Příloha č.4 Formuláře nabídky *"Služby podpory provozu a rozvoje CA Service Desk Manager MPSV II"*

Prokázání úrovně kybernetické bezpečnosti dodavatele a poddodavatelů

Pododavatel: CATTA Consulting s.r.o.

Postup vyplnění:

1. Dodavatel odpoví na **VŠECHNY** otázky v SEKCI A - E.
2. Dodavatel nemusí vyplňovat odpovědi na NEPOVINNÉ OTÁZKY.
3. Dodavatel a poddodavatelé vyplňují každý vlastní tabulku podle stavu bezpečnosti jejich vlastního prostředí.

Zbývá vyplnit 0 otázek.

SEKCE A – STANDARDY A NEJLEPŠÍ PRAKTIKY		
1	Které standardy a nejlepší praktiky na své informační systémy organizace dodavatele aplikuje:	
a.	ISO 9001	ANO
b.	ISO/IEC 27001	ANO
c.	ISO 22301, BS 25999	ANO
d.	ISO/IEC 20000-1, ITIL, CobIT	ANO
SEKCE B – ZÁKLADNÍ OPATŘENÍ		
2	Má organizace dodavatele manažera bezpečnosti nebo jinou určenou osobu s ekvivalentní odpovědností?	ANO
3	Byl v organizaci v posledních 12ti měsících proveden třetí stranou audit či analýza, jejichž obsahem byla kontrola v oblasti informační bezpečnosti?	ANO
4	Bylo v organizaci v posledních 12ti měsících provedeno hodnocení rizik v oblasti informační bezpečnosti?	ANO
5	Které oblasti pokrývá dokument bezpečnostní politiky, pokud v organizaci dodavatele existuje?	
a.	Procesy řízení rizik	ANO
b.	Klasifikace aktiv	ANO
c.	Ochrana dat proti prozrazení, zničení, narušení integrity a dostupnosti	ANO
d.	Ochrana osobních dat	ANO
e.	Identifikace a autentizace uživatelů	ANO
f.	Přístup k datům na základě rolí (RBAC, Role Based Access Control)	ANO
g.	Řízení privilegovaných přístupů	ANO
h.	Ochrana koncových stanic	ANO
i.	Ochrana mobilních zařízení a vzdáleného přístupu	ANO
j.	Ochrana emailu a vnitrofiremní komunikace (instant messaging)	ANO
k.	Ochrana přístupu do internetu	ANO
l.	Ochrana médií	ANO
m.	Procesy řízení změn	ANO
n.	Ochrana bezdrátových sítí a komunikace	ANO
o.	Fyzická bezpečnost informačních aktiv	ANO
p.	Bezpečnostní školení koncových uživatelů a administrátorů	ANO
q.	Ochrana proti škodlivému softwaru	ANO
r.	Ochrana při výměně dat	ANO
s.	Procesy zvládání kybernetických incidentů	ANO
t.	Procesy řízení rizik dodavatelů	ANO
u.	Bezpečnost lidských zdrojů	ANO
v.	Bezpečnostní audity a analýzy	ANO
w.	Řízení kontinuity činností a havarijní plánování	ANO
SEKCE C – BEZPEČNOSTNÍ TECHNOLOGIE		
6	Které níže uvedené bezpečnostní technologie organizace dodavatele provozuje s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním systémům?	
a.	Antivirový software na pracovních stanicích	ANO
b.	Antivirový software na mobilních zařízeních	ANO
c.	Nástroj pro detekci narušení sítě (IDS/IPS, Intrusion Detection/Prevention System)	ANO
d.	Nástroj pro řízení privilegovaných účtů a oprávnění (PIM/PAM, Priviledge Identity/Access Management)	ANO
e.	Více-faktorová autentizace	ANO
f.	Automatizovaný nástroj pro řízení technologických zranitelností	ANO
g.	Nástroj pro řízení přístupu k síti (NAC, Network Access Control)	ANO
h.	Nástroj pro ochranu před útoky DDoS (Distributed denial-of-service)	ANO
i.	Šifrovací nástroje a techniky	ANO
j.	Firewall	ANO
k.	Nástroj pro vyhodnocování bezpečnostních událostí (SIEM, Security Informaton and Event Management)	ANO
7	Byly interní systémy organizace dodavatele v posledních 12ti měsících podrobeny penetračnímu testování?	ANO
SEKCE D – PROCES ZVLÁDÁNÍ KYBERNETICKÝCH INCIDENTŮ		
8	Má organizace dodavatele zaveden proces zvládání bezpečnostních incidentů?	ANO
9	Jsou všichni zaměstnanci organizace dodavatele pravidelně (min. 1x za 24 měsíců) vzdělávání v identifikaci bezpečnostních incidentů?	ANO
SEKCE E – KOMUNIKACE BEZPEČNOSTI A VZDĚLÁVÁNÍ		
10	Má organizace dodavatele zaveden proces vzdělávání a zvyšování bezpečnostního povědomí pro zaměstnance?	ANO
11	Jsou noví zaměstnanci organizace dodavatele vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům?	ANO
12	Dokumentuje organizace dodavatele účast pracovníků na bezpečnostních školeních a vzdělávacích programech?	ANO
13	Vyžaduje organizace dodavatele po zaměstnancích s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?	ANO
14	Vyžaduje organizace dodavatele po zaměstnancích podepsání etického kodexu?	ANO

Zbývá vyplnit 0 otázek.

NEPOVINNÉ OTÁZKY		
101	Je organizace dodavatele orgánem nebo osobou povinnou dle §3 zákona 181/2014 o kybernetické bezpečnosti?	NE
102	Má organizace dodavatele zaveden certifikovaný systém řízení dle ISO/IEC 27001:2005?	ANO
103	Jsou dodavatelé organizace dodavatele vyškoleni v oblasti kybernetické bezpečnosti dříve, než získají přístup k datům a informačním systémům?	ANO
104	Vyžaduje organizace dodavatele po pracovnících dodavatele s přístupem k datům a informačním systémům podepsání individuální dohody o mlčenlivosti?	ANO
105	Jaké negativní dopady pocítila organizace dodavatele v souvislosti s kybernetickým incidentem, pokud v minulosti nastal:	
a.	Výpadek sítě	NE
b.	Nedostupnost emailu a kancelářských aplikací	NE
c.	Neoprávněné zneužití identity	NE
d.	Prozrazení chráněných dat	NE
e.	Ztráta nebo zničení dat	NE
f.	Finanční ztráta	NE
g.	Ztráta duševního vlastnictví	NE
h.	Poškození pověsti organizace dodavatele	NE
i.	Negativní publicita v médiích	NE
j.	Ztráta hodnoty organizace dodavatele	NE
k.	Trestní stíhání organizace dodavatele	NE