

## Manuál pro žadatele

---

### nástroj OMIS

## Přímo řízené organizace MZD mohou bezplatně využívat nástroj OMIS pro podporu řízení kybernetické bezpečnosti

Přímo řízené organizace Ministerstva zdravotnictví ČR mohou bezplatně využívat nástroj **OMIS** od společnosti **Open Apps Development, a.s.** Nástroj je určen pro podporu řízení kybernetické bezpečnosti, zejména v oblasti správy systému řízení bezpečnosti informací, evidence aktiv a řízení rizik.

Ústav zdravotnických informací a statistiky ČR realizoval pořízení nástroje v rámci projektu „**Rozvoj resortní infrastruktury elektronického zdravotnictví ČR**“, vedeného pod registračním číslem **CZ.31.2.0/0.0/0.0/22\_033/0007725**. Softwarová podpora pro provozovatele je aktuálně zajištěna do listopadu 2030, samotná licence je časově neomezena.

Prostřednictvím tohoto článku je zprostředkována informace o možnosti jeho využití přímo řízenými organizacemi.

Záměrem bylo pořídit jednotné prostředí pro podporu řízení kybernetické bezpečnosti, které organizacím umožní systematicky pracovat s bezpečnostními informacemi, vyhodnocovat rizika, plánovat opatření a vytvářet potřebné přehledy a reporty.

### Účel nástroje OMIS

OMIS slouží jako podpůrný nástroj pro správu a auditování ISMS a pro vedení souvisejících evidencí v oblasti kybernetické bezpečnosti. Organizacím může pomoci zejména při identifikaci a hodnocení aktiv, posuzování hrozeb a zranitelností, řízení rizik a sledování navržených či realizovaných opatření.

Nástroj zároveň umožňuje mapovat vazby mezi jednotlivými oblastmi kybernetické bezpečnosti, například mezi aktivy, hrozbami, zranitelnostmi, riziky a opatřeními. Díky tomu může být využit nejen pro operativní evidenci, ale také pro manažerské řízení a průběžné vyhodnocování stavu kybernetické bezpečnosti v organizaci.

## Přínosy pro přímo řízené organizace

Využitím nástroje OMIS mohou přímo řízené organizace získat jednotný a strukturovaný způsob vedení údajů potřebných pro řízení kybernetické bezpečnosti. Nástroj může podpořit sjednocení postupů, lepší přehled o stavu aktiv a rizik, plánování bezpečnostních opatření i přípravu podkladů pro interní řízení, kontrolu nebo audit.

OMIS současně podporuje standardní proces řízení aktiv a rizik podle vzorové metodiky Národního úřadu pro kybernetickou a informační bezpečnost a je koncipován v souladu s principy, procesy a názvoslovím kybernetické bezpečnosti podle ISO/IEC 27001, ISO/IEC 27002 a požadavků směrnice NIS2 a její implementace do právního řádu ČR.

## Žádost o zpřístupnění nástroje

Přímo řízené organizace Ministerstva zdravotnictví ČR, které mají zájem nástroj OMIS využívat, mohou podat žádost o umožnění jeho používání.

Vzor žádosti je k dispozici ke stažení na adrese <https://www.uzis.cz/omis>. Do žádosti se doplní základní údaje o žadateli, kontakt na oprávněnou osobu žadatele pro zaslání přístupových údajů a vyplněnou a elektronicky podepsanou žádost se zašle na [mkb@uzis.cz](mailto:mkb@uzis.cz) nebo v písemně formě ve dvou vyhotoveních na podatelnu ústavu.

Žádost obsahuje přímo smluvní ujednání mezi žadatelem a provozovatelem. Po podepsání za obě strany budou na oprávněnou osobu zaslány přístupové údaje.