|  |  |
| --- | --- |
| **Aktualizace „Bezpečnostní dokumentace IS VaVaI“** | **343/B1** |
| ***Souhrn***  K zajištění systematického přístupu k řešení bezpečnosti informací, resp. kybernetické bezpečnosti, informačního systému pro vědu, výzkum a inovace (dále jen „IS VaVaI“), je v souladu s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a normy ČSN ISO/IEC 27001:2014 na Úřadu vlády České republiky zaveden systém řízení bezpečnosti informací (Information Security Management Systém - ISMS). **IS VaVaI splňuje všechny požadavky, a proto získal 11. února 2019 certifikát ISO/IEC 27001:2014.**  Rozsah řízení bezpečnosti ISMS je definován tak, aby byly jednoznačně vymezeny hranice, ve kterých je uplatňováno řízení bezpečnosti. V rámci definovaného rozsahu ISMS musí být „začleněna“ všechna aktiva IS VaVaI.  Bezpečnost IS VaVaI musí být založena na základě řízení rizik bezpečnosti informací.  K zajištění této zásady musí být přijata opatření a periodicky prováděno hodnocení rizik a na tomto základě stanovovány bezpečnostní cíle a opatření o ošetření rizik bezpečnosti IS VaVaI.  **Součásti „Bezpečnostní dokumentace IS VaVaI“**  **Politika bezpečnosti informací IS VaVaI** – stanovuje základní požadavky a pravidla  k zajištění bezpečnosti aktiv tohoto informačního systému. Vychází z požadavků zákona  č. 181/2014 Sb., o kybernetické bezpečnosti a dále též z normy ČSN ISO/IEC 27001:2014.  **Metodika identifikace a hodnocení aktiv IS VaVaI** – metodika stanovující způsob naplnění vybraných povinnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti v oblasti identifikace a správy informačních aktiv IS VaVaI.  **Metodika řízení rizik kybernetické bezpečnosti IS VaVaI** – metodika definující způsob naplnění vybraných povinnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti  v oblasti identifikace, analýzy a řízení rizik IS VaVaI.  **Příručka ISMS** – je základním dokumentem systému řízení bezpečnosti informací ISMS pro informační systém pro výzkum, vývoj a inovace, jsou v ní stanovena pravidla, postupy  a kompetence při provozování ISMS, bezpečnostní cíle, postupy a pravidla pro zajištění bezpečnosti aktiv IS VaVaI.  S ohledem na maximální zajištění stanovené úrovně bezpečnosti informací bude prováděno periodické, dokumentované monitorování a vyhodnocování bezpečnostních rizik a incidentů. Rovněž bude zajišťováno neustálé zlepšování bezpečnosti informací (tj. zabezpečení včasné dostupnosti informací, zamezení jejich neoprávněné modifikace, zneužití a ztráty) v souladu s obecně závaznými právními a interními předpisy a smluvními požadavky.  Předložená aktualizovaná „Bezpečnostní dokumentace IS VaVaI“ je závazná pro všechny dotčené zaměstnance Úřadu vlády České republiky, stejně jako pro členy Rady a případné další osoby, které IS VaVaI rozvíjejí, spravují nebo využívají. | |
| ***Přílohy***  Politika bezpečnosti informací IS VaVaI  Metodika identifikace a hodnocení aktiv IS VaVaI  Metodika řízení rizik kybernetické bezpečnosti IS VaVaI  Příručka ISMS  Certifikát ISO/IEC 27001:2014. | |