informační aktiva vytvořená nebo používaná v rámci VISu, a • na uživatele těchto aktiv.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 3, 4, 5, 6
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	6 + 4
Verze:	1.1
Význam a benefity:	Tato politika má za cíl stanovit postupy a protokoly podporující účinnou správu aktiv JU, konkrétně zaměřenou na primární a podpůrná aktiva VISu.
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

Lze rozlišit dva druhy aktiv – primární a podpůrná aktiva. Jako aktivum se může chápat vše, co má pro JU hodnotu – informační systémy, výzkum, znalosti atd.

V rámci celkového řízení aktiv je čerpáno z dokumentu průvodce řízení aktiv dle vyhlášky kybernetické bezpečnosti od NÚKIB (příloha č. 1).

a) Identifikace, hodnocení a evidence primárních aktiv

JU vede evidenci aktiv s přiřazenou strategickou hodnotou. Stanovení této hodnoty vychází z analýzy klíčových informací o aktivu, přičemž jsou zohledňovány zejména tyto faktory:

- ekonomické (pořizovací cena, hodnota grantů),
- odborné (význam výzkumu),
- provozní (důležitost a dostupnost informačního systému).

Evidence aktiv JU se provádí v rámci služby správy aktiv (Asset Management).

Evidence výzkumu se provádí v rámci služby či aplikace určené prorektorem pro vědu a výzkum JU.

1. Určení a evidence jednotlivých primárních aktiv včetně určení jejich garanta

Primární aktiva jsou jedinečná (IT služby, systémy, informace, výzkum, …), vycházející z klíčových procesů a činností VVŠ.

Při jejich identifikaci se vychází z dokumentů např.:

- organizačního řádu,
- zakládací listiny,
- legislativních zdrojů,
- smluv, směrnic, příruček, manuálů,
- interních aktů řízení organizace atd.

Pro analýzu a dokumentaci vlastností, závislostí a složení všech aktiv jsou klíčové pohovory s vedoucími odborných útvarů a součástí JU. K těmto pohovorům je možné si přizvat další klíčové zaměstnance JU, kteří figurují v provozu aktiv.

Každé jednotlivé primární aktivum má přiřazeného garanta, v případě služeb technického správce. Tito musí být uvedeni v evidenci primárních aktiv – propojení dotyčné osoby vazbou s primárním aktivem ve službě správy aktiv JU.

Garant zodpovídá za zajištění rozvoje, použití a bezpečnost aktiva. Garanty primárních aktiv bývají nejčastěji pracovníci zastávající role typu vedoucí oddělení, ředitelé odborů, vlastník procesu atd.

Primární aktivum je pro JU jedno z těchto čtyř typů:

- systém;
- informace/agenda;
- výzkum/výzkumná data;

- služba;

Aktiva jsou evidována v systému správy aktiv a evidence obsahuje podrobné údaje. Zejména:

- název aktiva,
- garant aktiva,
- hodnocení aktiva z hlediska důležitosti (DDI – Dostupnost, Důvěrnost, Integrita), včetně detailního hodnocení:
  - důvěrnost (prozrazení): interně v rámci skupiny, interně v rámci organizace, mimo organizaci.
  - integrita: neúmyslná modifikace (chyba), systémová chyba, úmyslná chyba.
  - dostupnost: nefunkčnost po dobu 15 minut, 1 hodiny, 4 hodin, 1 den, 1 týden, 1 měsíc.
- Hodnota aktiva DDI,
  - Hodnota vypočtena z průměru sečtených hodnot DDI.
- strategická hodnota aktiva,
- detailní popis – v případě, že se jedná o typové aktivum tak i specifikace toho, co zahrnuje,
- další informace o aktivu – např. kdo jsou jeho uživatelé, jaké agendy jej využívají, jaká legislativa se aktiva týká atd.

2. Hodnocení důležitosti primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti (DDI)

Hodnocení primárních aktiv se provádí ve službě správy aktiv JU.

Minimální rozsah hodnocení důležitosti primárních aktiv (§4, bod 2 Vyhlášky):

- rozsah a důležitost osobních údajů, zvláštních kategorií osobních údajů nebo obchodního tajemství,
- rozsah dotčených právních povinností nebo jiných závazků,
- rozsah narušení vnitřních řídicích a kontrolních činností,
- poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty,
- dopady na poskytování důležitých služeb,
- rozsah narušení běžných činností,
- dopady na zachování dobrého jména nebo ochranu dobré pověsti,
- dopady na bezpečnost a zdraví osob,
- dopady na mezinárodní vztahy a
- dopady na uživatele informačního a komunikačního systému.

K hodnocení důležitosti aktiv dle DDI, včetně detailního hodnocení, se na JU využívají tabulky v příloze č. 2. Je nutné dodržet jednoznačné vazby mezi používaným způsobem hodnocení důležitosti aktiv a stupnicemi a úrovněmi pro hodnocení důležitosti aktiv.

Při posuzování hodnoty aktiv je nutné uvažovat o nejhorším možném scénáři a nebrat v úvahu bezpečnostní opatření, například:

- výpadek aktiva v den, kdy aktivum provádí důležité procedury
  - Př.: finanční IS v den výplat, IS studijních agend v den státnic, ...

U hodnocení je důležité udržovat konzistentnost a zabránit nadhodnocení či podhodnocení významu primárního aktiva.

Hodnocení DDI je ovlivněno detailním hodnocením. Detail ovlivnění záleží na manažerovi KB a garanta aktiva.

V případě hodnocení primárního aktiva typu *služba* je nutné také zahrnout primární aktiva typu *informace/agenda*, se kterými služba pracuje. Primární aktivum služby následně vždy přebírá nejvyšší hodnoty DDI navázaných primárních aktiv (informací/agend).

Stejné pravidlo platí i pro primární aktivum typu *výzkum* či *systém,* pokud pracují s informacemi/agendami.

V případech, kdy nelze snadno identifikovat primární aktiva přímo z informací/agend zpracovávaných službou, systémem, či výzkumem, a je proto vytvořeno souhrnné primární aktivum patřičného typu zahrnující i tyto informace, hodnotí se toto primární aktivum včetně všech obsažených informací.

b) Identifikace, hodnocení a evidence podpůrných aktiv

Podpůrná aktiva zajišťují existenci primárních aktiv. Bývají sdílená pro více primárních aktiv.

1. Určení a evidence jednotlivých podpůrných aktiv včetně určení jejich garanta

Podpůrná aktiva mohou být společná pro více primárních aktiv.

Podpůrné aktivum (na které spoléhají primární aktiva) je jednoho že šesti typů:

- HW – technické vybavení
- SW – programové vybavení
- Objekty – prostory, budovy
- Komunikační prostředky – infrastruktura
- Lidské zdroje
- Dodavatelé

Při identifikaci podpůrných aktiv je nutné vycházet z architektury systému a potřeby pro funkčnost primárního aktiva. Co se týče míry detailu podpůrných aktiv, JU musí zvolit takový detail, aby byla schopna adekvátně identifikovat a řídit rizika s aktivy spojená.

Aktuální míra detailu pro identifikaci podpůrných aktiv je na úrovni jednotlivých objektů ve službě správy aktiv JU.

K identifikaci podpůrných aktiv je dobré pokládat otázky na tento způsob:

- Co je potřeba k zajištění dostupnosti primárního aktiva?
- Kdo zajišťuje správu, technickou podporu a má povědomí o podpůrných aktivech?
- Kdo jsou uživatelé nebo role využívající primární aktivum a kdo jsou jejich původci?
- Kde jsou primární aktiva umístěna a kdo jsou jejich dodavatelé?
- Kdo je za podpůrné aktivum odpovědný?

Evidence podpůrných aktiv musí obsahovat i jejich garanty. Jelikož jsou to pracovníci, kteří se podílí na provozu, rozvoji, správě a bezpečnosti daného podpůrného aktiva, je často role garanta totožná s rolí správce podpůrného aktiva.

Určení jednotlivých garantů podpůrných aktiv určuje ředitel CIT ve spolupráci manažera kybernetické bezpečnosti a garantů primárních aktiv a vedoucích oddělení pracovníků, kteří mají za podpůrná aktiva odpovědnost.

Pro další inspiraci u identifikace podpůrných aktiv a garantů podpůrných aktiv je možné využít informace v kapitolách 4.2.1 a 4.2.3 přílohy č. 1.

Stejně jako všechna primární aktiva, je nezbytné evidovat i podpůrná aktiva. U podpůrných aktiv se evidují tyto údaje:

- ID aktiva/inventární číslo,
- název,
- garant aktiva,
- hodnocení aktiva z hlediska důvěrnosti, integrity a dostupnosti,
- detailní popis – v případě, že se jedná o typové aktivum tak i specifikace toho, co zahrnuje,
- další informace o aktivu – např. kdo jsou jeho uživatelé, jaké agendy jej využívají, jaké mají dodavatele, zda se jedná o významné dodavatele či provozovatele atd.

Pro potřeby řízení aktiv a rizik je nutné zahrnout do evidence vlastnosti a zranitelnosti jednotlivých typových podpůrných aktiv:

- switch (výpadek napájení, chyba administrátora, přetížení, uplink, …)
- klimatizace (výpadek napájení, porucha, nefunkční monitoring, …)
- UPS (výdrž na baterie, nefunkční monitoring, automatické testování, …)
- motorgenerátor (doba náběhu, porucha, nefunkční monitoring, spotřeba paliva, …)
- apod.

2. Určení vazeb mezi primárními a podpůrnými aktivy

Hodnocení podpůrných aktiv musí být v souladu s hodnocením primárních aktiv. Stejně jako u primárních aktiv se provádí jejich hodnocení a posouzení dopadu narušení bezpečnosti informací – aktiva jsou hodnocena z pohledu DDI.

Evidence podpůrných aktiv se společně s evidencí primárních aktiv provádí v rámci služby správy aktiv JU. Ve službě správy aktiv je nutné spojit primární a podpůrná aktiva pomocí níže uvedené vazby, která zajišťuje dědění hodnot DDI primárního aktiva na podpůrná aktiva:

- Parametry KB jsou určeny / Určuje parametry KB
  - Tato vazba se využívá i při spojení primárních aktiv se souhrnným primárním aktivem

Jednotlivá další podpůrná aktiva, která na sebe navazují, se následně spojují vazbami:

- Je používán / Používá – Systémy, databáze, PC apod.
- Je hostován / Hostuje – Virtualizační prostředí apod.

- Je zálohován / Zálohuje – Zálohování apod.
- Je směrován / Směruje – Síťové prvky apod.

Tyto vazby zajišťují, že podpůrná aktiva dědí hodnoty DDI primárních aktiv z hierarchie závislostí a vytváří konfigurační databázi aktiv (CMDB).

Protože podpůrná aktiva pouze dědí hodnoty DDI primárních aktiv, je důležité si dát pozor na nadhodnocení podpůrných aktiv.

c) Pravidla ochrany jednotlivých úrovní aktiv

Aby bylo možné určit pravidla ochrany aktiv, je nejdřív nutno provést hodnocení důležitosti aktiv podle stupnic hodnocení DDI.

Následně je nutné vybrat nejvyšší hodnotu z hodnocení DDI, čímž dojde k zařazení informace do výsledné úrovně, podle které budou aplikována pravidla pro ochranu informací.

Tabulka pravidel ochrany jednotlivých úrovní aktiv je k dispozici v příloze č. 3.

1. Způsoby rozlišování jednotlivých úrovní aktiv – informace

Na základě hodnocení aktiv se musí určit možné způsoby zacházení s jednotlivými aktivy, které obsahují informace a stanovit možné způsoby likvidace dat pro jednotlivé úrovně aktiv.

Způsoby zacházení s jednotlivými aktivy musí být zvoleny přiměřeně k jednotlivým úrovním aktiv. Klasifikaci informací musí provést odpovědný garant aktiva nebo autor informace.

Úroveň aktiva ovlivní sdílení a následné využití informací o aktivu. Pro sdílení informací je doporučeno používat protokol TLP (Traffic Light Protocol).

TLP protokol je detailně popsán v příloze č. 4.

2. Pravidla pro manipulaci a evidenci aktiv podle úrovní aktiv

Pravidla pro manipulaci a evidenci aktiv platí pro všechna aktiva, která obsahují informace. Aktiva jsou označována v souladu s nastavenými pravidly podle jejich klasifikace, které jsou součástí přílohy č. 3.

3. Přípustné způsoby používání aktiv

JU musí definovat pravidla pro přijatelné použití aktiv. Tato pravidla se musí vztahovat na všechny uživatele aktiv, dodavatele a třetí strany a musí být zdokumentována v politice přijatelného použití nebo alespoň poznamenána v evidenci jednotlivých aktiv.

d) Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií

Způsoby likvidace jsou popsány v příloze č. 3, která vychází z tabulky vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti. Tabulka v příloze je rozdělena do 4 úrovní podle důležitosti aktiv. Pravidla pro likvidaci dat by měla být stanovena přiměřeně hodnotě a důležitosti aktiv.

Historie revizí

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