MAGISTRÁT HLAVNÍHO MĚSTA PRAHY

Odbor informatiky

Verze: 1.0

Datum vydání: 1. 4. 2020

Pravidla použití IDM pro MČ a organizace zřizované MHMP

Dokument shrnuje pravidla spojená s provozem sytému řízení jednotných identit MHMP. Tento nástroj je vyžadován zákonem o kybernetické bezpečnosti a zároveň vytváří legitimní, bezpečné a systémové řešení přidávání a odebírání uživatelů a jejich oprávnění – řízení identit a přístupů. Ke správě uživatelů je zapotřebí přistupovat s maximální mírou péče, neboť svou činností ovlivňujete přístupy do „významných informačních systémů“ dle zákona o kybernetické bezpečnosti a nesprávnou činností můžete způsobit úniky dat, osobních údajů apod.

1. K čemu IDM

IdM MHMP a IdM pro MČ je zjednodušeně řečeno ověřená databáze osob, které mají oprávněný důvod k přístupu do minimálně jedné aplikace v informačním systému MHMP. Do databáze je zadává a jejich přístupy upravuje garant subjektu, pro který vykonávají pracovní činnost. V případě úřadu městské části, nebo subjektu zřizovaného MHMP je garantem nejvyšší představitel tohoto subjektu (u městských částí – tajemník). Ten následně sám, nebo prostřednictvím svého zástupce (osoby, na kterou deleguje správcovství), provádí aktivaci a deaktivaci osob (identit) a následně přiřazuje role (přístupy do aplikací).

2. Základní bezpečnostní podmínky a pravidla

2.1. Zásada „potřeby znát“ – do IDM se zadávají uživatelé, kteří mají potřebu přistupovat do informačních systémů a aplikací organizace. Jakmile tato potřeba pomine, musí být uživatelé v systému IDM zneplatněni. V případě, že se změní pracovní náplň uživatele, nebo pomine potřeba přístupu do jedné z přidělených aplikací, musí být neprodleně upraven jeho profil rolí v systému IDM dle odpovídajících potřeb.

2.2. Dodržování procesů – je zapotřebí dodržovat obecné standardní postupy při výkonu správy identit (žádosti, změny, informace). Jakékoliv nestandardní řešení a výjimky by neměly být umožněny nebo provedeny.

2.3. V případě zjištění jakýchkoliv nestandardních událostí nebo stavů je zapotřebí kontaktovat neprodleně Service desk nebo administrátora MHMP.

2.4. Pro účely IDM je administrátorem MHMP Ing. Milan Kasan (778 410 833, milan.kasan@praha.eu).

3. Garant subjektu (tajemník MČ)

3.1. Garantem subjektu je vždy nejvyšší výkonný představitel. U úřadu MČ se jedná o tajemníka, u zřizovaných subjektů se může jednat o ředitele, předsedu apod.

3.2. Roli garanta přiděluje vždy administrátor MHMP a to na základě ustanovení tajemníka do funkce.

3.3. Garant subjektu nevytváří další garanty. Vytváří pouze běžné uživatele (role „uživatel“) a to jak pro kmenové zaměstnance, tak pro externisty.

3.4. Garant smí delegovat svá práva výkonu funkce správce a to formou delegace na uživatele, který je v IDM zaveden. Delegace musí být provedena v aplikaci IDM v profilu garanta v záložce „Delegace“ (postup dle uživatelského manuálu). Jakékoliv jiné formy delegací (předání přístupových údajů jiné osobě apod.) jsou zakázána.

3.5. V případě, že garant deleguje práva výkonu funkce správce, jedná se pouze o delegaci správy identit (obsluhy aplikace), odpovědnost za správnost údajů zadaných do IDM a dodržování právních předpisů zůstává na garantovi.

3.6. Garant subjektu by měl minimálně jednou za kvartál provést nevyžádanou kontrolu seznamu uživatelů a jejich oprávnění a kontrolu platnosti a rozsahu delegací.

3.7. V případě, že garant nebo jím určený správce objeví jakoukoli chybu ve funkčnosti nebo obsahu aplikace IdM, je povinen tuto chybu neprodleně nahlásit na Service desk nebo administrátorovi MHMP.

4. Správa uživatelů

4.1. Každá osoba smí mít v IDM právě jednu identitu. Jedné osobě nesmí být vytvářeno vícero identit a to ani v případě nefunkčnosti aktuální identity. V případě takového stavu je správným řešením kontaktovat Service desk nebo administrátora MHMP a vyřešit nefunkčnost, nikoliv zakládat identitu novou.

4.2. Vytvoření uživatele je provedeno vyplněním všech požadovaných polí ve formuláři dle manuálu a zadáním termínů platnosti. „Platnost od“ dle doby nástupu, nebo vzniku potřeby přístupu do aplikací MHMP, „platnost do“ je nutné zvolit tak, aby buďto korespondovala s délkou trvání pracovní smlouvy (zejména u externistů), nebo s dobou plánovaného využívání přístupu do aplikací. V případě pracovních smluv na dobu určitou nesmí být hodnota vyšší než termín konce pracovní smlouvy.

4.3. Vymazání uživatele se neprovádí. Provádí se vždy pouze jeho zneplatnění („deaktivace“). Zneplatnění se provádí editací profilu uživatele a zadáním hodnoty „Platný do“ na termín požadovaného zneplatnění.

5. Správa rolí

5.1. Role představují základní nástroj pro udělení přístupů do aplikací. Za jednu roli se považuje konkrétní typ přístupu do konkrétní aplikace.

5.2. Role jsou vytvářeny garanty aplikací MHMP. V případě, kdy v nabídce rolí není k dispozici role požadovaná, je zapotřebí kontaktovat administrátora MHMP, který na žádost zajistí postup vytvoření nové role (předá požadavek na vytvoření role garantovi dané aplikace na MHMP).

5.3. Přiřazení role konkrétnímu uživateli provádí garant v profilu daného uživatele. Při všech činnostech přiřazování a odebírání rolí dodržuje garant zásadu „potřeby znát“.

5.4. Odebrání / změnu role provádí garant formou ukončení platnosti přiřazení dané role.

6. Uživatelé a hesla

6.1. Běžný uživatel si prostřednictvím IDM mění heslo ke svému účtu v síti MHMP. V rámci zavádění IDM se může stát, že do první změny hesla bude heslo do sítě MEPNET odlišné od hesla do IDM. Bezprostředně po první změně hesla v IDM bude tento stav narovnán.

6.2. Platnost hesla je 90 dní, před jejím vypršením obdrží uživatel tři notifikační zprávy.

6.3. Heslo je nutné vyměnit vždy před vypršením jeho platnosti, nebo kdykoliv, kdy existuje možnost, že heslo k danému účtu bylo zveřejněno jiným osobám.

6.4. Při tvorbě hesla musí být dodržena politika tvorby hesel MHMP (viz příloha), heslo nesmí obsahovat diakritiku a musí být odlišné od soukromě používaných hesel.

6.5. V případě ztráty hesla kontaktuje uživatel garanta svého subjektu, který provede jeho obnovu.