# Seznam podkladů a vzorů dokumentace k systému řízení bezpečnosti informací dle ČSN EN ISO/IEC 27001:2023 s podporou požadavků zákona č. 264/2025 Sb. (dříve z.č.181/2014 a vyhl. č. 82/2018)

- 01_Bezpečnostní příručka ISMS (ISO27001)
    - A1 Organizační schéma společnosti FIRMA – třeba vytvořit
    - A2 Fyzický perimetr – třeba vytvořit
    - A3 Logický bezpečnostní perimetr – třeba vytvořit
    - B1 Informační aktiva společnosti – identifikace a vlastníci
    - B2 Analýza rizik, popis metodiky
    - B3 Proces identifikace slabých míst
    - B4 Proces zvládání rizik
    - B5 Plán zvládání rizik
    - B6 Seznam a hodnocení rizik
    - B7 Aktiva, hrozby, zranitelnosti
    - C1 Zpráva o vyhodnocení rizik
    - C2 Prohlášení o Aplikovatelnosti (PoA)
    - D1 Plán kontinuity činností (BCP)
    - J1 Jmenování bezpečnostního manažera
    - J2 Jmenování představitele vedení pro ISMS
    - J3 Jmenování bezpečnostní komise
    - J4 Souhlas se zbytkovými riziky
    - P1 Pracovní postupy ISMS (část 1-4)
    - P2 Postup pro přezkoumání systému managementu bezpečnosti informací
    - Z1 Registr zákonných požadavků
    - Z2 Registr technických norem, směrnic a externí dokumentace
    - Z3 Registr záznamů ISMS a externí dokumentace – třeba vytvořit dle skutečnosti

- 02_Politika systému řízení bezpečnosti informací
- 03_Politika řízení aktiv
- 04_Politika organizační bezpečnosti
- 05_Politika řízení dodavatelů
- 06_Politika bezpečnosti lidských zdrojů
- 07_Politika řízení provozu a komunikací
- 08_Politika řízení přístupu
- 09_Politika bezpečného chování uživatelů
- 10_Politika zálohování a obnovy a dlouhodobého ukládání
- 11_Politika bezpečného předávání a výměny informací
- 12_Politika řízení technických zranitelností
- 13_Politika bezpečného používání mobilních zařízení
- 14_Politika akvizice, vývoje a údržby
- 15_Politika ochrany osobních údajů
- 16_Politika fyzické bezpečnosti
- 17_Politika bezpečnosti komunikační sítě
- 18_Politika ochrany před škodlivým kódem
- 19_Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
- 20_Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- 21_Politika bezpečného používání kryptografické ochrany
- 22_Politika řízení změn
- 23_Politika zvládání kybernetických bezpečnostních incidentů
- 24_Politika řízení kontinuity činností
- 25_Politika pro interní audit
- 26_Checklist 27001-23
- 27_Program interních auditů
- 28_Zpráva z auditu
- 29_Cíle ISMS
- 30_Monitorování ISMS, ukazatele a hodnocení
- 31_Zpráva z přezkoumání vedením
- 32_Dopadová analýza pro kontinuitu podnikání- šablony BIA