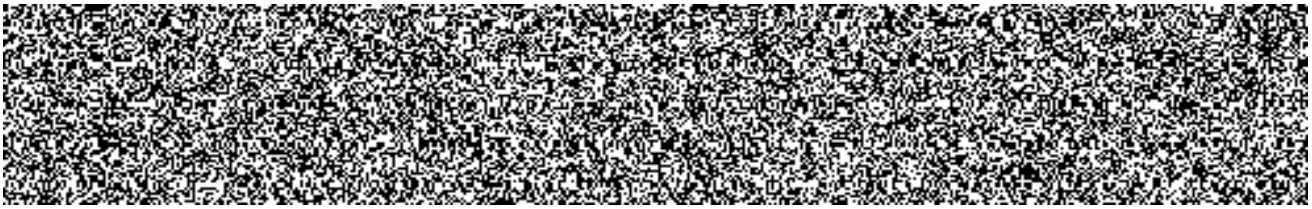
Příloha k žádosti o oprávnění přístupu do IS

Počet stran: 3

Poučení o bezpečnosti a ochraně dat v systému EKIS MV



1) Systém EKIS MV je určen pro potřeby oprávněných pracovníků, zejména rezortu Ministerstva vnitra, k plnění pracovních a služebních povinností určených vedoucími, představenými a správcem systému EKIS MV. Činnost každého uživatele v systému EKIS MV, z hlediska informační bezpečnosti, podléhá kontrole ze strany odborného útvaru EKIS, administrátora a bezpečnostního správce, bezpečnostního manažera.
2) Žádný uživatel nesmí provádět takovou činnost,
   a) která by poškodila nebo by mohla poškodit informace nebo služby systému EKIS MV (z hlediska ztráty, neoprávněné modifikace dat, poškození dat nebo poškození systému včetně jeho nastavení apod.),
   b) která by byla nebo mohla být škodlivá pro Ministerstvo vnitra (ohrožení ochrany osobních údajů, zneužití osobních údajů apod.).
3) Každý uživatel:
   a) musí heslo uchovávat v tajnosti, tzn. nesdělovat ho druhé osobě;
   b) vstupní heslo do pracovní stanice může sdělit pouze pro servisní účely správci počítačového programu. Jakmile takový pracovník ukončí svou servisní činnost, musí uživatel heslo neprodleně změnit.
4) Hesla:

   Heslo do všech aplikací systému EKIS MV:

   - Platnost generovaného inicializačního hesla bude nastavena na 14 dní od zřízení účtu uživatele (uživatel je povinen v co nejkratší době po obdržení přístupových údajů si změnit inicializační heslo na uživatelské heslo),
   - Heslo musí obsahovat minimálně 8 znaků, doporučeno 9 a více,
   - Heslo musí obsahovat kombinaci minimálně jednoho znaku z každé z následujících kategorií: velká písmena (A až Z), malá písmena (a až z), číslice (0 až 9),
   - Nové heslo se musí lišit od předchozího hesla minimálně ve třech znacích a nesmí být stejné jako 5 předchozích hesel,
   - Není umožněno použití hesel, která jsou definována ve výjimkách (jména, dny atd.),
   - Při nečinnosti uživatele v systému po dobu delší než 60 minut dojde k automatickému odhlášení,

- Platnost hesla do produktivního systému maximálně 30 dní (po tomto termínu bude uživatel vyzván k změně hesla),
- Po 3 neúspěšných pokusech o přihlášení dojde k automatickému zablokování účtu uživatele *(pro odblokování je nutné kontaktovat pracoviště Help Desk EKIS MV prostřednictvím e-mailového účtu uvedeného v žádosti o přístup do systému, popřípadě telefonicky)*,
- Heslo je vždy nutné okamžitě změnit, když existuje podezření, že bylo (nebo mohlo být) prozrazeno. Prozrazení hesla, nebo své podezření neprodleně a prokazatelně (písemně) oznámit bezpečnostnímu správci a svému nadřízenému pracovníkovi.

5) Veškeré činnosti týkající se systému EKIS MV jsou uživatelé povinni provádět v souladu s obecně závaznými právními předpisy a interními akty řízení.
6) Každá pracovní stanice, ze které se přistupuje do systému EKIS MV musí mít instalovány všechny potřebné aktualizace, včetně antivirového programu. Instalaci a údržbu provádí administrátor koncového zařízení. Uživatel nesmí svévolně do této instalace zasahovat. Podporu uživatelům a hlášení o podezření, že došlo ke kybernetickému incidentu nebo po zjištění zranitelnosti informačního systému lze realizovat prostřednictvím příslušného pracoviště Help Desk EKIS MV.
7) Na koncových zařízeních přistupujících do informačního systému se smí používat pouze legálně užívaný software.
8) Povinností uživatele je dodržovat preventivní opatření doporučená k ochraně před počítačovými viry.
9) Bezpečnostní opatření:
   a) informační systém EKIS MV musí splňovat podmínky zákona č. 181/2014 Sb., o kybernetické bezpečnosti, dále zákona č. 101/2000 Sb., o ochraně osobních údajů, a porušení bezpečnostních pravidel je pod sankcí zákona č. 101/2000 Sb. v §§ 44 – 46, případně ve smyslu zákona č. 40/2009 Sb., trestní zákoník (§ 180, dále §§ 230 – 232).
   b) informace o postupu přihlášení do systému EKIS MV, tzn.: údaje o ID uživatele a používaných heslech, nesmí být v žádné formě zapisovány do kalendářů, diářů, souborů na PC, poznámek na stole atd.;
   c) všechna externí elektromagnetická média obsahující osobní údaje, musí být uschovávána na zabezpečeném místě a zajištěna před neautorizovaným přístupem. V případě likvidace dat na těchto médiích musí být použita technologie bezpečného výmazu dat popř. likvidace médií;
   d) s nosiči informací (např. tiskové výstupy, elektromagnetická a optická záznamová média) obsahující osobní údaje dle zákona č. 101/2000 Sb., o ochraně osobních údajů, musí být nakládáno v souladu s tímto zákonem a s NMV č. 5/2008, kterým se vydává spisový a skartační řád MV;
   e) všechny zastaralé a/nebo nepoužitelné materiály, obsahující citlivé informace, musí být bezpečně zlikvidovány v souladu s platnými předpisy o likvidaci materiálů obsahujících citlivé informace;
   f) pokud je uživateli přiděleno více autorizací (např. autorizace administrátora a autorizace uživatele), musí být použita vyšší autorizace pouze na nezbytně nutnou dobu potřebnou pro činnosti vyžadující vyšší autorizaci;
   g) pracovní stanice musí být zajištěny před neautorizovaným užitím (zavedením přístupového hesla při spuštění počítače, spořiče obrazovky chráněné heslem s intervalem spuštění max. 5 minut, uzamykáním SW, příp. HW apod.); uživatel

mobilního zařízení musí učinit taková opatření, která jsou v dané situaci adekvátní k dosažení potřebného stupně fyzické bezpečnosti, která vyloučí možnost přístupu neoprávněné osoby k aktivům EKIS MV (v případě ztráty kontroly nad zařízením v důsledku kybernetického bezpečnostního incidentu, po předchozím posouzení IT administrátorem uživatelského útvaru, bezodkladně hlásit na Help Desk EKIS, v mimopracovní době na Situační a informační centrum Ministerstva vnitra/Help Desk MV, t: 974 801 [illegible], resp. v pracovní době Help Desk EKIS t: 974 [illegible]

Svým podpisem stvrzuji, že jsem byl/a poučen/a o bezpečnosti a ochraně dat v systému EKIS MV. Současně tento dokument slouží jako dohoda o mlčenlivosti.

Jméno pracovníka: OEČ/č. O[illegible] O[illegible]	Školení provedl: OEČ
Podpis / datum: ……..……..	Podpis / datum: ……