**Příloha k Žádosti o certifikaci č. ZCS /Z**

*(vyplní certifikační orgán)*

Dotazník vyplňujte zaškrtnutím příslušného políčka, případně použijte kolonky pro poznámky, kde uvedete bližší specifikaci.

V případě potřeby Vám s vyplněním dotazníku pomůže pracovník certifikačního orgánu DOM-ZO 13, s.r.o. na kontaktech uvedených v žádosti.

|  |
| --- |
| Požadavky dle ISO/IEC 27001:2022 |
| 4. Kontext organizace |
| Máte určeny externí a interní aspekty významné z hlediska ISMS? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte určeny zainteresované strany (ZS) a jejich požadavky z hlediska bezpečnosti informací? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte stanoven rozsah ISMS zohledňující jeho hranice a aplikovatelnost, zvažující externí a interní aspekty, požadavky ZS a propojení s jinými organizacemi)? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte ustaven, implementován, udržován, monitorován a neustále zlepšován ISMS? | [ ]  ANO | [ ]  NE | Pozn.: |
| 5. vůdčí role |
| Máte stanovenou politiku a cíle bezpečnosti informací? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte zajištěnou integraci požadavků ISMS do procesů organizace?  | [ ]  ANO | [ ]  NE | Pozn.: |
| Zajišťuje vedení organizace dostupnost zdrojů potřebných pro ISMS? | [ ]  ANO | [ ]  NE | Pozn.: |
| Je komunikován význam efektivního ISMS a význam dosažení shody s požadavky ISMS? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte určeny role a stanoveny odpovědnosti, pravomoci a vzájemné vztahy všech pracovníků, kteří provádějí činnosti ovlivňující ISMS? | [ ]  ANO | [ ]  NE | Pozn.: |
| Je vedením prosazováno a zajištěno neustálé zlepšování ISMS? | [ ]  ANO | [ ]  NE | Pozn.: |
| 6. plánování |
| Máte definovaný a aplikujete proces posuzování rizik bezpečnosti informací?  | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte vybrány cíle opatření a jednotlivá opatření z přílohy A normy ISO/IEC 27001? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte vytvořené Prohlášení o aplikovatelnosti? (Do poznámky prosím uveďte platnou verzi.) | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte formulován a zaveden plán ošetření rizik bezpečnosti informací? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte stanoveny cíle bezpečnosti informací relevantní jednotlivým funkcím a úrovním řízení? | [ ]  ANO | [ ]  NE | Pozn.: |
| **7. PODPORA** |
| Máte určeny nezbytné kompetence a zajišťujete tyto kompetence u pracovníků, kteří mají vliv na výkonnost ISMS a udržujete o tom dokumentované informace? | [ ]  ANO | [ ]  NE | Pozn.: |
| Jsou pracovníci seznámeni s politikou bezpečnosti informací a jsou si vědomy svého přínosu k efektivnosti ISMS a důsledků nepřizpůsobení se požadavkům ISMS? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte zaveden proces interní a externí komunikace? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte stanoven rozsah dokumentovaných informací?  | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte zaveden a uplatňován proces řízení dokumentovaných informací? | [ ]  ANO | [ ]  NE | Pozn.: |

|  |
| --- |
| 8. provozování |
| Máte plánovány, implementovány a realizovány procesy potřebné z hlediska provozu ISMS? | [ ]  ANO | [ ]  NE | Pozn.: |
| Provádíte v pravidelných intervalech posouzení rizika bezpečnosti informací a uchováváte dokumentované informace o výsledcích posuzování? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte zaveden a uplatňujete plán ošetření rizik bezpečnosti informací a uchováváte dokumentované informace o výsledcích ošetření? | [ ]  ANO | [ ]  NE | Pozn.: |
| 9. hodnocení výkonnosti |
| Vyhodnocujete výkonnost bezpečnosti informací a efektivnost ISMS? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte stanoveny ukazatele výkonnosti bezpečnosti informací a vytvořeny procesy pro jejich monitorování, měření, analýzu a vyhodnocování? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte zajištěno provádění pravidelných interních auditů ISMS včetně postupu a odborné způsobilosti interních auditorů? Provedli jste alespoň jeden interní audit pokrývající rozsah požadované certifikace? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte zajištěno provádění pravidelného přezkoumání ISMS vedením včetně vyhodnocení a rozhodnutí vztahující se k příležitostem neustálého zlepšování a příslušných dokumentovaných informací? Bylo provedeno během provozování vašeho ISMS alespoň jednou přezkoumání vedením? | [ ]  ANO | [ ]  NE | Pozn.: |
| **10. zlepšování** |
| Máte zaveden proces řízení neshod a udržujete záznamy jako dokumentované informace o podstatě neshod a následných přijatých opatření, výsledcích nápravných opatření a opatření k zamezení opakování neshody? | [ ]  ANO | [ ]  NE | Pozn.: |
| Využíváte výstupy z hodnocení výkonnosti pro identifikaci potřeby a příležitosti ke zlepšování? | [ ]  ANO | [ ]  NE | Pozn.: |
| Realizujete naplňováním stanovených cílů bezpečnosti neustálé zlepšování vhodnosti, přiměřenosti a efektivnosti ISMS? | [ ]  ANO | [ ]  NE | Pozn.: |
| Doplňující poznámky: |

|  |
| --- |
| údaje o podniku / organizační jednotceV případě více organizačních jednotek je třeba vyplnit všechny potřebné údaje ke každé organizační jednotce zahrnuté do rozsahu certifikace! |
| **Organizační jednotka (sídlo, provozovna, lokalita)**Název a adresa: |
| Činnosti realizované v organizační jednotce: |  |
| Počet zaměstnanců podstatných pro ISMS: |  |
| Počet pracovníků na částečný úvazek: |  |
| **Podrobnosti k IT infrastruktuře** |
| Přibližný počet uživatelů (pro finanční služby, státní správu, nemocniční systémy apod.) |  |
| Počet serverů: |  |
| Umístění serverů (geografické umístění): |  |
| Počet pracovních stanic: |  |
| Počet pracovníků používajících pracovní stanice: |  |
| Počet platforem IT: |  |
| Počet operačních systémů: |  |
| Počet operačních databází: |  |
| Počet sítí: |  |
| Počet internetových připojení: |  |
| Typ připojení: |  |
| Jak velký podíl (%) představuje práce na dálku? |  |
| Používáte šifrování? | [ ]  ANO | [ ]  NE | Pozn.: |
| Pokud ano, uveďte, jakou síťovou a šifrovací technologii používáte: |  |
| S jakým objemem dat pracujete? | [ ]  malý | [ ]  střední | [ ]  velký |
| **Podrobnosti k obchodním činnostem** |
| Uveďte oborově – specifická rizika (např.: zdravotní péče, vzdělávání, telekomunikace, peněžní služby, společnost registrovaná na burze, citlivé státní informace…): |  |
| Typ komerčních a regulatorních požadavků: | [ ]   | organizace působí v nekritických komerčních a v neregulovaných oborech |
| [ ]  | organizace má zákazníky v kritických komerčních oborech |
| [ ]  | organizace působí v kritických komerčních oborech |
| Uveďte právní a jiné požadavky v oblasti zabezpečení Vašich informací: |  |  |
| Úroveň závislosti na outsourcovaných a dodavatelských činnostech: | [ ]   | žádná nebo malá závislost |
| [ ]  | určitá závislost vztahující se k některým, ale ne ke všem podnikatelským činnostem |
| [ ]  | velká závislost, velký dopad na významných podnikatelských činnostech |
| Pokud ano, jaký z Vašich procesů outsourcujete: |  |
| Vývoj informačního systému: | [ ]   | žádný nebo velmi nízký vlastní nebo outsourcovaný vývoj systému nebo aplikací |
|  | [ ]  | vlastní nebo outsourcovaný vývoj systému nebo aplikace pro některé významné podnikatelské záměry |
|  | [ ]  | rozsáhlý vlastní nebo systému nebo outsourcovaný vývoj systému nebo aplikace pro významné podnikatelské záměry |
| Provádíte elektronické peněžní transakce? | [ ]  ANO | [ ]  NE | Pozn.: |
| Máte oddělení IT nebo manažera IT? | [ ]  ANO | [ ]  NE | Pozn.: |
| Pracujete s citlivými informacemi?  | [ ]  ANO | [ ]  NE | Uveďte jaké: |
| Existují záznamy ISMS, které nemohou být zpřístupněné pro audit z důvodu obsahu důvěrných nebo citlivých informací (např. certifikát NBÚ): | [ ]  ANO | [ ]  NE | Uveďte jaké: |
| Je nutné, aby auditní tým absolvoval nějaké zvláštní školení nebo prověření týkající se důvěrnosti informací, resp. bezpečnosti práce? | [ ]  ANO | [ ]  NE | Uveďte jaké: |
| Které z činnosti prováděných Vaší organizací u zákazníka nejvíce souvisejí s riziky bezpečnosti informací, resp. ohrožením jejich bezpečnosti: |  |
| Doplňující poznámky: |

S informacemi získanými o Vaší společnosti bude zacházeno jako s důvěrnými a jejich předání třetím osobám nebo zveřejnění může být provedeno jen se souhlasem subjektu a certifikačního orgánu.

Dotazník zpracoval (jméno, datum, podpis): ................................................................................................................