Splnění podmínek dle vyhlášky č. 82/2018 Sb.

Hodnocení úrovně kybernetické bezpečnosti účastníka

Postup vyplnění:		
	1. Účastník odpoví na všechny otázky v SEKCI A - E.	
	2. Účastník doloží splnění otázky označené hvězdičkou samostatným dokumentem nebo certifikátem	
	3. Účastník může vymazat hodnotu buňky klávesou DEL.	
	Každá otázka, resp. podotázka má stejnou bodovou hodnotu.	
	Zbývá vyplnit 0 otázek.	
SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY		
1	**Které standardy a postupy nejlepší praxe organizace účastníka využívá v rámci poskytování služeb (tam, kde je to relevantní, na certifikované úrovni):**	
a.	systém řízení kvality, například ISO 9001, CAF, TQM	
b.	systém řízení bezpečnosti informací, například ISO/IEC 27001 *	
c.	systém řízení ochrany osobních údajů dle ISO / IEC 27701	
d.	systém řízení kontinutiy podnikových procesů, například ISO 22301	
e.	systém řízení IT služeb, například ISO/IEC 20000-1, ITIL, CobIT	
2	**Audity provedené subjektem akreditovaným ČIA nebo obdobným subjektem v rámci EU pro poskytování certifikačních služeb**	
a.	Certifikační nebo dohledový audit, dle otázky Sekce A 1.a v posledních dvou letech	
b.	Certifikační nebo dohledový audit dle otázky Sekce A 1.b v posledních dvou letech	
c.	Certifikační nebo dohledový audit dle otázky Sekce A 1.c v posledních dvou letech	
d.	Certifikační nebo dohledový audit dle otázky Sekce A 1.d v posledních dvou letech	
e.	Certifikační nebo dohledový audit dle otázky Sekce A 1.e v posledních dvou letech	
3	**Audit Významného dodavatele provedený správcem KII nebo VIS**	
a.	Audit Významného dodavatele dle zákona 181/2014 Sb. Správcem KII	
b.	Audit Významného dodavatele dle zákona 181/2014 Sb. Správcem VIS	
SEKCE B – ZÁKLADNÍ OPATŘENÍ		
1	Má organizace účastníka manažera kybernetické bezpečnosti nebo jinou určenou osobu s ekvivalentní odpovědností *	
2	Byl v organizaci v posledních 12ti měsících proveden třetí stranou audit či analýza, jejichž obsahem byla kontrola v oblasti kybernetické bezpečnosti	
3	Bylo v organizaci v posledních 12ti měsících provedeno hodnocení rizik v oblasti kybernetické bezpečnosti	
4	Je účastník vůči nějaké organizaci v postavení Významného dodavatele dle zákona 181/2014 Sb.*	
5	**Které oblasti pokrývá dokument bezpečnostní politiky, pokud v organizaci účastníka existuje?**	
a.	Procesy řízení rizik	
b.	Klasifikace aktiv	
c.	Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti *	
d.	Ochrana osobních dat *	
e.	Identifikace a autentizace uživatelů *	
f.	Přístup k datům na základě rolí (RBAC, Role Based Access Control)	
g.	Řízení privilegovaných přístupů *	
h.	Ochrana koncových stanic	
i.	Ochrana mobilních zařízení a vzdáleného přístupu	
j.	Ochrana emailu a vnitrofiremní komunikace (instant messaging)	
k.	Ochrana přístupu do internetu	
l.	Ochrana médií	
m.	Procesy řízení změn	
n.	Ochrana bezdrátových sítí a komunikace	
o.	Fyzická bezpečnost informačních aktiv	
p.	Bezpečnostní školení koncových uživatelů a administrátorů *	
q.	Ochrana proti škodlivému softwaru	
r.	Ochrana při výměně dat	
s.	Procesy zvládání kybernetických incidentů *	
t.	Procesy řízení rizik dodavatelů	
u.	Bezpečnost lidských zdrojů *	
v.	Bezpečnostní audity a analýzy	
w.	Řízení kontinuity činností a havarijní plánování	

SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE		
1	**Které níže uvedené bezpečnostní technologie organizace účastníka provozuje s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním systémům?**	
a.	Antivirový software na pracovních stanicích *	
b.	Antivirový software na mobilních zařízeních	
c.	Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System)*	
d.	Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management)	
e.	Více-faktorová autentizace	
f.	Automatizovaný nástroj pro řízení technologických zranitelností	
g.	Nástroj pro řízení přístupu k síti (NAC, Network Access Control)	
h.	Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service)	
i.	Šifrovací nástroje a techniky	
j.	Firewall kategorie Next Generation *	
k.	Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management)	
2	Byly interní systémy organizace účastníka v posledních 12ti měsících podrobeny penetračnímu testování?	
SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ		
1	Má organizace účastníka zaveden proces zvládání kybernetických incidentů? *	
2	Jsou všichni zaměstnanci organizace účastníka pravidelně (min. 1x ročně) vzdělávání v identifikaci kybernetických incidentů?	
SEKCE E – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ		
1	Má organizace účastníka zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro zaměstnance? *	
2	Jsou noví zaměstnanci organizace účastníka vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům? *	
3	Dokumentuje organizace účastníka účast pracovníků na bezpečnostních školeních a vzdělávacích programech?	
4	Vyžaduje organizace účastníka po zaměstnancích s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?	
5	Vyžaduje organizace účastníka po zaměstnancích podepsání etického kodexu?	
	Zbývá vyplnit 0 otázek.	

[redacted]