OBJEDNÁVKA č. 0948/2020/KŘ/O

Odběratel

IČ: 70890692 DIČ: CZ70890692

Moravskoslezský kraj

28. října 2771/117

70218 Ostrava

Vyřizuje: [redacted]

Telefon:

Odbor:

Dodavatel

IČ: 29462177 DIČ: CZ29462177

Scenario s.r.o.

Pohraniční 1435/86

70300 Ostrava

Vyřizuje:

Telefon:

Objednáváme u Vás:

Předmětem objednávky je vytvoření vzdělávacího e-learningového kurz na téma Kybernetická bezpečnost – kybernetické povědomí.

Datum požadovaného splnění: 27.11.2020

Přílohy: příloha č. 1 - vymezení rozsahu kurzu
příloha č. 2 - zásady

UPOZORNĚNÍ: Úhrada faktury se provádí 14. kalendářní den od data doručení faktury.

Povinnost zaplatit cenu je splněna dnem odepsání příslušné částky z účtu objednatele.
Dodavatel prohlašuje, že není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (člen vlády nebo vedoucí jiného ústředního správního úřadu, v jehož čele není člen vlády), nebo jím ovládaná osoba vlastní podíl představující alespoň 25% účast společníka v obchodní společnosti. Dodavatel bere na vědomí, že pokud je uvedené prohlášení nepravdivé, bude smlouva považována za neplatnou.

MAX. CENA CELKEM	**80 949,00 Kč**

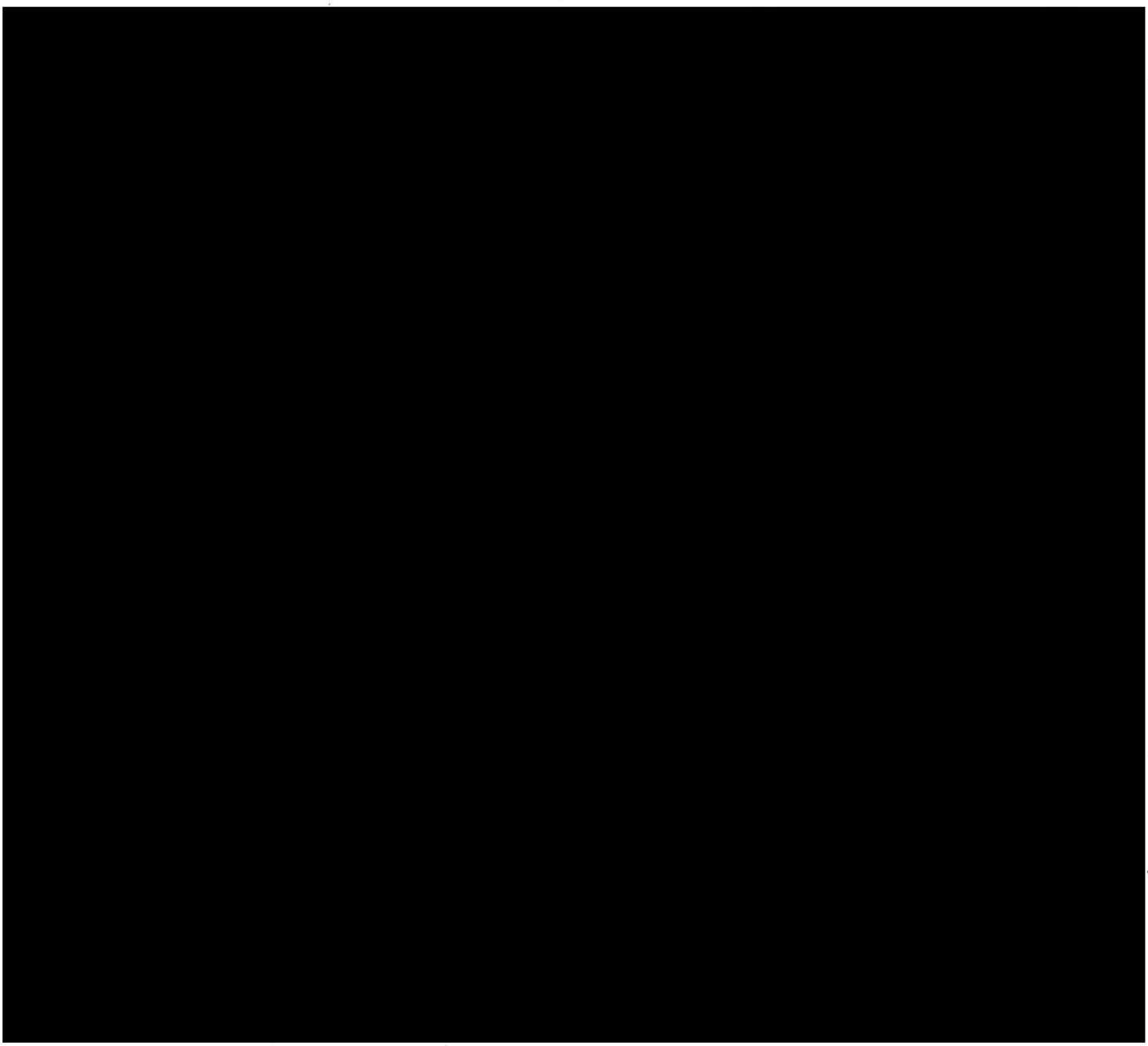
Podrobnosti platby:

Na účet

Číslo výdajového účtu MSK : 27-1650676349/0800

Datum: 25. 09. 2020

[redacted]



[redacted]

Předmět: FW: Obj. 0948/2020/KŘ/O

[redacted]
Sent: Tuesday, September 29, 2020 12:54 PM
[redacted]
Cc: textoris <textoris@scenario.cz>
Subject: Re: Obj. 0948/2020/KŘ/O

Dobrý den, [redacted]

v příloze naleznete ze strany Scenario s.r.o. potvrzenou/el. podepsanou objednávku dle Vašeho požadavku.
V případě dotazů mě prosím neváhejte kontaktovat.

S pozdravem

[redacted] Scenario s.r.o.

OBJEDNÁVKA č. 0948/2020/KŘ/O

Odběratel

IČ: 70890692 DIČ: CZ70890692

Moravskoslezský kraj

28. října 2771/117

70218 Ostrava

Vyřizuje: [redacted]

Telefon:

Odbor:

Dodavatel

IČ: 29462177 DIČ: CZ29462177

Scenario s.r.o.

Pohraniční 1435/86

70300 Ostrava

Vyřizuje:

Telefon:

Objednáváme u Vás:

Předmětem objednávky je vytvoření vzdělávacího e-learningového kurzu na téma Kybernetická bezpečnost – kybernetické povědomí.

Datum požadovaného splnění: 27.11.2020

Přílohy: příloha č. 1 - vymezení rozsahu kurzu
příloha č. 2 – zásady

UPOZORNĚNÍ: Úhrada faktury se provádí 14. kalendářní den od data doručení faktury.

Povinnost zaplatit cenu je splněna dnem odepsání příslušné částky z účtu objednatele.
Dodavatel prohlašuje, že není obchodní společností, ve které veřejný funkcionář uvedený v § 2 odst. 1 písm. c) zákona č. 159/2006 Sb., o střetu zájmů, ve znění pozdějších předpisů (člen vlády nebo vedoucí jiného ústředního správního úřadu, v jehož čele není člen vlády), nebo jím ovládaná osoba vlastní podíl představující alespoň 25% účast společníka v obchodní společnosti. Dodavatel bere na vědomí, že pokud je uvedené prohlášení nepravdivé, bude smlouva považována za neplatnou.

MAX. CENA CELKEM	**80 949,00 Kč**

Podrobnosti platby:

Na účet

Číslo výdajového účtu MSK : 27-1650676349/0800

Datum: [redacted]

[redacted]

Digitálně podepsal [redacted]

Datum: 2020.09.29 12:39:37 +02'00'

Vymezení rozsahu kurzů

Bezpečnostní kurz se skládá z několika částí.

1. Základy bezpečnosti

1.1. Základy bezpečnosti pro uživatele na KÚ MSK

a) Co je bezpečnost informací.

- *Cíle bezpečnosti.*
- *Jaké jsou hrozby, jak vypadají typické útoky.*
- *Základní pravidla bezpečnosti pro uživatele informací.*
- *Kde co najdu (bezpečnostní dokumentaci).*

b) Odpovědnost za bezpečnost.

- *Ochrana osobních údajů a autorského práva.*
- *Co mám kontrolovat a kdo mne může kontrolovat.*
- *Klasifikace, ukládání, odesílání a likvidace informací.*
- *Co je bezpečnostní incident. Kde případný incident hlásit.*

1.2. Řízení přístupu a ochrana hesel

Řízení přístupu k prostředkům IT.

- *K čemu se heslo používá.*
- *Jak má vypadat bezpečné heslo.*
- *Jak heslo chránit.*
- *Co dělat v případě jeho vyzrazení nebo podezření.*

2. Fyzická bezpečnost

2.1 fyzické zabezpečení

Jak jsou zabezpečeny prostory.

- *Režim pro návštěvy.*
- *Způsob výkonu práce v zabezpečených oblastech.*

Princip čistého stolu a prázdné obrazovky.

- *Uklízení pracovních pomůcek do uzamykatelných kontejnerů.*

2.2. Bezpečnost zařízení USB

- *Pravidla pro využívání pracovních USB zařízení, SD karet apod.*
- *Zákaz užívání soukromých zařízení.*
- *Šifrování dat na vyměnitelných zařízeních.*

2.3. Ochrana a likvidace dat

- *Postupy a předpisy pro ukládání dat (fileserver, lokální úložiště).*
- *Šifrování pevných disků koncových zařízení.*
- *Hlášení ztráty zařízení a dat.*
- *Proces opravy a likvidace nosičů a zařízení.*

3. Kybernetické útoky a sociální inženýrství

3.1. Kybernetické útoky

- *Kybernetické útoky – kdo za nimi stojí a důvody úspěchu.*
- *Fáze kybernetického útoku.*

3.2. Sociální inženýrství

- *Definice sociálního inženýrství*
- *Metody sociálního inženýrství – jak a čím.*
- *Možné příklady útoku.*
- *Shrnutí – Taktiky útoku a obrana.*

4. Práce na dálku

4.1. Zajištění bezpečnosti mimo pracoviště

Pravidla práce na dálku.

- *Možnost připojení do organizace.*
- *Princip vzdáleného přístupu.*
- *Zákaz využívání pracovních pomůcek k soukromým účelům.*

4.2. Bezpečnost na služebních cestách

- *Specifické hrozby na pracovních cestách.*
- *Pravidla pro přepravu a uložení prostředků IT.*
- *Lokální předpisy, nařízení a embarga pro exotické destinace.*

4.3. Bezpečnost mobilních zařízení

- *Pravidla užívání mobilních zařízení.*
- *Způsob zabezpečení mobilních zařízení.*
- *Zákaz použití vlastních zařízení. Princip správy mobilních zařízení.*
- *Možnost vymazání obsahu mobilních zařízení.*

5. Elektronická pošta

5.1. Rozeznání podvodných emailů

- *Jak vypadá typický podvodný email.*
- *Jak můžeme podvodný email poznat.*
- *Co je Spoofing.*

Elektronický podpis v emailové komunikaci.

- *Šifrování emailů.*

5.2. Jak se vyhnout nebezpečným přílohám a odkazům

- *Jak vypadá typická nebezpečná příloha.*
- *Oblíbené typy zneužívaných souborů.*
- *Typické falešné URL v emailu. Tipy na obranu.*

5.3. Ransomware

- *Co je ransomware.*
- *Jak ho poznat.*
- *Co dělat při podezření na ransomware.*

6. Web

6.1 Bezpečnost procházení webu

- *Firemní pravidla pro procházení webu.*
- *Možnost využívání webového prohlížeče pro soukromé účely.*
- *Jaké jsou hrozby.*
- *Příklady útoků.*

6.2 Formuláře a zadávání údajů

- *Jak být opatrný co a kam zadávám. Které údaje jsou zneužitelné.*
- *Pravidla pro ochranu osobních údajů.*

6.3 Rozeznání podvodných URL

- *Co je URL.*
- *Jak funguje zabezpečený webový protokol HTTPS.*
- *Co jsou certifikáty a jak je zkontrolovat.*
- *Důvěryhodné autority.*

6.4 Bezpečné sociální sítě

- *Pravidla pro využívání sociálních sítí pro pracovní účely.*
- *Co může/nesmí uživatel sdílet na sociál. sítích (fotky z práce, informace o produktech*

Vymezení rozsahu kurzu.docx

Příloha č.2

Základní zásady a pravidla chování v oblasti kybernetické a informační bezpečnosti pro dodavatele

Tato příloha stanovuje základní zásady, pravidla a normy chování v oblasti kybernetické a informační bezpečnosti pro dodavatele zařízení, systémů a služeb z oblasti informačních a komunikačních technologií pro KÚ MSK (externí organizace).

1. Ochrana informací Krajského úřadu

1.1 Přístup dodavatelů k neveřejným informacím nebo do chráněných oblastí Krajského úřadu není před uzavřením smlouvy (objednávky) dodavatelům povolen.

1.2 Dodavatel je povinen ochránit informace krajského úřadu poskytované v rámci plnění smluvního vztahu.

1.3 Dodavatel je povinen vrátit či zničit neveřejné informace na požádání KÚ během doby trvání smluvního vztahu, respektive vždy při jeho ukončení.

1.4 Dodavatel nesmí kopírovat a sdělovat informace krajského úřadu poskytované v rámci plnění smluvního vztahu dodavatelem dalším subjektům.

1.5 U informací klasifikace chráněné, pokud se informace přenášejí prostřednictvím mobilních zařízení nebo zařízení s výměnnými médii nebo přes komunikační linky, musí být vždy použito šifrování.

1.6 Při přenášení dat veřejnými nebo bezdrátovými sítěmi se z důvodu zabezpečení jejich důvěrnosti a integrity a také ochrany připojených systémů a aplikací používají šifrované protokoly, případně VPN.

2. Pravidla řízení přístupů uživatelů externích organizací (dodavatelů)

1.1 Uživatelé externích organizací (dále jen uživatelé) jsou odpovědni za ochranu svých autentizačních informací.

1.2 Pro každého uživatele musí existovat jedinečný přístupový účet.

1.3 Každý uživatel zodpovídá za svůj účet.

1.4 Účet nesmí být sdílen více osobami.

1.5 Každý uživatel zodpovídá za své heslo.

1.6 Heslo uživatele nesmí být sdíleno více osobami.

1.7 Uživatel nesmí heslo sdělovat jiným osobám, zapisovat je na lehce viditelné, nebo přístupné místo (zápisník, okraj monitoru, kalendář apod.).

1.8 Heslo administrátora (uživatele s privilegovanými oprávněními) musí obsahovat minimálně 17 znaků.

1.9 Heslo administrátora (uživatele s privilegovanými oprávněními) musí obsahovat kombinace znaků ze všech zde uvedených kategorií:

- Velká písmena:

  A, B, C, D, E, F, G, H I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z
- Malá písmena:

  a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y, z
- Číslice:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9

- Symboly na klávesnici:

  ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /

1.10 Heslo administrátora (uživatele s privilegovanými oprávněními) nesmí obsahovat uživatelské jméno, skutečné jméno, jméno společnosti nebo jiné úplné slovo a musí být výrazně odlišné od předchozích hesel.

1.11 Heslo administrátora (uživatele s privilegovanými oprávněními) má platnost max. 12 měsíců.

3. Pravidla pro řízení vzdálených přístupů

1.12 Vzdálený přístup do sítě KÚ pro dodavatele/externího uživatele je možné zřídit pouze na základě schválené žádosti, žádost schvalují pověření pracovníci odboru informatiky KÚ.

1.13 Veškerá komunikace prostřednictvím vzdáleného přístupu do sítě KÚ musí být šifrována a uživatel externího spojení musí být autentizován.

1.14 Pro přístup externího uživatele je použita jedinečná identifikace uživatele tak, aby byly identifikovatelné jeho aktivity a zodpovědnost za ně.

1.15 Uživatelům vzdálených přístupů do sítě KÚ, u nichž se změnila jejich role nebo skončil důvod vzdáleného přístupu (vyplývající ze smlouvy), jsou vzdálené přístupy blokovány nebo odejmuty.

1.16 Přístupy do sítě KÚ jsou přiděleny pouze na systémy potřebné k provedení specifikovaných činností (dle smlouvy s dodavatelem).

1.17 Přístupy do sítě KÚ jsou přiděleny na dobu, která je uvedená v žádosti o zřízení vzdáleného přístupu.

1.18 Vzdálené přístupy do sítě KÚ jsou realizovány přes terminál server.

1.19 Heslo přidělené uživateli pro vzdálený přístup je předáno uživateli a není správcem sítě nikde uloženo;

1.20 Uživatel si po prvním přihlášení nastaví nové heslo.

1.21 Hesla nesmějí být nikdy ukládána v počítači v nezabezpečené (volně čitelné) podobě a nesmějí být na pracovišti uživatele snadno dostupná.

1.22 Veškerá činnost dodavatelů využívající vzdálený přístup do sítě KÚ je monitorována.

1.23 Přístup externího uživatele, který je součástí projektového nebo pracovního týmu, k internímu cloudovému úložišti Moravskoslezského kraje je možný na základě žádosti o povolení přístupu ke cloudovému úložišti který uplatňuje vedoucí oddělení nebo vedoucí odboru prostřednictvím aplikace Service Desk.

4. Pravidla fyzické bezpečnosti

4.1 Technologické místnosti (Serverovny) jsou jako prostory se zvláštním režimem.

4.2 Do serverovny mají přístup pouze oprávněné osoby definované vedoucím odboru informatiky, ostatním je umožněn přístup do serverovny jen v doprovodu oprávněné osoby.

4.3 Pracovníci externích servisních organizací, kteří provádějí servis v serverovnách, musí být poučeni o zásadách bezpečnosti v objektech KÚ.

5. Pravidla pro omezení instalace programového vybavení

1.24 Provozní systémy mohou obsahovat pouze schválený spustitelný kód, a nikoliv vývojový kód nebo kompilátory.

1.25 Všechny změny v instalacích musí být zaznamenány do konfigurační databáze provozované odborem informatiky KÚ (ve spolupráci s pracovníky odboru informatiky KÚ).

1.26 Dříve než jsou implementovány změny, musí být známa strategie návratu do předchozího stavu.

1.27 Předchozí verze aplikačního softwaru jsou, v případech, kdy je to možné, zachovány jako náhradní opatření.

6. Pravidla řízení změn

1.28 Významná změna je takový typ změny, který podstatným způsobem ovlivňuje konfiguraci významného (VIS) nebo klíčového (KLIS) informačního systému, zásadně mění vazby na ostatní systémy, zásadně mění výstupy procesů nebo nutnost změny je dána změnou legislativy, smluvních nebo regulatorních požadavků nebo změnu vyvolá bezpečnostní incident a jeho řešení anebo bylo identifikováno neakceptovatelné riziko, které se musí řídit. Významnou změnou je také změna, která má nebo může mít vliv na kybernetickou bezpečnost.

1.29 Nasazení významných změn je plánováno a tyto změny jsou, je-li to možné, před nasazením do produkčního prostředí otestovány. Výsledek testu je schválen správci všech systémů, jichž se nasazení této změny týká.

1.30 Před nasazením každé významné změny do produkčního prostředí jsou vypracovány nouzové postupy pro přerušení změn a obnovení po neúspěšných změnách a nepředvídaných událostech.

1.31 V rámci plánování významné změny musí být posouzeny možné dopady těchto změn, včetně dopadů na bezpečnost informací na všech dotčených IS.

1.32 Každá změna aktiva musí být schválena (vedoucím oddělení, které aktivum spravuje).

1.33 Před realizaci významné změny jsou s touto změnou seznámeni všichni dotčení pracovníci.

1.34 O změně aktiva musí být zpracován a uchován záznam, který obsahuje všechny důležité informace.

7. Zaznamenávání událostí informačního a komunikačního systému a činností administrátorů

1.1 Záznamy (logy) systémů jsou zaznamenávány v jednotlivých systémech a v systému SIEM.

1.2 Záznamy o činnostech administrátorů se evidují do provozního deníku.

1.3 Činnosti externích firem, které mohou ovlivnit bezpečnost dat nebo jsou pro bezpečnost dat relevantní jsou monitorovány.

8. Odpovědnost za újmu

1.1 Obě smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.

1.2 Žádná ze smluvních stran neodpovídá za újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé smluvní strany.

1.3 Smluvní strany se dohodly, že celková výše náhrady újmy, kterou může smluvní strana požadovat po druhé smluvní straně v souvislosti s porušením této těchto obchodních podmínek, se omezuje do výše celkové ceny za poskytování Služeb bez DPH dle čl. 3.1 těchto obchodních podmínek. Ujednání dle předchozí věty se nevztahuje na újmu způsobenou člověku na jeho přirozených právech, anebo způsobenou úmyslně nebo z hrubé nedbalosti.

9. Ochrana informací

1.1 Žádná ze smluvních stran nesmí zpřístupnit třetí osobě důvěrné informace, které při plnění této objednávky získala od druhé smluvní strany v souvislosti s poskytováním Služeb. To neplatí, mají-li být za účelem poskytování Služeb potřebné informace zpřístupněny zaměstnancům smluvních stran, jejich orgánům nebo jejich členům nebo subdodavatelům smluvních stran.

1.2 Za důvěrné informace jsou dle těchto obchodních podmínek považovány veškeré informace poskytnuté vzájemně, zejména informace, které se strany dozvěděly v souvislosti s touto objednávkou, jakož i know-

how, jímž se rozumí veškeré poznatky obchodní, výrobní, technické či ekonomické povahy související s činností smluvní strany, které mají skutečnou nebo alespoň potenciální hodnotu a které nejsou v příslušných obchodních kruzích běžně dostupné a mají být utajeny, a to za předpokladu, že jsou předmětné informace označeny jako důvěrné informace. Za důvěrné informace se výslovně považují rovněž veškerá uživatelská data, údaje či informace, obsažené v informačních systémech, jichž se plnění této objednávky dotýká.

1.3 Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace:

- které se staly veřejně známými, aniž by to zavinila záměrně či nedbalostně přijímající strana,
- které měla přijímající strana legálně k dispozici před uzavřením této objednávky, pokud takové informace nebyly předmětem jiné, dříve mezi stranami uzavřené smlouvy o ochraně informací,
- které jsou výsledkem postupu, při kterém k nim přijímající strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany,
- které poskytne přijímající straně třetí osoba, jež takové informace přitom nezíská přímo ani nepřímo od strany, jež je jejich vlastníkem.

1.4 Za porušení povinnosti chránit důvěrné informace se nepovažuje zpřístupnění důvěrných informací třetí osobě:

- jsou-li poskytovány ekonomickým, daňovým a právní poradcům smluvních stran a přijímající strana nezbaví tyto osoby povinnosti mlčenlivosti,
- je-li jejich zveřejnění nezbytné k tomu, aby se smluvní strana mohla domáhat ochrany svých práv u soudu nebo rozhodčího soudu,
- je-li jejich zveřejnění důvodně vyžadováno zákonem či pravomocným rozhodnutím orgánu státní správy, obecných či rozhodčích soudů.

1.5 Obě smluvní strany se zavazují nakládat s důvěrnými informacemi, které jim byly poskytnuty druhou smluvní stranou nebo je jinak získaly v souvislosti s plněním této objednávky, jako s obchodním tajemstvím; zavazují se zejména uchovávat je v tajnosti a učinit veškerá smluvní a technická opatření zabraňující jejich zneužití či prozrazení.

1.6 Povinnost utajovat důvěrné informace zavazuje smluvní strany po dobu účinnosti této objednávky a pět let po ukončení její účinnosti.