

**Odůvodnění ke služebnímu předpisu nejvyššího státního tajemníka  
ze dne 30. prosince 2024, kterým se stanoví pravidla pro práci  
v Informačním systému o státní službě**

## **OBECNÁ ČÁST**

### **1. Zhodnocení platného právního vztahu**

Informační systém o státní službě (dále jen „ISoSS“) je zřízen v § 180 odst. 1 zákona o státní službě a jeho účelem je vedení tímto zákonem vymezených údajů nezbytných pro správu organizačních věcí státní služby a služebních vztahů v rámci služebních úřadů i mezi nimi a činění některých úkonů podle tohoto zákona.

Na zpracování osobních údajů v ISoSS se vztahují povinnosti stanovené nařízením Evropského parlamentu a Rady (EU) 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) a zákonem č. 110/2019 Sb., o zpracování osobních údajů.

Vzhledem k tomu, že Informační systém o státní službě představuje významný informační systém veřejné správy, je rovněž nezbytné důsledně naplňovat požadavky v oblasti kybernetické bezpečnosti v návaznosti na zákon o kybernetické bezpečnosti ve spojení s vyhláškou 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), a to zejména podmínky přístupu uživatelů do ISoSS a bezpečnostní pokyny správce ISoSS, kterým je Ministerstvo vnitra.

### **2. Odůvodnění hlavních principů navrhované úpravy**

ISoSS obsahuje rejstřík státních zaměstnanců a zaměstnanců ve služebních úřadech, evidenci obsazovaných služebních míst, portál pro přihlašování na úřednickou zkoušku, evidenci uskutečněných úřednických zkoušek a evidenci systemizace a organizační struktury.

Návrh služebního předpisu nejvyššího státního tajemníka, kterým se stanoví pravidla pro práci v Informačním systému o státní službě, se předkládá v souvislosti s ustanovením § 180 odst. 1 a 2 zákona o státní službě, podle kterého je Informační systém o státní službě (dále také „ISoSS“) informačním systémem veřejné správy, jehož účelem je vedení údajů nezbytných pro správu organizačních věcí služby a služebních vztahů v rámci služebních úřadů i mezi nimi a činění některých úkonů podle zákona o státní službě. Správcem ISoSS je Ministerstvo vnitra, sekce pro státní službu plní roli věcného správce, přičemž technickou a provozní správu zajišťuje odbor informačních technologií ve spolupráci s NAKIT, s. p.

Návrhem služebního předpisu nejvyššího státního tajemníka se stanovují základní požadavky na práci státních zaměstnanců a zaměstnanců služebních úřadů v ISoSS, s přihlédnutím jak k zajištění bezpečnosti v oblasti zpracování a zabezpečení evidovaných osobních údajů, tak v oblasti základního naplňování požadavků kybernetické bezpečnosti, tj. ochrany přístupových údajů, hlášení zjištěných závad, oprávnění správce ISoSS omezit činnost v informačním systému v případě vzniku bezpečnostních hrozeb apod.

Činnosti prováděné za účelem vedení údajů nezbytných pro správu organizačních věcí služby a služebních vztahů a provádění některých úkonů podle zákona o státní službě by měly být v souladu s povinnostmi stanovenými v uvedených jiných právních předpisech a v neposlední řadě též v uživatelských příručkách a dalších dokumentacích zveřejněných na internetových stránkách sekce pro státní službu<sup>1</sup> nebo na Portálu ISoSS<sup>2</sup>.

## **ZVLÁŠTNÍ ČÁST**

### **K čl. 1**

Úvodní ustanovení odkazuje na právní předpisy, které mají přímý dopad na činnosti vykonávané v ISoSS.

### **K čl. 2**

Ustanovením se definují základní používané pojmy. Úlohu autentizačního informačního systému pro přístup na Portál ISoSS v současnosti zajišťuje Jednotný identitní prostor Czech Point a Katalog autentizačních a autorizačních služeb (JIP/KAAS), do kterého zadává jednotlivé uživatele a přiřazuje jim příslušné činnostní role lokální administrátor příslušného služebního úřadu. Autentizovanému uživateli jsou pak na základě přidělených činnostních rolí zpřístupněny příslušné moduly a funkcionality Portálu ISoSS. Ten je rovněž částečně přístupný veřejnosti (bez autentizovaného přístupu) v rozsahu, jaký definuje zákon o státní službě. Jde především o přístup k seznamu volných služebních míst, na jejichž obsazení bylo vyhlášeno výběrové řízení, a k seznamu termínů konání obecné části úřednické zkoušky nebo zvláštní části úřednické zkoušky v jednotlivých oborech služby. Ustanovení tohoto článku upravuje rovněž způsob komunikace prostřednictvím Servisdesk ISoSS, který slouží jako základní komunikační kanál mezi zaměstnanci služebních úřadů a manažery nastavení ISoSS.

---

<sup>1</sup> Dostupné z <https://www.mvcr.cz/sluzba/clanek/podpora-a-technicke-informace.aspx?q=Y2hudW09NQ%3d%3d>

<sup>2</sup> Dostupné z [https://portal.isoss.gov.cz/irj/portal/light/dokument?cd=servismenu/dokumenty\\_ke\\_stazeni\\_interni/\\_u\\_zivatelske\\_prirucky\\_a\\_souvisejici\\_pokyny](https://portal.isoss.gov.cz/irj/portal/light/dokument?cd=servismenu/dokumenty_ke_stazeni_interni/_u_zivatelske_prirucky_a_souvisejici_pokyny)

### **K čl. 3**

Ustanovení upravující užívání ISoSS apeluje na dodržování postupů stanovených uživatelskými příručkami a dalšími dokumenty publikovanými na internetových stránkách [portal.isoss.gov.cz](http://portal.isoss.gov.cz). Dodržení těchto postupů umožní správně a efektivně pracovat s moduly ISoSS, vyhnout se chybám, nutným zásahům prováděným manažery nastavení ISoSS a následným opravám. Vzhledem k tomu, že účelem ISoSS je vést údaje nezbytné pro správu organizačních věcí služby a služebních vztahů a činění některých úkonů dle zákona o státní službě, a také s ohledem na to, že některé vedené údaje jsou podle § 182 zákona o státní službě přístupné způsobem umožňujícím dálkový přístup, je nutné zadávat do ISoSS pravdivé a úplné údaje.

### **K čl. 4**

Ustanovení o pravidlech bezpečnosti reagují na aktuální povinnosti spojené s aplikací zákona o kybernetické bezpečnosti, zařazením ISoSS jako významného informačního systému a na případnou potřebu zásahu v případě ohrožení bezpečnosti ze strany správce systému. Naplňování parametrů kybernetické bezpečnosti je zásadně povinností správce systému. Ve vztahu k uživatelům upozorňuje čl. 4 na v podstatě základní a standardní potřeby chování uživatele informačních systémů. Zaměstnanec služebního úřadu, který pracuje se systémem ISoSS, je povinen dodržovat pravidla vydaná služebním předpisem, postupy formulované v uživatelských příručkách, technickém manuálu a dalších dokumentech publikovaných v Informačním systému o státní službě. Rovněž je povinen účastnit se školení v aplikační bezpečnosti za účelem zvyšování svého bezpečnostního povědomí v naplňování bezpečnostní politiky. Ustanovení o pravidlech přístupu upozorňuje na základní pravidla pro přistupování do ISoSS, zajištění ochrany přístupových údajů do významného informačního systému, který obsahuje osobní údaje státních zaměstnanců.

### **K čl. 5**

Ustanovení o zpracování a ochraně osobních údajů plně odkazuje na zákon o zpracování osobních údajů, jeho prováděcích právních předpisů a vnitřních předpisů přijatých ve služebním úřadu k naplňování tohoto zákona.

### **K čl. 6**

Ustanovení o poskytování součinnosti upozorňuje na základní povinnosti spojené s užíváním informačních systémů, jako je hlášení závad a potřebu nutné spolupráce při údržbě systému, např. při jeho aktualizaci a technických úpravách. Pokud je uživateli známo, že shodná závada již byla Servisdesku ISoSS oznámena jiným uživatelem, není nutné Servisdesk ISoSS opakovaně informovat. Cílem je dosáhnout efektivního procesu, který nezahltí ani Servisdesk ISoSS, ani jeho uživatele. V tomto ustanovení je rovněž stanovena povinnost služebního úřadu předem prostřednictvím Servisdesku uvědomit

Ministerstvo vnitra o veškerých změnách týkajících se jeho oprávnění, které mohou mít vliv na užívání ISoSS. Jde zejména o změny v ohlášené působnosti k agendě státní služba v Registru práv a povinností, které mohou nastat ze zákona nebo z jiné organizační změny služebního úřadu. Tato povinnost souvisí se správným nastavením přístupů jednotlivých služebních úřadů do ISoSS a k určitým činnostním rolím.

#### **K čl. 7**

Služební orgán může stanovit svým služebním předpisem další a podrobnější požadavky podle potřeb a specifík činností nebo organizace práce konkrétního služebního úřadu. Zároveň, s ohledem na ochranu osobních údajů, je potřebné vést jmenný seznam uživatelů ISoSS vykonávajících činnostní role na Portálu ISoSS. Jednotlivé činnostní role jsou uvedeny v příloze tohoto služebního předpisu. Z této evidence uživatelů je patrné, jaká oprávnění pro práci v ISoSS má nastavena konkrétní uživatel, tzn. do jakých modulů a funkcionalit ISoSS za konkrétní služební úřad nebo úřady vstupuje, s jakými údaji je oprávněn pracovat a jaké činnosti v rámci ISoSS provádí.

#### **K čl. 8**

Navrhovaný služební předpis ruší dosavadní služební předpis náměstka ministra vnitra pro státní službu č. 1/2017 ze dne 25. ledna 2017.

#### **K čl. 9**

Účinnost tohoto služebního předpisu se stanovuje od 1. ledna 2025.

#### **K příloze**

Příloha obsahuje výčet činnostních rolí přiřazených k výkonu agendy „A1761 - Státní služba“ v agendovém informačním systému Registr práv a povinností, včetně stručného popisu vykonávaných činností na základě přidělené role. Příslušnou činnostní roli jednotlivým uživatelům přiděluje na základě pověření služebního orgánu lokální administrátor v autentizačním informačním systému. Roli autentizačního informačního systému v současnosti plní JIP/KAAS, jehož správcem je Digitální a informační agentura. Správu uživatelských účtů v JIP provádí lokální administrátor na adrese <https://www.czechpoint.cz/spravadat/>.