Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-013**
Název dokumentu:	**Politika akvizice, vývoje a údržby**
Typ dokumentu:	Interní dokument – **TLP:GREEN**
Rozsah:	Politika se vztahuje na plánovanou akvizici, vývoj a údržbu informačních a komunikačních systémů.
Prvek legislativy:	Vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti § 10, 11, 13
Datum vydání:	07. 07. 2026
Datum účinnosti:	**07. 07. 2026**
Platnost do:	odvolání
Počet stran + příloh:	2 + 0
Verze:	1.1
Význam a benefity:	Politika zajišťuje bezpečnost vývojového a testovacího prostředí a ochranu používaných testovacích dat. Rovněž uchovává zajištění bezpečnosti ostatních aktiv.
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

Předmětem politiky jsou postupy pro vznik a využívání nových aktiv v celém jejich životním cyklu.

a) Bezpečnostní požadavky pro akvizici, vývoj a údržbu

Každé pořizované nebo vyvíjené aktivum, je již při jeho plánování posuzováno z hlediska dostupnosti, důvěrnosti a integrity (DDI) jako ostatní stávající aktiva a je opětovně posuzováno/zahrnuto do analýzy rizik.

Vlastní vývoj musí být dokumentován.

V úvahu připadají také rizika, která mohou vyplývat ze vzájemných závislostí mezi různými projekty a ze závislostí více projektů na týchž zdrojích nebo odborných znalostech.

Aktivum je pořizováno v souladu se strategií JU a se zásadami budování ICT/IT služeb.

Plán pořízení aktiva dále zahrnuje (vedle DDI) funkční a jiné než funkční požadavky, požadavky na údržbu komponent, technické cíle a požadavky (implementace/podpora/provoz) na dodavatele.

Pro vývoj a testování aktiva existuje oddělené prostředí, které nesmí ovlivnit běh stávajících služeb a integritu provozních informací.

b) Řízení zranitelností

Za údržbu aktiva v období vývoje, testování i provozu zodpovídá jeho správce, stejně za údržbu jeho komponent zodpovídají správci podpůrných aktiv.

Požadavky na řízení zranitelností se musí vztahovat i na případné poskytovatele (dodavatele) SW a souvisejících služeb.

c) Politika poskytování a nabývání licencí programového vybavení a informací

Politika nabývání programových licencí nebo přijímání informací bývá určována výrobcem, dodavatelem nebo poskytovatelem.

Obsahem návrhu smluv do výběrových řízení je podle významnosti IS výčet požadavků vyhlášky KB. U nevýznamného IS zjednodušený, u významného IS nebo u IS zahrnujícího jeho vývoj, úplný seznam požadavků vyhlášky. Viz 1.4. Politika řízení dodavatelů.

Při uzavírání smluv (dle dodaných nabídek) obsahujících licenční podmínky dodavatele/výrobce/poskytovatele jsou vzata v úvahu rizika plynoucí z povinností jejich dodržování.

Politika poskytování licencí programového vybavení obsahuje ochranné prvky autora i JU minimálně v oblastech:

- předmět licenční smlouvy
- uživatelský účet
- licence k SW
- rozsah a způsob užití SW nabyvatelem

- funkcionalita SW
- práva z vadného plnění a náhrada újmy
- trvání licenční smlouvy
- ochrana informací
- profylaxe/opravy a nasazování patchů a změn do produkčního prostředí.

1. Pravidla a postupy nasazení programového vybavení a jeho evidence

Převzetí aktiva před realizací změny (nasazením) je podmíněno úspěšným testováním a schválením aktiva s ohledem na výše uvedené požadavky a cíle. Doporučen je dále seznam slabých míst, možných způsobů jejich narušení a typických bezpečnostních incidentů.

Ochrana aktiva zahrnuje ochranu:

- integrity zdrojového kódu (použité bezpečnostní standardy pro tvorbu, implementaci a užívání aplikačních software, např.: ISO/IEC 27034, BSIMM, Microsoft SDL nebo OWASP),
- související aktuální dokumentace a návody,
- dokumentace vývoje a zavádění aktiva do provozu.

Proces nasazení aktiva do provozu je řízenou změnou dle politiky 1. 21. Politika řízení změn.

Může být vyžadován plán reakce na případné bezpečností selhání viz „nejčastějších 10 rizik“.

Po nasazení je bezpečnost aktiva otestována v reálném prostředí a proveden bezpečnostní audit.

2. Pravidla a postupy pro kontrolu dodržování licenčních podmínek

Správci SW licencí provádí kontrolu platných SW licencí a jejich využití nejméně 1x ročně.

Poskytovatel může vyžadovat kontrolu dodržování licenčních podmínek. Stupně kontrol:

1. výzva k provedení interní samokontroly;
2. výzva k umožnění/provedení SW kontroly;
3. oznámení o provedení řízeného auditu.

Postup:

1. Výzvu neignorovat, komunikovat, zjistit podrobnosti.
2. Určit rozsah.
3. Provést interní analýzu, přizvat další odborníky.
4. Případně zdůvodnit oddálení kontroly (max. 6 měsíců) a provést nápravná opatření

Historie revizí

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