Smlouva o správě výpočetní techniky, počítačového vybavení a počítačové sítě

Dodavatel:
Přemysl Fadrný, Pod vlekem 158, 564 01 Dlouhoňovice,
IČO: 72924012, DIČ: [redacted](dále jen dodavatel)
Provozovna: Orlická kasárna 740, 56401 Žamberk

a

odběratel:
Název: Správa budov Žamberk s.r.o.
Sídlo: Klostermanova 990
IČO: 25280091, DIČ: CZ25280091 (dále jen odběratel)

I. Předmět smlouvy

Předmětem smlouvy je zajištění provozu počítačové sítě, počítačů a počítačového příslušenství, rozsahu uvedeném v příloze smlouvy (dále rozsah).

II. Práva a povinnosti smluvních stran

Dodavatel se zavazuje vykonávat pro odběratele správu počítačové sítě, počítačů a počítačového příslušenství, která zahrnuje udržování provozu počítačové sítě, provádění údržby, oprav a dodávek výpočetní techniky, počítačového příslušenství a počítačové sítě (dále IT infrastruktura).

Dodavatel vykonává správu IT infrastruktury dle svých odborných schopností a znalostí.

Dodavatel se zavazuje navrhnout dodavateli legální získání vhodného software. Pokud odběratel používá na počítačích nelegálně získaný software, dodavatel za toto nenese odpovědnost.

Dodavatel provádí správu IT infrastruktury v místě pracoviště objednatele osobní návštěvou pracovníka, nebo pomocí dálkového přístupu prostřednictvím aplikace TeamViewer, Vzdálené plochy Windows a WinBox.

Dodavatel se zavazuje, okamžitě reagovat na nahlášenou závadu IT infrastruktury. Pokusit se uvedenou závadu alespoň dočasně či provizorně odstranit v nejkratší možné době.

Dodavatel neodpovídá za škodu, která byla způsobena jinou osobou než dodavatelem, či jím pověřeným subjektem, nesprávným nebo neadekvátním přístupem odběratele a v důsledku událostí vyšší moci.

Dodavatel odpovídá odběrateli za škodu způsobenou odběrateli zaviněným porušením povinností stanovených touto smlouvou, maximálně však do výše hodnoty plnění jednoho poplatku za kontrolu dle bodu VI.

Odběratel se dále zavazuje, že veškeré opravy, správu a předpokládaný zásah IT infrastruktury svěří pouze dodavateli a bude s ním předem konzultovat. Dodavatel není povinen připojit do počítačové sítě odběratele, dodavatelem neschválené IT prvky.

Odběratel se zavazuje seznámit své pracovníky se Směrnicí bezpečného chování s ICT.

Odběratel je povinen zajistit, v době přítomnosti dodavatele, přítomnost pověřeného pracovníka, případně jiným způsobem zajistit přístup k výpočetní technice.

III. Udržování provozu počítačové sítě – vzdálený dohled

K udržení provozu počítačové sítě, používá dodavatel nástroje pro vzdálený přístup a vzdálený dohled na IT infrastrukturu. Nástroje pro vzdálený přístup jsou TeamViewer, Vzdálená plocha a Winbox. Slouží dodavateli ke vzdálené pomoci pracovníkům odběratele, v pracovní době ve všední dny od 7.30 do 16 hodin.

Nástroje pro monitoring síťového provozu a funkčnosti sítě jsou EasyNet a protokol SNMP. Dodavatel vyhodnocuje nestandardní pohyb v datovém toku a případně provádí korekce. Dodavatel shromažďuje data o síťovém provozu na vyhrazeném serveru, a to po dobu nejdéle 3 měsíce. Slouží pro zpětnou analýzu nestandardních situací v provozu IT infrastruktury.

IV. Pravidelné kontroly IT infrastruktury – tzv. „Revize“

Pravidelné kontroly slouží ke konzultaci dotazů pracovníků odběratele s technikem dodavatele a kontrole technického stavu IT infrastruktury odběratele. Předmětem pravidelné kontroly jsou zařízení uvedené v příloze ROZSAH a označená ve sloupci „Předmět revize“ hodnotou ANO. Četnost kontrol je stanovena na jednu kontrolu prováděnou každý měsíc.
Pracovník dodavatele při pravidelné kontrole vykonává tyty práce:

- Správa software určenému k ochraně počítačů a notebooků proti počítačovým virům.
- Správa software určeného k odstraňování Spyware a Malware.
- Správa zálohovacího software Acronis.
- Správa aktualizací MS Windows, MS Office.
- Kontrola hardware (diagnostika pevných disků, celkový stav IT infrastruktury).
- Konzultace ohledně zlepšení, vývoje, zabezpečení IT infrastruktury odběratele.
- Informovanost pracovníkům objednatele ohledně obsluhy software a aktuálních bezpečnostních rizik.

Množství práce vyčleněné na každý 1 prvek IT infrastruktury:

- Počítač, notebook, nebo server 30 minut práce.
- Router (Mikrotik) 20 minut práce.
- Terminál vzdálené plochy 10 minut práce.
- Záložní disk NAS 10 minut práce.
- Aktivní prvek sítě (wifi vysílač, switch) 5 minut práce.
- Na vzdálený dohled na chybové zprávy zálohování je vyčleněno 5 minut práce.

Na základě přílohy ROZSAH, v součtu celkem 6,5h.

Dodavatel na základě kontroly vygeneruje a pošle odběrateli prostřednictvím e-mailu „Revizní zprávu“ za danou kontrolu.

V. Kontrola záloh:

Kontrola záloh zařízení, uvedených v příloze ROZSAH a označená ve sloupci „Kontrola záloh“ hodnotou ANO. Pracovník dodavatele při „revizi“ testuje obnovu náhodně vybraného souboru z poslední provedené zálohy, vyhodnocuje stáří zálohy, jestli odpovídá nastavenému plánu zálohování a obnovitelnost souboru.

V nepravidelných intervalech pracovník dodavatele testuje také kompletní obnovitelnost náhodně vybraného zařízení (server, PC, notebook) ze záložní kazety RDX, nebo jednotky NAS, tato operace není součástí pravidelných „revizí“.

Dodavatel dohlíží na chybové zprávy, které v případě neúspěšné zálohy odesílají tato zařízení na email dodavatele. Dodavatel operativně tyto závady odstraňuje, provádí korekce Plánu zálohování.

VI. Cena plnění a platební podmínky

Smluvní strany se dohodly, že cena plnění je stanovena následně:

- Poplatek za jednu kontrolu IT infrastruktury je stanovený součtem v bodu IV, účtovaný sazbou 1353,- Kč a **sníženou o 15 % na 1150,- Kč za hodinu, celkem ve výši 7.500, - Kč bez DPH.**
- Každá další odpracovaná hodina pracovníka je účtována sazbou 1150,- Kč bez DPH.
- Dodavatel provádí fakturaci následně po provedené kontrole a fakturu se splatností deset dní zasílá elektronicky na e-mailovou adresu: [redacted]

Odběratel se zavazuje, že dodrží splatnost obdržených faktur od dodavatele.

VII. Závěrečná ustanovení

- Smlouva se uzavírá na dobu neurčitou. Platnost a účinnost této smlouvy je dána dnem podpisu smluvních stran.
- Smlouva může být ukončena vzájemnou dohodou smluvních stran, nebo odstoupením od smlouvy v případě závažného porušení povinností stanovených touto smlouvou, nebo z důvodů stanovených zákonem. Odstoupení od smlouvy nabývá účinnosti dnem doručení písemného oznámení o odstoupení druhé smluvní straně.
- Tato smlouva ruší veškeré předchozí dohody a ujednání smluvních stran týkajících se předmětu této smlouvy.
- Změny a doplňky této smlouvy mohou být prováděny pouze písemnou formou.
- Smluvní strany se zavazují řešit případné spory vzájemnou dohodou.
- Tato smlouva je vyhotovena ve dvou výtiscích, každá strana obdrží jeden výtisk.
- Smluvní strany vzájemně prohlašují, že tato smlouva nebyla uzavřena v tísni, ani jinak za jednostranně nevýhodných podmínek či na nátlak kterékoliv strany, popř. třetích osob, což stvrzují svým podpisem.
- Smluvní strany prohlašují, že si tuto smlouvu před podpisem přečetly, že s jejím obsahem souhlasí.

Dne: ……

[redacted]

…… ……

Podpis a razítko dodavatele Podpis a razítko odběratele

ROZSAH

Příloha smlouvy o správě výpočetní techniky, počítačového vybavení a počítačové sítě

Stav k 1. 1. 2022

Dodavatel:
Přemysl Fadrný, Pod vlekem 158, 564 01 Dlouhoňovice,
IČO: 72924012, DIČ: [redacted] dále jen dodavatel)
Provozovna: Orlická kasárna 740, 56401 Žamberk
a
odběratel:
Název: Správa budov Žamberk s.r.o.
Sídlo: Klostermanova 990
IČO: 25280091, DIČ: CZ25280091
(dále jen odběratel)

Skupina	IP ADRESA	Název	Lokalizace	Předmět revize	Kontrola záloh
MODEM	[redacted]	[redacted]	[redacted]	NE	NE
ROUTER				ANO	NE
PC				ANO	ANO
				ANO	ANO
				ANO	ANO
				ANO	ANO
				ANO	ANO
				ANO	NE
Tiskárny				NE	NE
				NE	NE
				NE	NE
				NE	NE
ENERGETIKA				NE	NE
DHCP 100-130				ANO	ANO
				ANO	ANO
				ANO	ANO
Wifi		K Z)		ANO	NE
				ANO	NE
				ANO	NE
SWITCHE				ANO	NE
				ANO	NE
SERVER				ANO	ANO
NAS				ANO	NE
VLAN18: ETH3 - VOIP - TELEFONY				NE	NE
				NE	NE
				NE	NE
				NE	NE
				NE	NE
				NE	NE
ROUTER			Kote í	ANO	NE

Červeně označené položky podléhají revizní kontrole.

Dne: ……

[redacted]

……
Podpis a razítko dodavatele

……
Podpis a razítko odběratele

PLÁN ZÁLOHOVÁNÍ

Příloha smlouvy o správě výpočetní techniky, počítačového vybavení a počítačové sítě

Stav k 1. 1. 2022

Dodavatel:
Přemysl Fadrný, Pod vlekem 158, 564 01 Dlouhoňovice,
IČO: 72924012, DIČ: [redacted] (dále jen dodavatel)
Provozovna: Orlická kasárna 740, 56401 Žamberk
a
odběratel:
Název: Správa budov Žamberk s.r.o.
Sídlo: Klostermanova 990
IČO: 25280091, DIČ: CZ25280091 (dále jen odběratel)

PLÁN ZÁLOHOVÁNÍ			
Název zařízení	**Místo uložení záloh**	**Plán zálohování obrazu celého disku**	**Doplňkové zálohování jednotlivých složek**
NB-UCETNI	[redacted]		
NB-JEDNATEL			
MUZIK			
PC-UCETNI			
pokladna			
charvat			
MORAVEK			
UCTO-PC			
server1			

Dne: ……

[redacted]

Podpis a razítko dodavatele

……

Podpis a razítko odběratele

Interní směrnice – BEZPEČNÉ CHOVÁNÍ PŘI PRÁCI S ICT

Číslo				Verze	
Účinnost od				Platnost do	
Zpracoval	Přemysl Fadrný	Dne	15.12.2021	Podpis	
Schválil		Dne		podpis	

Obsah dokumentu

1. Úvodní ustanovení

(1) Interní směrnice – BEZPEČNÉ CHOVÁNÍ PŘI PRÁCI S ICT je vydána v souladu se směrnicí na ochranu osobních údajů číslo [redacted]
(2) Směrnice stanovuje povinnosti uživatele ICT a základní bezpečnostní postupy při práci s ICT.
(3) Použití vlastních zařízení v ICT je zakázáno. Výjimky schvaluje bezpečnostní manažer ICT (vedoucí pracovník oddělení). Definice bezpečnostních požadavků pro použití vlastních zařízení zaměstnanců nebo externích subjektů v ICT bude řešena v metodickém pokynu „Bezpečnostní politika BYOD".
(4) Směrnice je závazná pro všechny zaměstnance firmy, externí pracovníky a externí subjekty, kterým byl povolen přístup k ICT.

2. Základní pojmy a názvosloví užívané v ICT

(1) Terminologie použitá v této příručce vychází z Bezpečnostní politiky ICT.
(2) Autentizace – je prokázání identity uživatele, zdroje nebo zařízení.
(3) Bezpečnost informací – znamená zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností jako např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.
(4) Bezpečnostní incident – je událost nebo události, které ohrožují bezpečnost informací, případně porušení bezpečnostních politik nebo navazujících řídících dokumentů.
(5) BYOD (Bring Your Own Device) – je využívání vlastních zařízení pro pracovní účely a přístup k datům a aplikacím.
(6) Dokument – je každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či elektronické (digitální), která byla vytvořena v rámci, nebo byla doručena.
(7) Dostupnost – znamená, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.
(8) Důvěrnost – znamená, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.
(9) Chráněná informace – je informace, která na základě rozhodnutí příslušné autority (vlastník informačního aktiva) musí být chráněna, protože její zpřístupnění, modifikace, zničení nebo ztráta by způsobilo někomu nebo něčemu znatelnou újmu a škodu. Viz také směrnice SM-5/2013 Ochrana informací.
(10) ICT (informační a komunikační technologie) - je veškerá technika, která se zabývá zpracováním a přenosem informací, a to je zejména výpočetní a komunikační technika a její programové vybavení.
(11) Integrita – znamená zajištění správnosti a úplnosti informací.
(12) Klasifikace informací – je definování kategorie informace z hlediska jejího významu a povahy. Podle stanovené kategorie se určuje konkrétní způsob její ochrany.
(13) Mobilní zařízení ICT – je malý přenosný elektronický přístroj s různým programovým vybavením jako např. mobilní telefon, notebook, netbook, smartbook, PDA, tablet, USB zařízení apod.
(14) Monitorování – je sledování, dozor, kritické pozorování nebo určování stavu pro identifikování odchylek od požadované nebo očekávané úrovně.
(15) Oprávněná osoba – je fyzická nebo právnická osoba, která splňuje podmínky přístupu nebo je oprávněna seznamovat se s příslušnou kategorií informace.
(16) Uživatel – každá fyzická osoba (zaměstnanec nebo smluvně pověřený zaměstnanec externí fyzické nebo právnické osoby), které byl přidělen přístup k ICT a příslušná přístupová oprávnění.

3. Povinnosti uživatele ICT

(1) Zabezpečit informace, se kterými se dostane do kontaktu při výkonu své pracovní činnosti, před případným zneužitím, poškozením, zničením nebo ztrátou.
(2) Chránit informace nelistinného charakteru v ICT v souladu s ustanoveními uvedenými ve směrnici GDPR001.
(3) Používat pouze schválené nástroje (např. certifikáty vydané certifikační autoritou) k elektronické ochraně informací.
(4) Chránit zařízení ICT před poškozením, zničením, ztrátou nebo zneužitím uzamykáním kanceláří nebo pracovních prostorů a při odchodu z pracoviště uzamknout pracovní plochu počítače (stisknutím Win+L nebo Ctrl+Alt+Delete) nebo se odhlásit ze systému.
(5) Používat bezpečná hesla podle níže uvedených zásad (pokud to systém ICT umožňuje):
a) heslo musí obsahovat nejméně velké písmeno (A-Z), čtyři malá písmena (a-z), číslici (0-9) a k zvýšení kvality hesla je doporučeno používat i speciální znaky (např.! ?, *, +, apod.),
b) heslem nebo jeho součástí nesmí být jméno uživatele nebo jeho blízkých, číslo jeho průkazu, organizační jednotky, pracoviště, pošty apod.,
c) délka hesla musí být minimálně 8 znaků (pokud to systém ICT umožňuje) a nedoporučuje se používat české znaky s diakritikou

a z důvodu záměny písmena Y a Z,
d) heslo nesmí uživatel sdílet s jiným uživatelem,
e) platnost hesla je u zařízení ICT není omezené, doporučuje se změna každých 90 dnů,
f) změněné heslo nesmí být shodné s předchozími hesly.
(6) Chránit autentizační a přístupové údaje (hesla, klíče apod.) před vyzrazením, ztrátou nebo zneužitím a v žádném případě je nikomu nesdělovat.
(7) Věnovat pozornost systémovým oznámením a hlášením bezpečnostních programů jako je například antivirová ochrana. Při zjištění nebo jen podezření na přítomnost počítačového viru vypnout zařízení ICT a neprodleně to oznámit na Správci ICT a dále se řídit jeho pokyny.
(8) Provést antivirovou kontrolu informací na všech záznamových médiích (celého záznamového média nebo jen datového souboru) při obdržení od externích subjektů. Při předávání záznamových médií externímu subjektu je uživatel povinen zabezpečit, aby na daném záznamovém médiu byly pouze informace určené pro daný externí subjekt.
(9) Nezasahovat do systémového nastavení jednotlivých zařízení ICT ani neprovádět instalaci programů.
(10) Nekopírovat SW na jiný počítač nebo jej předávat jiné osobě v rámci nebo mimo firmu.
(11) Bez souhlasu nadřízeného nepřemisťovat zařízení mimo určené prostory a dodržovat provozní řád daného pracoviště.
(12) Pracovat se zařízením ICT tak, aby chráněné informace nemohly být odposlechnuty, odpozorovány nebo vyčteny ze zpracovávaných dokumentů a obrazovek zařízení ICT jinou nepovolanou osobou.
(13) Účastnit se organizovaných školení bezpečnosti ICT.
(14) Hlásit zjištěné bezpečnostní incidenty (viz kapitola 6. této směrnice).

4. Uživateli ICT je zakázáno

(1) Přerušovat probíhající aktualizace systému, vypínat antivirovou (Eset), anti ransomwarovou (Acronis Active Protection), anti spywarovou (SpyHunter) ochranu nebo měnit konfiguraci bezpečnostních prvků ochrany ICT.
(2) Bez souhlasu vedení používat ICT pro svou osobní potřebu, instalovat jakýkoli SW, manipulovat s ICT jinak než povoleným způsobem, snažit se měnit HW komponenty či systémovou konfiguraci nebo připojovat vlastní (soukromá) zařízení. V případě dostupnosti oddělené „veřejné“ wifi sítě, uživatel po dohodě s pracovníky ICT a nadřízeným pracovníkem, může provést připojení soukromých zařízení, mobilních telefonů a tabletů na veřejnou wifi, nikoliv však na vnitropodnikovou wifi nebo síť. Totéž platí pro připojování zařízení obchodních zástupců externích firem.
(3) Pracovat s cizími autentizačními a přístupovými údaji.
(4) Zneužívat internetových služeb a emailu k jiným než služebním účelům.

5. Záznamová média

(1) Záznamová média používaná ve firmě jsou vyjímatelné HDD, USB zařízení, DVD, CD, magnetické pásky, případně další.
(2) Záznamová média musí být uživatelem před likvidací nebo opakovaným použitím kontrolována, zda neobsahují chráněné informace nebo licencované programové vybavení.
(3) Záznamová média obsahující chráněné informace musí být před opakovaným použitím jiným uživatelem bezpečně smazána.

6. Bezpečnostní incident

6.1. Základní seznam bezpečnostních incidentů:

a) projev počítačového viru nebo jiného zlomyslného SW,
b) nestandardní chování zařízení ICT,
c) kompromitace autentizačních a přístupových údajů (např. hesla) nebo podezření na ni,
d) ztráta zařízení ICT, mobilního zařízení ICT nebo záznamového média,
e) proniknutí nepovolané osoby na pracoviště uživatele, k zařízení ICT nebo i pokus o něj,
f) výstražné hlášení operačního systému nebo aplikačního SW,
g) neoprávněná změna HW, SW nebo konfigurace,
h) neúmyslné nebo úmyslné vyzrazení chráněných informací.
i) uživatel je postaven do situace, se kterou si neví rady, nebo ji není schopen v rámci svých znalostí správně vyhodnotit a následně vyřešit.

6.2. Řešení bezpečnostního incidentu

(1) Při podezření na projev počítačového viru (změny ikon, nestandardní chování programů), zařízení okamžitě vypnout, odpojit od přívodu elektrického proudu a datové sítě. Kontaktovat správce ICT a vedoucího pracovníka.
(2) Každý bezpečnostní incident musí uživatel neprodleně oznámit správci ICT a svému nadřízenému.
(3) Uživatel je povinen poskytnout správci ICT nezbytnou součinnost, mimo jiné umožnit připojení technika ICT k zařízení prostřednictvím aplikace TeamViewer. Správce ICT provede potřebná opatření podle vyhodnocení bezpečnostního incidentu pro uvedení ICT do bezpečného stavu.
(4) V případě nedostupnosti správce ICT a vedoucího pracovníka musí uživatel vyčkat s řešením problému až do dostupnosti alespoň jednoho z jmenovaných a po konzultaci teprve provést další kroky k úspěšnému vyřešení situace.

7. Havarijní situace

7.1. Základní typy havarijních situací:

(1) Oblast fyzické bezpečnosti
a) oheň, kouř nebo výbuch,
b) záplavy nebo prosakování kapalin,
c) narušení konstrukce budovy,
d) přírodní katastrofa.
(2) Oblast bezpečnosti ICT
a) porucha HW,
b) chyby SW,
c) výpadek elektrického proudu.

7.2. Postup uživatele při vzniku havarijních situací

(1) Uživatelé jsou povinni postupovat podle směrnice Zajištění bezpečnosti a ochrany zdraví při práci a směrnici Zajištění požární ochrany.
(2) Uživatel je pak povinen v případě, že je schopen situaci zvládnout, provést nezbytná opatření k minimalizaci dopadů pro ICT a chráněné informace v něm zpracovávané.
(3) Po provedení nezbytných opatření je uživatel povinen oznámit nadřízenému vznik mimořádné situace a opatření, která provedl.

7.2.1. Požár

(1) Vyhlásit požární poplach a řídit se příslušnou požární poplachovou směrnicí pracoviště.
(2) V rámci možností a stavu situace zabezpečit záznamová média, servery, počítače s chráněnými informacemi proti zničení nebo ztrátě.

7.2.2. Havárie ústředního topení, vodovodního řádu, kanalizačního řádu či jiná

obdobná havárie jako v bodě 7.2.1
Informovat o havárii nadřízeného a zodpovědnou osobu správy objektu a postupovat stejně jako v bodě 7.2.1

7.2.3. Havárie zařízení ICT

(1) Neodstraňovat závady zařízení ICT vlastními prostředky.
(2) Informovat nadřízeného a závadu nahlásit správci ICT.

8. Sankce

Porušení ustanovení bezpečnostních politik a navazujících metodických pokynů a příruček na základě posouzení závažnosti, míry zavinění, případně míry dopadu, a následků tohoto porušení (bezpečnostního incidentu) může být považováno za porušení povinností vyplývajících z interních dokumentů se všemi pracovněprávními důsledky v podobě upozornění na porušení povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci, ústního napomenutí nebo skončení pracovního poměru.

9. Související dokumenty

a) Směrnice na ochranu osobních údajů číslo GDPR001
b) Zajištění bezpečnosti a ochrany zdraví při práci

c) Zajištění požární ochrany

10. Závěrečné ustanovení

Výklad a aktualizaci této příručky zajišťuje pověřený pracovník organizace.