|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hodnocení úrovně kybernetické bezpečnosti dodavatele**  **Splnění podmínek dle vyhlášky č. 82/2018 Sb.** | | | | |
| **Dodavatel (název společnosti):** | |  | | |
| **IČO:** | |  | | |
| **Sídlo:** | |  | | |
|  | | | | |
| **Postup vyplnění:** | | | | |
| Dodavatel odpoví na všechny otázky v SEKCI A – E (***Ano / Ne / Neaplikovatelné***) | | | | |
| V rámci hodnocení rizikovosti dodavatele má každá otázka, resp. podotázka, stejnou hodnotu jednoho bodu. | | | | |
|  |  | | ***Vyplní dodavatel*** |
| **SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY** | | | | |
| A-1 | Které standardy a postupy nejlepší praxe organizace dodavatele využívá v rámci poskytování služeb (tam, kde je to relevantní, na certifikované úrovni): | | | |
| A-1.1 | Systém řízení bezpečnosti informací, např. ISO/IEC 27001 | |  |
| A-1.2 | Systém řízení IT služeb, např. ISO/IEC 20000-1, ITIL – Information Technology Infrastructure Library, COBIT – Control Objectives for Information and related Technology | |  |
| A-2 | Audity provedené subjektem akreditovaným ČIA nebo obdobným subjektem v rámci EU pro poskytování certifikačních služeb: | | | |
| A-2.1 | Certifikační nebo dohledový audit, dle otázky Sekce A 1.1, v posledních dvou letech | |  |
| A-2.2 | Jsou prováděny pravidelné audity systému řízení bezpečnosti informací interním subjektem dodavatele | |  |
| A-3 | Dodavatel se v rámci zakázky vyvaruje použití technologií výrobců uvedených ve varování NÚKIB č.j. 3012/2018-NÚKIB-E/110 ze dne 17. prosince 2018 k používání technických nebo programových prostředků společností, Huawei Technologies co., Ltd. a ZTE Corporation | |  |

|  |  |  |
| --- | --- | --- |
| **SEKCE B – ZÁKLADNÍ OPATŘENÍ** | | |
| B-1.1 | Má organizace dodavatele manažera kybernetické bezpečnosti nebo jinou určenou osobu s ekvivalentní odpovědností |  |
| B-1.2 | Byl v organizaci dodavatele v posledních 12-ti měsících proveden třetí stranou audit či analýza, jejichž obsahem byla kontrola v oblasti kybernetické bezpečnosti |  |
| B-1.3 | Bylo v organizaci dodavatele v posledních 12-ti měsících provedeno hodnocení rizik v oblasti kybernetické bezpečnosti |  |
| B-1.4 | Je dodavatel vůči nějaké organizaci v postavení Významného dodavatele dle zákona č. 181/2014 Sb. |  |
| B-1.5. | Organizace dodavatele má zaveden proces řízení rizik |  |
| B-1.6. | Organizace dodavatele má zavedenu klasifikaci aktiv/informací |  |
| B-1.7. | Je implementována ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti |  |
| B-1.8. | Organizace dodavatele má zavedeny postupy k ochraně osobních dat |  |
| B-1.9 | Identifikace a autentizace uživatelů |  |
| B-1.10 | Přístup k datům je řízen na základě rolí RBAC – Role Based Access Control |  |
| B-1.11 | Řízení privilegovaných přístupů |  |
| B-1.12 | Je implementována ochrana koncových stanic |  |
| B-1.13 | Je implementována ochrana mobilních zařízení a vzdáleného přístupu |  |
| B-1.14 | Je implementována ochrana e-mailů a vnitrofiremní komunikace |  |
| B-1.15 | Jsou zavedeny procesy řízení změn |  |
| B-1.16 | Je implementována ochrana bezdrátových sítí a komunikace |  |
| B-1.17 | Jsou zavedeny procesy fyzické bezpečnosti aktiv |  |
| B-1.18 | Je prováděno pravidelné bezpečnostní školení koncových uživatelů a administrátorů |  |
| B-1.19 | Je implementována ochrana proti škodlivému softwaru |  |
| B-1.20 | Jsou nastaveny procesy zvládání kybernetických incidentů |  |
| B-1.21 | Jsou nastaveny procesy řízení rizik poddodavatelů/subdodavatelů |  |
| B-1.22 | Jsou zavedeny procesy v oblasti bezpečnosti lidských zdrojů |  |
| B-1.23 | Jsou prováděny bezpečnostní audity a analýzy |  |
| B-1.24 | Je implementováno řízení kontinuity činností a havarijní plánování |  |

|  |  |  |
| --- | --- | --- |
| **SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE** | | |
| C-1 | Které níže uvedené bezpečnostní technologie organizace dodavatele provozuje s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním systémům: | |
| C-1.1 | Antivirový software na pracovních stanicích |  |
| C-1.2 | Nástroj pro detekci narušení sítě IDS/IPS – Intrusion Detection / Prevention System |  |
| C-1.3 | Nástroj pro řízení privilegovaných účtů a oprávnění PIM/PAM – Priviledge Identity / Access Management |  |
| C-1.4 | Více-faktorová autentizace |  |
| C-1.5 | Automatizovaný nástroj pro řízení technologických zranitelností |  |
| C-1.6 | Nástroj pro řízení přístupu k síti NAC – Network Access Control |  |
| C-1.7 | Nástroj na ochranu před útoky DDoS – Distributed Denial‑of‑Service |  |
| C-1.8 | Šifrovací nástroje a techniky |  |
| C-1.9 | Firewall kategorie Next Generation |  |
| C-1.10 | Nástroj pro vyhodnocování bezpečnostních událostí SIEM – Security Information and Even Management |  |
| C.1.11 | Byly interní systémy organizace dodavatele v posledních 12-ti měsících podrobeny penetračnímu testování |  |

|  |  |  |
| --- | --- | --- |
| **SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTU** | | |
| D-1 | Má organizace dodavatele zaveden proces zvládání kybernetických incidentů? |  |
| D-2 | Jsou zaměstnanci organizace dodavatele pravidelně vzděláváni v identifikaci kybernetických incidentů? |  |

|  |  |  |
| --- | --- | --- |
| **SEKCE E – KOMUNIKACE BEZPEČNOSTI a VZDĚLÁVÁNÍ** | | |
| E-1 | Má organizace dodavatele zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro zaměstnance? |  |
| E-2 | Jsou noví zaměstnanci organizace dodavatele vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům? |  |
| E-3 | Dokumentuje organizace dodavatele účast zaměstnanců na bezpečnostních školeních a vzdělávacích programech? |  |
| E-4 | Vyžaduje organizace dodavatele po zaměstnancích s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti? |  |

Dne:

|  |  |  |
| --- | --- | --- |
| za dodavatele vyplnil: |  |  |
|  | *jméno, příjemní* | *podpis* |