

Politika akvizice, vývoje a údržby

I. Úvodní ustanovení

- 1) Politika akvizice, vývoje a údržby stanovuje pravidla a postupy pro vznik a využívání nových aktiv v celém jejich životním cyklu informačního systému a rozpracovává požadavky na kybernetickou bezpečnost dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále také „zákon o kybernetické bezpečnosti“) a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále také „vyhláška o kybernetické bezpečnosti“) v podmínkách Univerzity Hradec Králové (dále také „UHK“).
- 2) Účelem této politiky je:
 - a) zajistit bezpečnost informací při akvizici, vývoji a údržbě IS a prvků informační a komunikační technologie,
 - b) stanovit pravidla a postupy při akvizici, vývoji a údržbě programového vybavení včetně jeho evidence,
 - c) stanovit pravidla a postupy pro kontrolu dodržování licenčních podmínek.
- 3) Tato politika se vztahuje na všechny osoby odpovědné za zajištění bezpečnosti vývojového a testovacího prostředí a ochranu používaných testovacích dat v rámci UHK.

II. Bezpečnostní požadavky pro akvizici, vývoj a údržbu

- 1) Požadavky na bezpečnost musí být zahrnuty již ve fázi výběru a návrhu systému, musí být zdokumentovány a uvedeny ve smlouvách s dodavateli.
- 2) Požadavky na bezpečnostní opatření musí být definovány a implementovány na základě klasifikace primárních aktiv daného systému a na základě provedené analýzy rizik.
- 3) Musí být vytvořena akceptační kritéria zahrnující funkční a bezpečnostní požadavky pro nový systém. Tato kritéria musí být vyhodnocena v rámci akvizice a před uvedením systému do provozu.
- 4) Při vývoji musí být zajištěna bezpečnost vývojového a testovacího prostředí a jejich oddělení od produkčního prostředí.
- 5) Přechod nového systému do produkčního prostředí a údržba všech systémů musí být prováděny dle pravidel pro řízení změn uvedených v *Politice řízení změn*.
- 6) Po celý životní cyklus systému musí být zajištěno řízení verzí programového vybavení včetně možnosti návratu na předchozí verzi.

- 7) Provozní, projektová, uživatelská a bezpečnostní dokumentace musí být udržována aktuální po celou dobu vývoje systému.
- 8) Proces akvizice a vývoje je plánován, dokumentován a řízen.
- 9) Garant primárního a podpůrného aktiva:
 - a) definuje funkční požadavky na akvizici a vývoj jednotlivých prvků informační a komunikační technologie,
 - b) zajišťuje klasifikaci aktiva,
 - c) stanovuje pravidla přístupu k aktivu.
- 10) Vedoucí oddělení informačních technologií (dále také „*OIT*“) navrhuje implementaci bezpečnostních opatření prvků informační a komunikační technologie alespoň na úrovni:
 - a) bezpečnosti vývojového prostředí,
 - b) metodologie vývoje software,
 - c) kontrolních bodů bezpečnosti v projektu,
 - d) bezpečného úložiště,
 - e) řízení verzí,
 - f) identifikace zranitelností a návrhu opatření.
- 11) Garant podpůrných aktiv ve spolupráci s OIT definuje požadavky na údržbu prvku informační a komunikační technologie.
- 12) Životní cyklus aktiva a proces akvizice obsahuje bezpečnostní požadavky a bezpečnostní opatření v závislosti na platné bezpečnostní politice, identifikovaných rizicích a požadavcích Garantů primárních a podpůrných aktiv.
- 13) Vývoj, změny a údržba aktiv jsou prováděny v souladu se stanoveným procesem, který zohledňuje zásady bezpečného vývoje a řízení změn, testování v rámci odděleného prostředí, kontrolu vytvořeného kódu, případně nezávislou kontrolu bezpečnosti třetí stranou.

III. Řízení zranitelností

- 1) V rámci akvizice systému a po implementaci významných změn musí být na základě provedené analýzy rizik rozhodnuto o provedení testů zranitelností nebo penetračních testů.
- 2) Proces řízení zranitelností aktiv je plánován, dokumentován a řízen. Je založen na:
 - a) identifikaci zranitelností,
 - b) řešení zranitelností dle priorit,
 - c) kontrole aplikovaných opatření.
- 3) Technické přezkoumání aplikací po změnách provozní platformy jednotlivých prvků informační a komunikační technologie vyžaduje alespoň:
 - a) přezkoumání postupů řízení a integrity aplikací k zajištění, že nebyly změnami provozních platforem kompromitovány,
 - b) zajištění včasného oznámení změn provozních platforem, aby bylo před implementací umožněno provedení příslušných testů a přezkoumání,
 - c) zajištění provedení příslušných změn v plánech kontinuity činností.
- 4) Změny programového vybavení jsou omezeny na nezbytné změny a všechny jsou řízeny. V případě, že je nutno programové vybavení upravit, jsou posuzovány následující body:
 - a) rizika navrhovaných opatření a procesů zajišťujících integritu,
 - b) dodržení licenční politiky,
 - c) součinnost s dodavatelem při aktualizaci programového vybavení,
 - d) kompatibilita s dalším používaným programovým vybavením.

IV. Politika poskytování a nabývání licencí programového vybavení a informací

- 1) Na všech zařízeních provozovaných na UHK musí být instalován pouze autorizované programové vybavení s platnou licencí, případně autorizované programové vybavení, pro které zakoupení licence není vyžadováno výrobcem, dodavatelem nebo poskytovatelem.

Pravidla a postupy nasazení programového vybavení a jeho evidence

- 2) Aplikační správce VIS vede evidenci programového vybavení v souladu s obecně platnými právními předpisy a vnitřními předpisy UHK.

- 3) Evidence obsahuje alespoň tyto údaje:
 - a) název programového vybavení,
 - b) dodavatele nebo výrobce programového vybavení,
 - c) počet pořízených licencí,
 - d) druh licencí,
 - e) platnost licencí,
 - f) osobu odpovědnou za použití licencí.
- 4) Za distribuci, instalaci, údržbu, změny, rozvoj a vyřazování programového vybavení odpovídá aplikační správce VIS.
- 5) Nasazení programového vybavení je v souladu s licenčními podmínkami a zvláštním právním předpisem.

Pravidla a postupy pro kontrolu dodržování licenčních podmínek

- 6) Proces kontroly dodržování licenčních podmínek je řízen a dokumentován.
- 7) Pravidelnou kontrolu dodržování licenčních podmínek včetně návrhu na nápravné opatření provádí aplikační správce VIS.

V. Závěrečná ustanovení

Politika akvizice, vývoje a údržby vstupuje v platnost i účinnost dnem jejího podpisu.

V Hradci Králové dne 31. 5. 2024

prof. Ing. Kamil Kuča, Ph.D., v. r.
rektor