cendis

PŘEHLED POSKYTNUTÝCH SLUŽEB:

	0,00
(neobsazeno)	0,00
CELKEM :	**0,00**

Smlouva o poskytování služeb	**ze dne**	**evidenční číslo**
Požadavek	**ze dne**	**evidenční číslo**
Dodavatel		
ICT odborník		

Přehled činností (EXT)

Datum	Pracovník	Projekt	Objednávka	Upřesnění činnosti	Výstupy	ČLH
					Celkem	**0,00**

Schvalovací doložka

	Jméno a příjmení	Datum	Podpis	Organizace
Vyhotovil				
Schválil				CENDIS, s. p.

Akceptační protokol CEN/2023/XX

SMLOUVA O POSKYTOVÁNÍ SLUŽEB	
POŽADAVEK	
DODAVATEL	
ICT ODBORNÍK	
OBJEDNATEL	CENDIS, s. p.
PŘEDMĚT AKCEPTACE	
DATUM	
ZÚČTOVACÍ DATA	0X23/xx.xxx,xx Kč bez DPH

1. Předmět akceptace

ČÍSLO	POPIS	AKCEPTOVÁNO	VÝHRADA
1		ANO	NE

* Akceptováno / Akceptováno s výhradou / Neakceptováno

2. Seznam příloh

ČÍSLO	POPIS
1	Měsíční výkaz za období XX/2023
2	

3. Seznam výhrad

ČÍSLO VÝHRADY	POPIS	DATUM VYPOŘÁDÁNÍ
-	-	-

4. Podpisová doložka

S výsledky akceptace souhlasím.

V Praze dne:

CENDIS, s. p.

_____

5. Akceptace

Zástupce dodavatele CENDIS, s. p. a zástupce dodavatele svým podpisem stvrzují Předání a Akceptaci Předmětu plnění dle výše specifikovaných služeb.

	DODAVATEL/OBJEDNATEL	JMÉNO	DATUM	PODPIS
PŘEDAL				
AKCEPTOVAL	CENDIS, s. p.	Ing. Jan Paroubek		

Prohlášení o zachování mlčenlivosti a zajištění bezpečnosti informací CENDIS, s.p.

Já, níže podepsaný/á žadatel/ka čestně prohlašuji, že:

1. budu používat svěřené přístupy, vybavení a svěřené předměty pouze k plnění činností vyplývajících z výše uvedené smlouvy (pracovní smlouva, smluvní vztah);
2. nebudu pod privilegovaným přístupem instalovat SW bez předchozího schválení Manažerem provozu;
3. nebudu zneužívat privilegovaný přístup k získání přístupových údajů uživatelů CENDIS, s.p.;
4. nebudu testovat a prověřovat bezpečnostní slabiny v systémech a nastavených procesech CENDIS, s.p.;
5. v případě nevyužití dvoufaktorové autentizace budu vytvářet silná a bezpečná (obtížně uhodnutelná) hesla a při jejich vytváření budu dodržovat následující pravidla v souladu s Vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti:
    a) jsem-li uživatel VIS (významný informační systém), minimální délka hesla je 12 znaků;
    b) jsem-li administrátor VIS, minimální délka hesla je 17 znaků;
    c) při tvorbě hesla použít min. 3 z následujících požadavků:
        i) nejméně jedno malé písmeno (a-z);
        ii) nejméně jedno velké písmeno (A-Z);
        iii) nejméně jednu číslici (0–9);
        iv) nejméně jeden speciální znak (např. . - +), znaky s diakritikou jsou zakázány;

    zároveň budu vytvářet dostatečně silná hesla i mimo VIS;
6. tato hesla budu pravidelně měnit, minimálně jednou za 120 dní;
7. nebudu používat stejná hesla pro různé systémy (zejména nebudu používat stejná hesla, jako používám v rámci své společnosti, u jiných organizací, popř. v soukromé činnosti);
8. nebudu začleňovat hesla do jakýchkoliv automatizovaných přihlášení, např. uložená ve webovém prohlížeči, makru nebo pod funkční klávesou, stejně jako nebudu ukládat hesla do jiných než bezpečnostním ředitelem CENDIS, s.p. schválených manažerů hesel (v současné době KeePassXC v kombinaci s YubiKey tokenem);
9. budu udržovat heslo v naprosté tajnosti a nakládat s ním tak, aby nemohlo jeho prozrazením dojít ke zneužití účtu neoprávněným vstupem do systému jinou osobou;
10. v případě prozrazení nebo podezření na jeho prozrazení jej okamžitě změním a neprodleně budu informovat bezpečnostního ředitele CENDIS, s.p.;
11. v případě opuštění pracovní stanice (počítač, notebook, tablet, mobil) nebo jiného zařízení pro zpracování informací, zajistím toto zařízení proti neoprávněnému zneužití uzamčením obrazovky nebo zajistím odhlášení tohoto zařízení od prostředků CENDIS, s.p. tak, aby nemohlo dojít k jeho zneužití;
12. pro připojení k síti CENDIS, s.p. budu používat jen správně nastavené a dostatečně zabezpečené zařízení (šifrovaná partition, vynucené přihlašování k PC), včetně funkční a aktuální ochrany proti škodlivému software, a to i v těch případech, kdy takové zařízení není majetkem CENDIS, s.p. Zároveň na vyžádání tato zařízení zpřístupním ke kontrole, která ověří požadovaná nastavení;
13. vzdálené připojení VPN budu používat jen k pracovním účelům, pro přístup k aplikacím a/nebo technickým prostředkům vyplývajících z výše uvedené smlouvy;
14. neposkytnu přístup ke vzdálenému připojení žádné externí straně ani jinému uživateli v rámci stejného subjektu;

15. v rámci prvního přístupu k informačním aktivům CENDIS, s.p. jsem povinen se seznámit s řídicí, bezpečnostní a provozní dokumentací CENDIS, s.p. přístupné z vnitřní sítě v DMS CENDIS (https://dms.cendis.lan), v případě nemožnosti přístupu k DMS CENDIS dodá dokumentaci k seznámení ředitel úseku žadatele;
16. budu dodržovat pravidla a zásady, definované ve výše uvedené řídicí, bezpečnostní a provozní dokumentaci;
17. informace, které mi budou poskytnuty, nebo je jinak získám v souvislosti s plněním činností vyplývajících z pracovní smlouvy, budu uchovávat v tajnosti a učiním veškerá možná opatření zabraňující jejich zneužití či prozrazení;
18. nebudu manipulovat s HW s výjimkou toho, který je svěřen do mé servisní péče nebo jehož přemístěním jsem pověřen;
19. jsem si vědom, že jakékoliv porušení výše uvedených pravidel bude postihováno v souladu se zákony a souvisejícími právními předpisy České republiky;
20. v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů jsem držitelem platného osvědčení fyzické osoby stupně

Vyhrazené	☐	platné od: _____
Důvěrné	☐	platné do: _____
Tajné	☐	platné do: _____
Přísně tajné	☐	platné do: _____

21. jsem nebyl/a pravomocně odsouzen/a za trestný čin a v současné době není proti mně vedeno trestní řízení. Jsem si plně vědom/a možných právních důsledků, které by pro mě vyplývaly v případě nepravdivých údajů uvedených v tomto čestném prohlášení. Beru na vědomí, že pokud by došlo k jakékoliv změně skutečností uvedených v tomto čestném prohlášení, jsem povinen/na neprodleně toto oznámit bezpečnostnímu řediteli CENDIS, s.p.

V dne:

jméno a příjmení žadatele

vlastnoruční nebo elektronický podpis žadatele