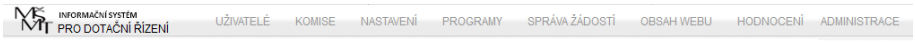


PRAVIDLA

pro bezpečnou práci s uživatelským účtem v administrátorském prostředí IS pro dotační řízení MŠMT

Určeno pro instanci (modul): **.....**

Uživatel (majitel účtu): **.....**

1. Úvodní ustanovení

Hesla jsou důležitou součástí počítačové bezpečnosti a v práci s osobními, resp. citlivými údaji. Stojí na prvním místě v ochraně pro uživatelské účty. Špatně zvolené heslo, resp. nevhodná péče o heslo k některým službám může za jistých okolností kompromitovat a degradovat celou práci všech uživatelů IS.

Všichni pracovníci, kteří mají přístup do administrátorského prostředí IS pro dotační řízení (dále jen redakčního systému), jsou zodpovědní za dodržování kroků, které jsou uvedeny v těchto pravidlech, k maximálnímu zabezpečení svého uživatelského účtu.

2. Účel pravidel ochrany

Účelem těchto pravidel je vytvořit standardy pro bezpečnou práci s uživatelským účtem a heslem, a tedy pro zabezpečení obsahu garantovaného webu před vstupem nepovolaných osob.

3. Rozsah a popis uživatelských rolí

Tato pravidla se vztahují na všechny osoby, které vstupují do redakčního systému v libovolné roli:

- **Formální hodnotitel** – kontroluje v modulu Správa žádostí jednotlivé žádosti, nastavuje (ne)splnění kritérií formálního hodnocení a nastavuje stav projektu.
- **Věcný hodnotitel** – kontroluje v modulu Hodnocení obsahovou (věcnou) stránku projektu a ve formuláři přiděluje projektům bodové případně slovní hodnocení.
- **Komisař** – má přístup ke všem projektovým žádostem daného dotačního programu a k odborným hodnocením.
- **Pracovník uživatelské podpory (helpdesku)** – má přístup k seznamu uživatelů, může se vtělit do jeho účtu a poradit v případě požadavku žadatele prostřednictvím helpdesku.

- **Tajemník komise** – má přístup k importu a exportu dat pro jednání výběrové komise, může přidělovat body jednotlivým projektům v průběhu hodnocení komise.
- **Administrátor systému** – působí jako správce celého systému, může vytvářet a konfigurovat nové dotační programy, může nastavovat číselníky polí, vytvářet a spravovat uživatele.

4. Bezpečnostní pravidla pro práci s uživatelským účtem

4.1. Podoba uživatelského jména

Uživatelské jméno je jednoznačně přidělený identifikátor účtu osoby, který má alfanumerickou podobu a generován informačním systémem a případně upraven správcem aplikace. O vytvořené podobě uživatelského jména je uživatel informován prostřednictvím mailu, který zasílá systém.

4.2. Nutná podoba hesla

Heslo je ve výchozí podobě automaticky generováno a přiřazeno informačním systémem. Je více než vhodné, aby si ho uživatel pro lepší zapamatovatelnost změnil. Heslo v jakékoliv fázi procesu (vygenerované, změněné) musí respektovat tzv. bezpečnostní politiku hesla:

- Heslo musí mít minimálně 8 znaků
- Znaky jsou bez diakritiky (háčky, čárky) zapsány pomocí anglické abecedy
- Heslo musí obsahovat minimálně jednu číslici
- Heslo musí obsahovat minimálně jedno velké písmeno anglické abecedy
- Heslo musí obsahovat minimálně jedno malé písmeno anglické abecedy

4.3. Nedoporučená podoba hesla

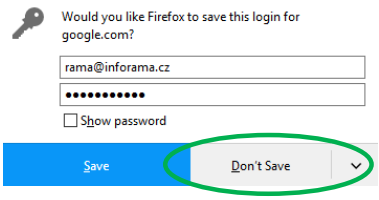
- Heslo by nemělo být slovem, které lze najít v českém slovníku
- Heslo by nemělo obsahovat, jméno nebo příjmení registrované osoby, jména rodinných příslušníků, domácích mazlíčků, apod.
- Heslo by nemělo obsahovat data narození, svátků a další soukromé informace, jako je adresa bydliště nebo telefonní čísla.
- Heslo nesmí obsahovat uživatelské jméno, nebo jeho části

4.4. Zadávání hesla při přístupu do aplikace/služby

a) Zadávejte heslo pouze a výhradně do systémů připojených pres HTTPS protokol s validním certifikátem (v adresním řádku musí být zeleně napsáno „zabezpečeno/secure“ před URL adresou (

)

b) Nikdy neukládejte heslo do prohlížeče nebo operačního systému zařízení, na kterém se připojujete.



c) Nezadávejte heslo v prostorách sledovaných kamerovým systémem zachycující klávesnici, nebo pokud jste během zadávání nahráváni.

d) Nezadávejte hesla mimo počítačovou síť Vašeho zaměstnavatele, například v kavárnách a restauracích, kde Vám internetové připojení zprostředkovává neověřená třetí strana (tzv. WIFI FREE).

4.5 Platnost hesla

Heslo je platné od: ..... do: .....
O změnách uživatelského účtu a nutnosti změny hesla je uživatel informován pomocí e-mailu uživatele: .....

4.6. Utajení přístupových uživatelských údajů

S přístupovými uživatelskými údaji (= uživatelské jméno a heslo) musí být nakládáno jako s důvěrnou informací. Je přísně zakázáno tyto údaje sdělovat třetím osobám. Dále je zakázáno ukládat tyto údaje v počítači, na papírku, kde s nimi mohou přijít do styku třetí osoby.
Je přísně zakázáno je sdělovat do jakýchkoliv nezabezpečených a nepřímých otevřených informačních kanálů jako jsou např. sociální sítě, různé formy IM (IM, Twitter, …).
V případě podezření na vyzrazení či kompromitaci hesla je uživatel povinen neprodleně informovat oddělení IT, kde dojde k zablokování uživatelského účtu. Po prošetření celé události je nutné vygenerovat heslo nové.
Shrnutí základních a často porušovaných pravidel pro utajení hesla:

a) NIKOMU nesdělujte heslo po telefonu.
b) Nepište heslo do emailové komunikace.
c) Nesdělujte heslo svému vedoucímu.
d) Nemluvte o heslu před ostatními.
e) Nepište heslo do dotazníků nebo formulářů o bezpečnosti.
f) Nesdílejte heslo s rodinnými příslušníky.
g) Nesdělujte heslo spolupracovníkům během Vaší dovolené (pokud je nutné, aby v průběhu Vaší dovolené měl Váš spolupracovník k Vašim datům, aplikacím, sdělte tuto potřebu správci aplikace prostřednictvím webového formuláře v dostatečném předstihu, který vás bude kontaktovat a navrhne vhodné řešení.

Pokud po Vás někdo neustále vyžaduje Vaše heslo, odkažte ho na tento dokument nebo kontaktujte správce aplikace. Ten má vyhrazeno právo kontrolovat plnění těchto bezpečnostních pravidel a v případě uznání, že heslo není bezpečné a že by to mohlo ohrozit bezpečnost webové aplikace, může uživatele požádat o změnu hesla, resp. mu účet zablokovat (znepřístupnit).

5. Únik informací ze systému

Uživatel se svým podpisem zavazuje, že nebude žádná data z IS DŘ kopírovat, tisknout ani jiným způsobem předávat třetím osobám či subjektům.

6. Zneužití pravomocí

Uživatel se svým podpisem zavazuje, že nebude neoprávněně svévolně měnit data v systému. Tzn. např. lze měnit heslo pouze na vyžádání žadatele prostřednictvím helpdesku na adrese příslušného IS …….

7. Porušení pravidel

7.1 Únik hesla

Pokud dojde k úniku / prozrazení hesla třetí osobě, je zaměstnanec povinen si heslo změnit a okamžitě nahlásit datum úniku a datum změny hesla, případně podezřelé (nestandardní) chování aplikace při přihlašování vedoucímu oddělení KaI.

7.2 Zavinění zaměstnance

Pokud bude shledáno, že zaměstnanec ~~nebo kdokoliv jiný, kdo je touto směrnicí vázán,~~ porušil některý z jejích bodů, může dojít k zahájení disciplinárního řízení.

Okomentoval(a): [JI1]: to mi už v minulosti někdo vrátil s tím, že přece nemůže ručit za "kohokoliv jiného"

7.3 Únik informací ze systému

Pokud bude shledáno, že zaměstnanec ~~nebo kdokoliv jiný, kdo je touto směrnicí vázán,~~ úmyslně nebo svojí nedbalostí zavinil únik dat ze systému, může dojít k zahájení disciplinárního řízení.~~.~~

8. Platnost pravidel

Souhlas s dodržováním těchto pravidel provádí každý registrovaný uživatel podpisem tohoto dokumentu. Platnost začíná dnem podpisu.

Uživatel (majitel) účtu: **……..**

Organizace: **……..**

Testovací server: **……..**

Produkční server: **……..**

Uživatelské jméno: **……..**

Heslo: **……..**

Heslo si můžete po přihlášení se do systému změnit, zvolte Můj profil | Nastavení.

Role v systému: **……..**

Platnost ***OD:*** **……** ***DO:*** **……**

Účet byl založen z pověření: **……..**

Svým podpisem potvrzuji souhlas s výše uvedenými pravidly a ponesu veškerou zodpovědnost za škody způsobené nedodržením těchto pravidel.

Dne ……..

…….. ……..

…….. ……..

Uživatel/majitel účtu~~i~~ Správce aplikace