

SLUŽEBNÍ PŘEDPIS

náměstka ministra vnitra pro státní službu
ze dne 25. ledna 2017,

kterým se stanoví pravidla pro práci v Informačním systému o státní službě

Čl. 1**Úvodní ustanovení**

Pravidla pro práci v Informačním systému o státní službě (dále jen „ISoSS“) specifikují v souvislosti s § 180 odst. 1 zákona č. 234/2014 Sb., o státní službě, (dále jen „zákon“) povinnosti při práci v ISoSS, základní předpoklady užívání ISoSS, podmínky přístupu do ISoSS, zásady nakládání s údaji vedenými v ISoSS a zásady bezpečnosti a ochrany osobních údajů vedených v ISoSS.

Čl. 2**Základní pojmy**

Pro účely tohoto služebního předpisu se rozumí

- a) uživatelem státní zaměstnanec, který se registruje do ISoSS prostřednictvím Jednotného identitního prostoru Czech Point a Katalogu autentizačních a autorizačních služeb (JIP a KAAS) a na základě pověření služebního orgánu pracuje na portálu ISoSS, nebo zasílá data do ISoSS přímo z vlastního personálního systému prostřednictvím webových služeb. Typy uživatelů a jejich činnostní role jsou uvedeny v přílohách č. 1 a 2 k tomuto služebnímu předpisu,
- b) Portálem ISoSS rozhraní, které slouží k provádění úkonů dle § 180 odst. 1 zákona. Je přístupný všem služebním úřadům na internetové adrese <https://portal.isoss.cz>,
- c) SAP GUI ISoSS uživatelské rozhraní pro systém SAP (SAP Graphical User Interface) a součást ISoSS přístupná pouze oprávněným uživatelům zařazeným v Ministerstvu vnitra za účelem provádění úkonů dle § 13 a § 180 odst. 1 zákona v oblasti věcné, technické a provozní správy ISoSS,
- d) Servisdeskem ISoSS systém podpory uživatelů Portálu ISoSS, zajištěný
 1. zadáním dotazu nebo informace do formuláře přímo na Portálu ISoSS,
 2. zasláním dotazu nebo informace v elektronické podobě na adresu elektronické pošty: sd.isoss.ekis@mvcv.cz.

Čl. 3

Užívání ISoSS

(1) Uživatel odpovídá za to, že všechny jím činěné úkony v ISoSS jsou v souladu s právními a služebními předpisy, uživatelskými příručkami a s další dokumentací zveřejněnou v ISoSS v části Dokumenty ke stažení. V případě pochybností o tomto souladu se uživatel před učiněním úkonu v ISoSS obrátí na Servisdesk ISoSS prostřednictvím adresy elektronické pošty.

(2) Uživatel nesmí zadávat do ISoSS nepravdivé nebo neúplné údaje.

(3) Uživatel nesmí užívat ISoSS a údaje v něm obsažené k jinému účelu, než který je stanoven právními a služebními předpisy a vyplývá z jeho úkolů.

Čl. 4

Zásady bezpečnosti

(1) Při práci v ISoSS uživatel dodržuje povinnosti v oblasti kybernetické bezpečnosti ve smyslu zákona o kybernetické bezpečnosti¹⁾, jeho prováděcích právních předpisů a interních předpisů přijatých ve služebním úřadu k naplňování tohoto zákona a zvyšuje své bezpečnostní povědomí, zejména školením v aplikační bezpečnosti.

(2) Služební orgán pro účely školení v aplikační bezpečnosti jmenuje z uživatelů zařazených v jeho služebním úřadu bezpečnostního správce, který se účastní bezpečnostního školení pořádaného správcem ISoSS²⁾. Bezpečnostní správce školí další uživatele zařazené v jeho služebním úřadu a o provedeném školení informuje správce ISoSS.

(3) Uživatel chrání jemu přidělené přístupové údaje do ISoSS proti zneužití neoprávněnou osobou a brání tomu, aby další osoba měla přístup do ISoSS pod uživatelským účtem, který byl přidělen uživateli. Pokud zjistí, že jakákoliv osoba získala nebo by mohla získat neoprávněně přístup do ISoSS, je povinen přijmout ve spolupráci s pracovníky Servisdesku ISoSS opatření proti takovému neoprávněnému přístupu.

(4) Správce ISoSS je oprávněn jednostranně omezit užívání ISoSS zejména v případě údržby a aktualizace ISoSS, bezpečnostní hrozby, přičemž o tomto rozhodnutí je dle okolností a možností uživatel řádně a včas informován.

(5) Správce ISoSS je oprávněn, v případě zvláště závažného porušení zásad bezpečnosti, a to zejména v případě neoprávněného zasahování do údajů, zamezit uživateli v přístupu do ISoSS, a to s okamžitou platností. Neoprávněné zasahování do údajů představuje úmyslné a neoprávněné vymazání, poškození, znehodnocení, pozměnění nebo potlačení údajů v informačním systému, nebo jejich zneprístupnění.

¹⁾ Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

²⁾ § 180 odst. 2 zákona č. 234/2014 Sb., o státní službě.

Čl. 5**Mlčenlivost a ochrana údajů**

(1) Uživatel zachovává mlčenlivost o veškerých údajích zpracovávaných v souvislosti s prací v ISoSS a využívá tyto informace pouze za účelem řádného užívání systému v rozsahu svých oprávnění.

(2) Uživatel zajišťuje ochranu osobních údajů, se kterými pracuje, a zabezpečuje je proti zneužití.

Čl. 6**Nezbytná součinnost**

(1) Služební úřad poskytuje správci ISoSS veškerou potřebnou součinnost nutnou pro údržbu a aktualizaci ISoSS.

(2) Uživatel bez zbytečného odkladu oznámí pracovníkům Servisdesku ISoSS jakoukoli zjištěnou závadu ve funkčnosti ISoSS.

(3) Uživatel vyvíjí v rámci svých možností maximální úsilí k předcházení vzniku škod a k minimalizaci vzniklých škod.

(4) Služební úřad je povinen předem písemně uvědomit správce ISoSS o veškerých změnách týkajících se jeho oprávnění, které mohou mít vliv na užívání ISoSS.

Čl. 7**Služební předpisy služebních orgánů**

(1) Tento služební předpis stanovuje pouze minimální požadavky na práci v ISoSS. Služební orgán může služebním předpisem stanovit další požadavky dle specifických potřeb ve svém služebním úřadu.

(2) Služební předpis vydaný podle odstavce 1 stanoví zejména, jakým způsobem se vede jmenný seznam uživatelů vykonávajících činnosti v Portálu ISoSS k agendě Státní služba dle přílohy č. 2 k tomuto služebnímu předpisu.

Čl. 8**Služební předpis státního tajemníka v Ministerstvu vnitra**

Státní tajemník v Ministerstvu vnitra upraví služebním předpisem činnost uživatelů zařazených v Ministerstvu vnitra v oblasti správy a užívání Portálu ISoSS a SAP GUI ISoSS, včetně technické správy a provozu ISoSS.

Čl. 9**Účinnost**

Tento služební předpis nabývá účinnosti dnem 1. února 2017.

Č. j. MV-153920-14/SSS-2016

Náměstek ministra vnitra pro státní službu

RNDr. Josef POSTRÁNECKÝ v. r.