Politika bezpečnosti lidských zdrojů

I. Úvodní ustanovení

1) Politika bezpečnosti lidských zdrojů stanovuje pravidla zvyšování bezpečnostního povědomí v oblasti kybernetické bezpečnosti 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 politiky je definovat postupy a zásady pro:
    - školení zaměstnanců UHK,
    - kontrolu dodržování bezpečnostních politik,
    - zabezpečení kybernetické bezpečnosti při nástupu, výkonu, ukončení a změně pracovního poměru.
3) Tato politika se vztahuje na všechny zaměstnance UHK, informační aktiva vytvořená nebo používaná v rámci významného informačního systému (dále také *„VIS*"), a na uživatele těchto aktiv.

II. Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení

1) Osobní a mzdové oddělení UHK (dále jako *„OMO*") ve spolupráci s Oddělením informačních technologií UHK (dále také *„OIT*") a Manažerem KB organizuje vstupní a periodické školení zaměstnanců UHK v oblasti informační a kybernetické bezpečnosti v souladu s *Plánem rozvoje bezpečnostního povědomí*.

Způsoby a formy poučení uživatelů

Uživatelé budou poučeni prostřednictvím elektronického vzdělávání (e-learning) nebo formou prezenčního vzdělávání o pravidlech zajišťování bezpečnosti informací, případně budou poučeni o specifických otázkách spojených s konkrétní skupinou aktiv VIS. Míra porozumění uživatelů se ověřuje testem v systému EDUNIO minimálně 1× za 2 roky. O provedení poučení je proveden zápis podepsaný uživatelem v systému EDUNIO.

Způsoby a formy poučení garantů aktiv

Garanti aktiv budou v rámci jmenování do role poučeni prostřednictvím elektronického vzdělávání (e-learning) nebo formou prezenčního vzdělávání o pravidlech zajišťování

bezpečnosti informací a o pravidlech výkonu funkce Garanta aktiva, případně budou poučeni o specifických otázkách spojených s konkrétní skupinou aktiv. Míra porozumění Garantů aktiv se ověřuje testem v systému EDUNIO minimálně 1× za 2 roky. O provedení poučení je proveden zápis podepsaný Garantem aktiva v systému EDUNIO.

Způsoby a formy poučení administrátorů VIS

Administrátoři VIS budou před svěřením konkrétních systémů či zařízení do správy poučeni prostřednictvím elektronického vzdělávání (e-learning) nebo formou prezenčního vzdělávání o pravidlech zajišťování bezpečnosti informací a o pravidlech výkonu funkce administrátora VIS, případně budou poučeni o specifických otázkách spojených se spravovanými zařízeními. Míra porozumění administrátorů VIS se ověřuje testem v systému EDUNIO minimálně 1× za 2 roky. O provedení poučení je proveden zápis podepsaný administrátorem VIS v systému EDUNIO.

Způsoby a formy poučení osob zastávajících bezpečnostní role

Osoby zastávající ostatní bezpečnostní role budou v rámci jmenování do role školeni prostřednictvím elektronického vzdělávání (e-learning) nebo formou prezenčního vzdělávání o pravidlech zajišťování bezpečnosti informací a o pravidlech výkonu dané role, případně budou poučeny o specifických otázkách spojených s danou rolí. Míra porozumění osob vykonávající bezpečnostní role se ověřuje testem v systému EDUNIO minimálně 1× za 2 roky. O provedení poučení je proveden zápis podepsaný osobou vykonávající bezpečnostní roli v systému EDUNIO.

Mimořádná školení

V případě závažných důvodů (např. kybernetický bezpečnostní incident, kybernetická bezpečnostní událost) může Manažer KB provést mimořádné školení za dodržení uvedených pravidel a principů u jednotlivých rolí nebo dotčeného rozsahu uživatelů.

III. Bezpečnostní školení nových zaměstnanců

1) Každý nový zaměstnanec je povinen v den nástupu absolvovat vstupní školení pro uživatele, a to včetně ověření porozumění prostřednictvím testu v systému EDUNIO. Poté minimálně 1× za 2 roky absolvuje pravidelné opakovací školení (se zohledněním případných změn v dokumentaci, postupech atd.).

2) Používat prostředky informačních a komunikačních technologií může pouze zaměstnanec, který byl náležitě proškolen v oblasti bezpečnosti informací a s bezpečnostními opatřeními odpovídající jeho pracovnímu zařazení a absolvoval školení o práci v těch informačních systémech, které bude při výkonu svého zaměstnání využívat. O seznámení s uvedenými dokumenty a o školení musí být proveden zápis, který bude uložen v systému EDUNIO.

3) Cílem bezpečnostního školení je především osvojení znalostí, jak předcházet bezpečnostním událostem a incidentům, jak se chovat v neobvyklých situacích a jak se z nich poučit. To znamená, že zaměstnanci UHK:

   a) porozumí své roli a budou si vědomi své zodpovědnosti vůči organizaci a okolí,

   b) pochopí zásady systému řízení bezpečnosti informací a z nich vyplývající postupy,

   c) se chovají v souladu se stanovenými bezpečnostními opatřeními,

   d) budou mít znalosti o řídících, provozních a technických mechanismech používaných k zajištění bezpečnosti aktiv, za které odpovídají anebo se kterými pracují.

4) Manažer KB zpracovává a vede o bezpečnostních vstupních i periodických školeních přehledy, které obsahují termín školení, předmět školení a seznam osob, které školení absolvovaly.

IV. Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací

1) V případě výskytu závažného bezpečnostního kybernetického incidentu, který byl způsoben porušením bezpečnostních politik UHK ze strany zaměstnanců UHK, je vůči těmto zaměstnancům zahájen postup v souladu s příslušnými ustanoveními zákona č. 262/2006 Sb., zákoník práce v platném znění. Způsob řešení porušení odpovídá povaze incidentu a jeho dopadu na UHK.

2) Při tomto porušení příslušný vedoucí zaměstnanec zohlední:

   a) absolvování bezpečnostního školení,

   b) povahu porušení bezpečnosti a jeho dopad,

   c) zda se jedná o první nebo opakované porušení,

   d) zda se jedná o záměrné nebo nedbalostní porušení,

   e) odpovídající legislativu,

   f) existující smlouvy,

   g) další relevantní okolnosti.

3) V případě podezření ze spáchání trestného činu postupuje UHK v souladu s příslušnými ustanoveními zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád) a souvisejícími právními předpisy.

V. Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice

1) Při rozhodování o ukončení nebo změně pracovněprávního vztahu je odpovědný vedoucí zaměstnanec povinen zohlednit následující rizikové faktory:
   a) z jakých důvodů dochází ke změně nebo ukončení pracovněprávního vztahu,
   b) stávající odpovědnosti zaměstnance,
   c) hodnotu aktiv, ke kterým může mít (mohl mít) přístup.
2) Před ukončením nebo změnou pracovněprávního vztahu odpovědný vedoucí zaměstnanec odebere nebo omezí přístupová práva k informačním aktivům a prostředkům pro zpracování informací nebo k tomu vydá písemný pokyn.
3) Pokud jsou přístupová práva sdílena mezi více zaměstnanci, rozhodne odpovědný vedoucí zaměstnanec o změně skupinových přístupových práv, tyto uživatele ze všech seznamů skupinových přístupových práv vyjme a všem ostatním zaměstnancům zakáže sdílet informace s odcházejícím zaměstnancem. Odpovědný vedoucí zaměstnance o tomto postupu informuje správce aktiv.
4) V závažných případech je zaměstnanec okamžitě zbaven svých přístupových práv a výsad.

Vrácení svěřených aktiv a odebrání práv při ukončení pracovního vztahu

1) V případě ukončení pracovněprávního vztahu musí zaměstnanec vrátit všechny zapůjčené prostředky, dokumenty a ostatní vybavení, vztahující se ke svěřeným aktivům. Věcně příslušný zaměstnanec odebere přístupová práva k informačním aktivům a prostředkům pro zpracování informací.
2) V případě ukončení pracovněprávního vztahu s klíčovými zaměstnanci (uživatelé s přidělenými rolemi ve VIS, garanti primárních aktiv, garanti podpůrných aktiv v kategoriích technické vybavení, programové vybavení a komunikační prostředky) nebo zaměstnanci zastávajícími bezpečnostní role musí být zajištěno předání odpovědností.
3) Za proces a náležitosti spojené s ukončením pracovněprávního vztahu je odpovědný příslušný vedoucí zaměstnanec, který dbá na to, aby byly dodrženy všechny aspekty bezpečnosti a odpovídající postupy. V případech, kdy je to obsahem smlouvy, musí informovat zaměstnance smluvní nebo třetí strany o provozních a personálních změnách.
4) V rámci procesu ukončování pracovněprávního vztahu odpovědný vedoucí zaměstnanec formálně potvrdí odebrání všech přístupových oprávnění odcházejícího zaměstnance, a to jak v rovině fyzického přístupu (vstupní karty, klíče, aj.), tak především oprávnění k informačním systémům UHK (zneplatnění všech přístupových oprávnění zaměstnance k datu ukončení pracovněprávního vztahu).

Změna přístupových oprávnění při změně pracovní pozice

1) V případě změny pracovněprávního vztahu musí odpovědný vedoucí zaměstnanec kromě úpravy popisu práce vydat písemný pokyn ke změně přístupových oprávnění, a to jak v rovině fyzického přístupu (vstupní karty, klíče, aj.), tak především oprávnění k informačním systémům UHK tak, aby reflektovaly nové pracovní zařazení zaměstnance. Odpovědný vedoucí zaměstnanec o tomto vyhotoví formální zápis.
2) Změny v řízení přístupu musí být logovány.

VI. Závěrečná ustanovení

Politika bezpečnosti lidských zdrojů vstupuje v platnost dnem jejího podpisu a v účinnost dne 1. 2. 2025.

V Hradci Králové dne 31. 5. 2024

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