Příloha č. 2 – Cena

Cena dle odst. 1.2 písm. a) Smlouvy **činí 462 000,- Kč / měsíčně**

Cena je uvedena bez DPH.

Příloha č. 3 – Harmonogram

1) Zaškolení pracovníků Callcentra započne nejpozději 3 dny ode dne nabytí účinnosti Smlouvy a bude probíhat v délce 15 pracovních dnů;
2) Pilotní fáze poskytování služeb Callcentra započne následující pracovní den po Zaškolení pracovníků Callcentra a bude probíhat v délce 3 měsíců;
3) Standardní provoz Callcentra započne následující pracovní den po ukončení Pilotní fáze poskytování služeb Callcentra a bude probíhat v délce 13 měsíců, anebo do vyčerpání maximální ceny dle odst. 2.3. této Smlouvy, podle toho, která ze skutečností nastane dříve.

Příloha č. 4 - Požadavky Objednatele na kybernetickou bezpečnost

1. Povinnosti Poskytovatele na základě kybernetické bezpečnosti

   1.1 Smluvní Strany jsou srozuměny s tím, že informační systémy Objednatele, tj. systémy SAP CRM, SAP FI-CA, GES, Intranet a IDM (dále jen „IS“) představují významný informační systém ve smyslu § 1 Vyhlášky o kybernetické bezpečnosti, vůči němuž Objednatel povinnou osobou ve smyslu § 3 zákona č. 181/2014 Sb. o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „ZKB“); konkrétně je Objednatel správcem tohoto významného informačního systému. Informační systémy se mohou v průběhu platnosti Smlouvy za účelem poskytnutí plnění změnit. Poskytovatel se v rámci plnění této Smlouvy zavazuje, v případě, že při plnění získá přístup anebo jinak ovlivní data IS Objednatele nad rámec plnění této Smlouvy upozornit Objednatele na takovou skutečnost do dvou (2) hodin po jejím zjištění.

   1.2 Objednatel v návaznosti na kvalitu, kvantitu a jiné aspekty přístupu či ovlivnění IS Objednatele Poskytovatelem ve smyslu výše uvedeného odstavce:

      (a) zamezí přístupu Poskytovatele k IS Objednatele, pokud takový přístup není nezbytný pro plnění této Smlouvy; nebo

      (b) přijme opatření k zajištění bezpečnosti informací ve smyslu ZKB a Vyhlášky o kybernetické bezpečnosti; součástí opatření mohou být i opatření dle bezpečnostní dokumentace, se kterými Objednatel Poskytovatele neprodleně po zjištění neoprávněného přístupu Poskytovatele k IS Objednatele seznámí. V takovém případě je Poskytovatel povinen řídit se požadavky Objednatele a poskytnout Objednateli veškerou součinnost nezbytnou pro naplnění právních povinností uložených Objednateli ZKB a Vyhláškou o kybernetické bezpečnosti.

   1.3 Nesplnění povinností dle odst. 1.2 písm. b) této Přílohy Poskytovatelem může mít za následek:

      (a) odstoupení od Smlouvy ze strany Objednatele pro její podstatné porušení Poskytovatelem v důsledku ohrožení bezpečnosti informací v IS Objednatele, k níž je Objednatel oprávněn; nebo (b) uplatňování sankcí stanovených ve Smlouvě ze strany Objednatele.

2. Povinnosti Poskytovatele ve vztahu k IS Objednatele jako významnému informačního systému

   2.1 Objednatel poskytnul Poskytovateli v rámci zadávacího řízení informace významné pro plnění této Smlouvy Poskytovatelem týkající se IS Objednatele, a z toho důvodu se na Poskytovatele uplatní ustanovení týkající se bezpečnosti dle této Přílohy.

   2.2 Poskytovatel je povinen dodržovat a plnit jednotlivé povinnosti a opatření uvedené v čl. 2 této Přílohy, případně v jejich aktualizované podobě ve smyslu odst. 2.4.

   2.3 Poskytovatel je povinen zabezpečit, aby jednotlivé povinnosti a opatření uvedené v čl. 2 této Přílohy dodržovali a plnili také poddodavatelé Objednatele, přičemž Poskytovatel odpovídá za poddodavatele dle odst. 5.10 Smlouvy.

   2.4 Smluvní strany se zavazují povinnosti a opatření uvedené v čl. 2 této Přílohy aktualizovat v návaznosti na:

(a) pravidelnou aktualizaci analýzy rizik dle odst. 2.15 této Přílohy,

(b) rozhodnutí, opatření obecné povahy, či jiný správní akt Národního úřadu pro kybernetickou a informační bezpečnost či jiného správního orgánu anebo vydání závazných podmínek pro Objednatele orgánem veřejné moci ukládající Objednateli další povinnosti ve smyslu ZKB a Vyhlášky o kybernetické bezpečnosti; a

(c) výsledky kontroly a auditu kybernetické bezpečnosti ve smyslu odst. 2.31 této Přílohy, vždy do deseti (10) pracovních dnů ode dne vzniku některé z okolností stanovených výše v tomto odst. 2.4, nejpozději však do dne stanoveného ze strany orgánu dle odst. 2.4 písm. b) této Přílohy.

2.5 Poskytovatel je povinen vyhodnocovat bezpečnostní události aplikací a nástrojů a souvisejících podpůrných aktiv, které přistupují do IS Objednatele.

2.6 Poskytovatel je povinen zaslat Objednateli hlášení kybernetického bezpečnostního incidentu a události, které se týkají jeho aplikací a nástrojů přistupujících do IS Objednatele, pokud je Poskytovatel klasifikuje jako „vysoké“ nebo „kritické“, nebo pokud by mohly mít negativní vliv na IS Objednatele nebo ohrozit chod IS Objednatele, vždy nejpozději do dvou (2) hodin po jejich zjištění. Poskytovatel zároveň sdělí Objednateli opatření, která již provedl ve vztahu k tomuto incidentu anebo události, aby Objednatel mohl splnit svou ohlašovací povinnost dle ZKB, případně zvolí jinou formu dohodnutou mezi Objednatelem a Poskytovatelem určenou ke včasnému hlášení kybernetického bezpečnostního incidentu nebo události a již učiněných opatření. Poskytovatel je povinen ohlásit jednotlivý kybernetický bezpečnostní incident nebo událost současně všemi následujícími způsoby:

(a) e-mailem na e-mailovou adresu uvedenou v odst. 15.9 Smlouvy;

(b) telefonicky na telefonní číslo uvedené v odst. 15.9 Smlouvy; a

(c) na Helpdesk Objednatele.

2.7 Poskytovatel je povinen pravidelně alespoň ke konci každého kalendářního čtvrtletí předkládat Objednateli zprávu o počtu a druhu útoků a kybernetických bezpečnostních incidentů a událostí, které zaznamenal ve spojení s plněním Smlouvy.

2.8 Poskytovatel je povinen přistupovat k IS Objednatele pouze na základě veřejných statických zdrojových IP adres (IPv4/IPv6). Poskytovatel nesmí umožnit, aby tyto veřejné statické IP adresy používala jakákoliv třetí osoba. V případě, že Poskytovatel není schopen tuto povinnost splnit, sjednají Smluvní strany alternativní řešení. Tím nejsou dotčeny další ustanovení Smlouvy (např. povinnost zachovávat důvěrnost Důvěrných informací).

2.9 Poskytovatel je povinen přistupovat k IS Objednatele pouze z IT prostředků, které jsou umístěny na území Evropské unie.

2.10 Poskytovatel je povinen zpracovávat a uchovávat veškerá data související s plněním Smlouvy pouze na IT prostředcích, které jsou umístěny na území Evropské unie.

2.11 Poskytovatel je povinen zabezpečit, aby z jeho IP adres nebyl generován provoz, který by ohrožoval:

(a) dostupnost, důvěrnost a integritu IS Objednatele; a

(b) dostupnost, důvěrnost a integritu informací, které IS Objednatele zpracovává.

2.12 Poskytovatel přijme a bude udržovat a dokumentovat systém řízení bezpečnosti spočívající v přijetí dostatečných organizačních a technických opatření pro zajištění bezpečnosti.

2.13 Poskytovatel je povinen přistupovat k IS Objednatele pouze z důvěryhodného prostředí za použití důvěryhodných prostředků. Za důvěryhodné se považují prostředí a prostředky, které jsou určené pro použití v podnikovém prostředí a jsou odpovídající pro plnění dle Smlouvy.

2.14 Poskytovatel je povinen zabezpečit, aby vývoj a implementace aplikací a nástrojů přistupujících do IS Objednatele byly v souladu s požadavky „best practise" dle metodik a standardů bezpečného vývoje software.

2.15 Poskytovatel je povinen pravidelně provádět analýzu rizik a dopadu změn na současný Systém Poskytovatele a IT prostředí Poskytovatele, a to nejméně vždy při každé významné změně funkčnosti IS Objednatele, který je předmětem plnění této Smlouvy, komponenty a aplikace včetně platformy pro provoz IS Objednatele, nebo při změně legislativních a bezpečnostních požadavků. V případě, že na základě změny IS Objednatele vyvstane nutnost provedení změny Systému Poskytovatele, Poskytovatel je povinen tuto změnu náležité otestovat před jejím nasazením do produkčního prostředí Systému Poskytovatele.

2.16 Poskytovatel je povinen provádět pravidelný bezpečnostní monitoring IT prostředí Poskytovatele, které je předmětem plnění této Smlouvy, informačního a komunikačního systému, periodické ověřování zranitelností u aplikací a nástrojů komunikujících s IS Objednatele a u souvisejících podpůrných aktiv a implementovat tzv. bezpečnostní záplaty do aplikací, operačních systému, nástrojů pro ošetření zranitelností, a to bez zbytečného prodlení v případě zjištění jakékoliv zranitelnosti. V případech, kdy to bude žádoucí a vhodné, je Poskytovatel povinen provádět i penetrační testování za spoluúčasti Objednatele.

2.17 Poskytovatel je povinen provádět pravidelné testování komponent a změn přistupujících do IS Objednatele v testovacím prostředí před nasazením do produkčního prostředí IS Objednatele. Cílem je zajištění bezpečnosti, stability a provozní spolehlivosti.

2.18 Poskytovatel je povinen provádět pravidelně aktualizace, řídit rizika a zranitelnosti pro aplikace a nástroje přistupující do IS Objednatele a u souvisejících podpůrných aktiv.

2.19 Poskytovatel je povinen pravidelně proškolovat veškeré osoby v dotčených provozních rolích a administrátory aplikací/nástrojů/podpůrných aktiv:

(a) z hlediska správné obsluhy systému Poskytovatele a fungování přístupu k IS Objednatele nezbytného pro řádné plnění Smlouvy;

(b) z hlediska aktuálních bezpečnostních rizik a hrozeb systému Poskytovatele;

(c) z hlediska bezpečného chování uživatelů v kybernetickém prostředí.

O proškolení bezpečnosti ICT a rozsahu je Poskytovatel povinen vést záznamy a tyto záznamy poskytnout na žádost Objednatele. Rozsah školení poskytne Objednatel nebo odsouhlasí rozsah školení prováděný Poskytovatelem.

2.20 Poskytovatel je povinen disponovat dostatečnou znalostí pro zajištění bezpečného provozu IS Objednatele.

2.21 Poskytovatel je povinen pro zajištění integrity a důvěrnosti IS Objednatele využívat šifrovací a hashovací algoritmy dle požadavků použitelných právních předpisů (zejména prováděcích vyhlášek ZKB) a v souladu s doporučeními Národního úřadu pro kybernetickou a informační bezpečnost https://www.govcert.cz/cs/doporuceni-v-oblasti-kryptografickych-prostredku/. Objednatel je oprávněn měnit zabezpečení API a Poskytovatel je povinen takové změny implementovat, pokud ho o tom Objednatel informuje.

2.22 Poskytovatel nesmí využívat přístup k IS Objednatele k jakýmkoli jiným aktivitám než k činnostem, které výslovně stanoví Smlouva.

2.23 Poskytovatel nesmí s výjimkou poddodavatelů umožnit přístup k IS Objednatele třetím osobám.

2.24 Poskytovatel nesmí provádět jakékoli bezpečnostní nebo funkční testování IS Objednatele.

2.25 Poskytovatel je povinen se systémy poskytujícími přístup k IS Objednatele komunikovat pouze na portech definovaných ze strany Objednatele.

2.26 Poskytovatel je povinen zasílat veškeré požadavky a zprávy na IS Objednatele pouze ve struktuře a obsahu odpovídajícím omezením a parametrům stanoveným Objednatelem.

2.27 Poskytovatel je povinen dodržovat limity pro počty zasílaných požadavků a zpráv na IS Objednatele za určité časové období, jak stanoví Objednatel.

2.28 Poskytovatel je povinen poskytnout Objednateli veškerou součinnost nezbytnou k tomu, aby Objednatel řádně naplňoval právní povinnosti stanovené touto Smlouvou v souladu se ZKB a Vyhláškou o kybernetické bezpečnosti.

2.29 V případě, že dojde k jakémukoliv rozporu mezi Poskytovatelem a třetí osobou, která není jeho poddodavatelem a je Poskytovatelem software nebo jiných technologií dotčených plněním povinností Poskytovatele dle této Smlouvy, je Poskytovatel povinen tuto skutečnost bez zbytečného odkladu oznámit Objednateli. Poskytovatel je dále povinen poskytovat Objednateli nutnou součinnost pro jednání s těmito třetími osobami a sám se těchto jednání účastnit, nebo na základě žádosti Objednatele jednat s těmito třetími osobami napřímo.

2.30 Objednatel má právo prostřednictvím určených osob kdykoli kontrolovat plnění této Smlouvy u Poskytovatele a jeho případných poddodavatelů, a to i prostřednictvím třetí osoby; předchozí věta se uplatní obdobně v případě kontroly některé ze Stran ze strany kontrolního orgánu ve smyslu zákona 255/2012 Sb., kontrolní řád, ve znění pozdějších předpisů.

2.31 Objednatel má právo prostřednictvím určených osob provést kdykoliv audit kybernetické bezpečnosti, tj. dodržování bezpečnosti dle požadavků ve Smlouvě a

Příručkou ICT u Poskytovatele a jeho případných poddodavatelů, a to i prostřednictvím třetí osoby. V rámci auditu kybernetické bezpečnosti je Objednatel oprávněn zejména porovnávat zjištěné skutečnosti s bezpečnostní dokumentací Poskytovatele. Poskytovatel je povinen poskytnout Objednateli požadovanou dokumentaci a součinnost v rámci auditu kybernetické bezpečnosti bez nároku na náhradu jakýchkoliv nákladů.

2.32 V rámci auditu kybernetické bezpečnosti je Objednatel oprávněn provádět penetrační testy na komponentech systému Poskytovatele (primární a podpůrná aktiva), které mají souvislost zejména s předmětem plněním, a to i prostřednictvím třetí osoby. K tomu Poskytovatel poskytne Objednateli požadovanou součinnost bez nároku na náhradu jakýchkoliv nákladů.

2.33 Poskytovatel je povinen umožnit Objednateli nebo jím pověřené osobě nebo osobě oprávněné dle obecně závazných právních předpisů kdykoli, a to i po zániku této Smlouvy (v rozsahu povinností trvajících i po zániku Smlouvy), provedení kontroly a auditu kybernetické bezpečnosti a zabezpečit (i smluvně) právo na provedení této kontroly a auditu kybernetické bezpečnosti u svých případných Poddodavatelů. O auditu, ledaže jeho provedení nesnese odkladu, informuje Objednatel Poskytovatele alespoň pět (5) pracovních dnů předem.

2.34 Poskytovatel je povinen během takového auditu Objednatelem nebo jím pověřenému auditorovi poskytnout veškerou nezbytnou součinnost, zejména:

(a) zpřístupnit veškeré prostory a veškeré dokumenty, údaje a záznamy, které přímo či nepřímo souvisejí s plněním Poskytovatelových povinností dle této Smlouvy; a

(b) poskytnout veškerou potřebnou součinnost tak, aby mohl být proveden řádný audit plnění Poskytovatelových povinností dle této Smlouvy.

2.35 Osoba provádějící audit je oprávněna pořídit kopie veškerých dokumentů, údajů a záznamů jí předložených a provést kontrolu v prostorách určených ze strany Objednatele.

2.36 Pokud Objednatel zjistí, že Poskytovatel porušuje své povinnosti dle odst. 2 této Přílohy, považuje se takový postup za podstatné porušení Smlouvy. Objednatel je v takovém případě oprávněn dožadovat se toho, aby Poskytovatel odstranil vady vzniklé vadným postupem Poskytovatele a zdržel se provádění postupů, které jsou v rozporu s odst. 2 této Přílohy, a dále tuto Smlouvou plnil řádným způsobem. Strany se dohodnou na podmínkách a lhůtě k odstranění nedostatků plnění Smlouvy ve smyslu odst. 2.36 této Přílohy, přičemž nedohodnou-li se Smluvní strany na konkrétní lhůtě, pak je Poskytovatel povinen odstranit nedostatky do třiceti (30) dnů. Jestliže Poskytovatel včas neodstraní nedostatky ve smyslu předchozí věty odstavce 2.36 této Přílohy nebo se jedná o porušení povinnosti podle odst. 2.6 této Přílohy (bez ohledu na jeho závažnost), pak je Objednatel oprávněn od Smlouvy odstoupit a požadovat po Poskytovateli úhradu smluvní pokuty dle Smlouvy.

2.37 Strany vzájemně komunikují v průběhu plnění Smlouvy za účelem dosažení standardů bezpečnosti dle odst. 2 této Přílohy. V případě ohrožení anebo porušení bezpečnosti, zejména v případě výskytu kybernetické bezpečností události anebo incidentu, jsou

Smluvní strany povinny vzájemně komunikovat, ihned po zjištění takových skutečností hlásit jejich výskyt druhé Straně a společně podnikat kroky k zajištění obnovení bezpečnosti.

2.38 Poskytovateli nenáleží za plnění povinností dle této Přílohy jakákoliv další odměna, resp. taková odměna je součástí provize.

3. Povinnosti po zániku Smlouvy

3.1 Poskytovatel je po zániku Smlouvy povinen dodržovat veškeré povinnosti dle kybernetického zákona a souvisejících předpisů.

3.2 Poskytovatel je povinen po přechodnou dobu vykonávat činnosti, které povedou k zachování kontinuity provozu a zachování bezpečnosti a ochrany informací. Zároveň má povinnost spolupracovat při předání dat Objednateli, migraci do nového řešení a podobně.

4. Poskytovatel je povinen po ukončení spolupráce průkazně zlikvidovat data, která vznikla po dobu plnění Smlouvy nebo v důsledku této činnosti v souladu s přílohou č. 4 k vyhlášce 82/2018 Sb.

Příloha č. 5 – Bezpečnostní příručka uživatele ICT ČP

1. Zkratky a pojmy

POJMY	
Autentizace	prokázání identity uživatele, zdroje nebo zařízení.
Bezpečnost informací	zachování důvěrnosti, integrity a dostupnosti informací a dalších vlastností jako např. odpovědnost, nepopiratelnost a spolehlivost.
Bezpečnostní incident	událost nebo události, které ohrožují bezpečnost informací, případně porušení bezpečnostních požadavků
Dostupnost	znamená, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.
Důvěrnost	znamená, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.
Informační a komunikační technologie (ICT)	veškerá technika, která se zabývá zpracováním a přenosem informací, a to je zejména výpočetní a komunikační technika a programové vybavení (např. firemní aplikace, e-mail, cloudová a interní úložiště, Skype pro firmy, atd.)
Integrita	znamená zajištění správnosti a úplnosti informací.
Mobilní zařízení	přenosný elektronický přístroj s různým programovým vybavením jako např. mobilní telefon, notebook, netbook, smartbook, PDA, tablet, USB zařízení apod.
Nepříznivá událost	jakákoliv událost, která vede nebo může vést k narušení bezpečnosti nebo činností ČP.
SW	Software je programové vybavení počítače - tedy programy a aplikace v počítači či mobilním zařízení.
Uživatel	každá fyzická osoba (zaměstnanec ČP nebo smluvně pověřený zaměstnanec externí fyzické nebo právnické osoby), které byl přidělen přístup k ICT ČP a příslušná přístupová oprávnění. Pro účely této příručky se jedná o uživatele ICT ČP.

2. Povinnosti uživatele

(1) Chránit informace ČP v listinné i elektronické podobě, se kterými se dostane do kontaktu při výkonu své činnosti, před případným zneužitím, poškozením, zničením nebo ztrátou.

(2) Používat pouze schválené postupy a nástroje (např. certifikáty vydané certifikační autoritou, schválený SW) k elektronické ochraně informací.

(3) Chránit zařízení a data ICT ČP před poškozením, zničením, ztrátou nebo zneužitím. Zejména uzamykáním kanceláří a pracovních prostor a vždy při odchodu z pracoviště uzamknutím pracovní plochy zařízení nebo odhlášením ze systému.

(4) Používat dostatečně silná hesla podle níže uvedených zásad:

a) heslem nebo jeho součástí nesmí být jméno uživatele nebo jeho blízkých, číslo průkazu, název organizace, pracoviště, pošty a jiné známé, nebo snadno zjistitelné informace, nejčastěji používaná hesla, hesla na základě mnohonásobně opakujících se znaků (3 a více), přihlašovací jména e-mailu, názvy systémů nebo obdobný způsob tvorby hesla.

b) délka hesla musí být dlouhé minimálně 8 znaků, doporučeno je použít délku hesla 12 znaků.

c) heslo nesmí uživatel sdílet s jinou osobou,

d) heslo je doporučeno preventivně měnit 1x za ¼ roku,

e) parametry hesla jsou kontrolovány systémem.

(5) Chránit autentizační a přístupové údaje (hesla, klíče apod.) před vyzrazením, ztrátou nebo zneužitím a v žádném případě je nikomu nesdělovat. V případě že k prozrazení dojde, musí být autentizační a přístupové údaje okamžitě změněny.

(6) Věnovat pozornost podezřelému chování lidí i ICT systémů, systémovým oznámením a hlášením bezpečnostních programů jako je například antivirová ochrana. Při zjištění nebo i jen podezření na zavirování či podezřelé chování, neprodleně toto oznámit na ServiceDesk ČP a dále se řídit jeho pokyny.

(7) Provést antivirovou kontrolu 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.

(8) Nezasahovat do systémového nastavení jednotlivých zařízení ani neprovádět instalaci nedůvěryhodných programů.

(9) Nekopírovat SW ČP na jiný počítač nebo jej předávat jiné osobě.

(10) Pracovat se zařízením tak, aby chráněné informace nemohly být odposlechnuty, odpozorovány nebo vyčteny ze zpracovávaných dokumentů a obrazovek zařízení jinou nepovolanou osobou.

(11) V případě žádosti operačního systému o restartování zařízení, v co nejkratší době ukončit veškerou činnost a restart provést.

(12) Hlásit zjištěné bezpečnostní incidenty (viz kapitola 4.1 této přílohy).

(13) Hlásit zjištěné mimořádné události Stálé operační službě na telefonní číslo 605 22 55 55. Jedná se zejména o narušení nebo zničení důležitých zabezpečovacích zařízení, výpadek dodávky elektrické energie spojený s vyřazením elektronických systémů.

3. Uživateli je zakázáno

(1) Přerušovat probíhající aktualizace systému, vypínat antivirovou ochranu nebo měnit konfiguraci bezpečnostních prvků ochrany.

(2) Pracovat s cizími autentizačními nebo přístupovými údaji.

(3) Využívat chybně přidělená oprávnění, která mu nepřísluší.

4. Bezpečnostní incident

4.1. Základní bezpečnostní incidenty

(1) Projev počítačového viru nebo jiného škodlivého SW.

(2) Nestandardní chování zařízení nebo uživatelů.

(3) Kompromitace nebo zneužití autentizačních a přístupových údajů (např. hesla), podezření nebo pokus o kompromitaci (např. podvodné emaily, neúmyslné prozrazení hesla, apod.).

(4) Ztráta nebo odcizení zařízení, mobilního zařízení nebo záznamového média obsahující informace ČP.

(5) Proniknutí nepovolané osoby na pracoviště Poskytovatele, k zařízení nebo i pokus o nepovolené proniknutí.

(6) Výstražné hlášení operačního systému nebo aplikačního SW indikující porušení bezpečnosti.

(7) Neoprávněná změna HW, SW nebo konfigurace.

(8) Ztráta důvěrnosti informací zapříčiněná například chybným nastavením oprávnění, kompromitací nebo zneužitím autentizačních údajů, nebo ztrátou či odcizením zařízení.

(9) Chybně přidělená oprávnění nad rámec mu svěřených pracovních povinností.

4.2. Řešení bezpečnostního incidentu

(1) Každý bezpečnostní incident nebo podezření na něj musí uživatel neprodleně oznámit na ServiceDesk ČP, případně přes svého nadřízeného, který incident oznámí na ServiceDesk ČP 800 26 00 26.

(2) Uživatel je povinen poskytnout ČP nezbytnou součinnost při šetření a řešení bezpečnostního incidentu. Na základě vyhodnocení bezpečnostního incidentu specializovaný útvar ČP provede potřebná opatření pro uvedení systému ČP do bezpečného stavu.

5. Doporučené nastavení zařízení Poskytovatele

V zájmu zajištění bezpečnosti doporučujeme při provozování systémů ČP používat zařízení, které:

- neobsahuje žádný nelegální SW či SW instalovaný z nedůvěryhodných zdrojů,
- používat výhradně podporovaný a aktualizovaný operační systém,
- používat pouze podporovaný a aktualizovaný Internetový prohlížeč,
- pokud je to možné používat SW pro antivirovou ochranu zařízení.

Příloha č. 6 – Etický kodex České pošty, s.p.

(Znění přílohy následuje na další straně)

Příloha č. 7 – Pravidla pro přijímání a poskytování darů a pohoštění

Tato pravidla jsou součástí Compliance programu podniku Česká pošta, s.p. (dále jen „podnik“ nebo „ČP“) a navazují na Rezortní interní protikorupční program Ministerstva vnitra ČR.

1. Obecné principy pro přijímání a poskytování darů a pohoštění

Zaměstnanci nesmí: (i) dávat a přijímat dary (ii) nabízet nebo akceptovat pozvánky na pohoštění, které by vedly ke střetu zájmů (mezi zaměstnancem a ČP a/nebo dceřinými společnostmi ČP) nebo k navození dojmu korupčního jednání či nesprávného očekávání, že touto cestou bude dosaženo ovlivnění obchodní transakce nebo výkonu pracovních povinností.

Za zcela nepřípustné bude považováno přijetí daru/pohoštění osobou blízkou zaměstnanci (nebo třetí osobou) za účelem zakrytí příjemce; tento zákaz se obdobně vztahuje i na poskytování daru nebo pohoštění.

Zcela zakázáno je poskytování/přijímání darů v penězích (v hotovostní i bezhotovostní formě) či v podobě jiných finančních instrumentů.

Dary a pohoštění je možné akceptovat nebo nabídnout pouze v průběhu běžných obchodních či jiných oficiálních vztahů a jen v odůvodněných případech, je-li to v nejlepším zájmu ČP. Vždy se musí jednat o takové dary a pohoštění, které může příjemce dárci bez problémů oplatit.

Dar (obdobně toto platí i pro pohoštění) lze přijmout/poskytnout pouze tehdy, jsou-li kumulativně naplněna následující kritéria:

- dar je vhodný za všech okolností, jeho přijetí/poskytnutí nepoškodí reputaci ČP;
- dar musí být přiměřený a akceptovatelný v kontextu podnikatelské příležitosti a v souladu s běžnou obchodní praxí. Hodnota, povaha a četnost darů musí odpovídat statutu příjemce (tj. pracovní pozici, na níž obdarovaný působí), charakteru a délce trvání obchodního či jiného oficiálního vztahu atd.;
- dar musí být nabízen otevřeně a s transparentním záměrem (např. poděkování za spolupráci, budování a rozvoj obchodních vztahů, propagace produktů a služeb ČP); lze o něm veřejně hovořit uvnitř i vně podniku, aniž by to ohrozilo reputaci a integritu ČP;
- přijetí/poskytnutí daru nesmí být načasováno shodně s obdobím probíhajícího výběrového řízení či s přijímáním rozhodnutí o obchodním případu nebo s finalizací jiné podnikatelské transakce, v níž se obdarovaný/dárce přímo či nepřímo angažuje.

Hodnotou daru/pohoštění se rozumí její vyjádření v tržních cenách (včetně DPH). Zaměstnanec ČP posuzuje hodnotu daru laickým odhadem, v případě pochybností o hodnotě daru se obrátí na svého nadřízeného nebo na odbor compliance a regulace. Zaměstnanec odpovídá za to, že jím provedený odhad hodnoty přijatého daru/pohoštění nebude ve zjevném rozporu s tržní hodnotou daru/pohoštění.

Pravidla a postupy při přijímání darů

Zaměstnanci ČP smí přijmout dar pouze výjimečně v situacích, kdy není vhodné dar odmítnout s ohledem na obchodní či jiný oficiální vztah mezi ČP a stranou nabízející dar. Je zakázáno nabízení darů jakýmkoliv způsobem podněcovat či vyžadovat.

Limitní hodnota darů, které zaměstnanec ČP smí přijmout, činí 2.000 Kč. Bez dalšího lze přijmout jen dary, které mají hodnotu do 500 Kč nebo obsahují firemní logo (reklamní předměty). V případě ostatních darů v hodnotě 500-2.000 Kč zaměstnanec informuje o jejich přijetí svého přímého nadřízeného.

Pokud hodnota nabízeného daru zjevně přesahuje výše stanovený stropní limit, zaměstnanec jeho přijetí odmítne s poukázáním na politiku ČP v této oblasti. V případě, že dar není možné odmítnout, protože by jeho nepřijetí mohlo poškodit obchodní a jiné oficiální vztahy ČP a druhé strany, může zaměstnanec ČP takovýto dar akceptovat, ale musí o této skutečnosti neprodleně písemně informovat svého nadřízeného v příslušné organizační linii (vždy na úrovni G-1; vedoucí zaměstnanci na úrovni G-1 informují generálního ředitele) a v kopii odbor compliance a regulace, který má právo dát k této záležitosti své stanovisko. V případě, že nadřízený přijetí nadlimitního daru neschválí, je zaměstnanec povinen dar bez zbytečného odkladu vrátit. Není-li možné či vhodné takovýto dar vrátit, rozhodne vedoucí zaměstnanec na úrovni G-1 nebo generální ředitel o dalším užití daru (např. pro charitativní účely).

V případech, kdy má být dar zaměstnanci doručen, je zaměstnanec povinen pro jeho doručení uvést pouze svou pracovní adresu. Případy, kdy obchodní partner nebo další subjekt vyžaduje soukromou adresu zaměstnance za účelem zaslání daru, musí být neprodleně oznámeny odboru compliance a regulace, stejně jako samotné případné doručení daru na tuto adresu.

Pravidla a postupy při nabízení darů

Zaměstnanci ČP nesmí nabízet ani slibovat dar za účelem získání neoprávněné výhody či ovlivnění oficiálního jednání. Poskytnutí daru, jeho forma, hodnota a způsob předání nesmí vzbudit zdání, že se ze strany ČP a jejích zaměstnanců jedná o korupční jednání.

V zájmu vyloučení pochybností o důvodu poskytování darů ze strany zaměstnanců ČP obchodním a dalším partnerům a jako prevence proti korupčnímu jednání musí každá organizační jednotka ČP vést přehled poskytnutých darů, jejichž kusová hodnota je rovna či přesahuje 2.000 Kč. Tato evidence, kterou je organizační jednotka povinna uchovávat po 3 roky, bude podléhat náhodným ověřovacím kontrolám, které bude provádět odbor compliance a regulace nebo odbor interní audit a řízení rizik. Minimální náležitosti evidence představují datum předání, jméno a funkce zaměstnance ČP předávajícího dar, jméno/název obdarovaného, popis daru, hodnota daru; odbor compliance a regulace je oprávněn upřesnit náležitosti této evidence.

Pravidla pro přijímání pohoštění (včetně účasti na společenských a dalších akcích)

Zaměstnanec ČP může bez dalšího akceptovat – jako projev zdvořilosti v obchodních či jiných oficiálních vztazích - příležitostné pozvání na občerstvení (např. pracovní oběd, pracovní večeře), avšak ve formě, úrovni a hodnotě, kterou může protistraně toto pozvání běžně oplatit.

V případě pozvání na společenské či další akce pořádané zákazníky ČP, dodavateli ČP a dalšími třetími stranami platí obdobně výše uvedená pravidla pro pozvání na občerstvení, jedná-li se o jednorázové akce s prokazatelně smíšeným obsahem (věcná náplň – např. prezentace nových produktů a služeb, odborný seminář; kulturní, sociální, sportovní a jiný, společensky obecně akceptovatelný, program, včetně občerstvení), které trvají maximálně jeden den a nezahrnují dopravu a/nebo ubytování na náklady hostitele.

Pokud pozvání na společenskou a další akci nesplňuje výše uvedené parametry, pak účast zaměstnance ČP na takovéto akci podléhá striktně předchozímu souhlasu jeho nadřízeného v příslušné organizační linii (vždy na úrovni G-1; vedoucím zaměstnancům na úrovni G-1 uděluje souhlas generální ředitel), který o svém rozhodnutí následně informuje odbor compliance a regulace. V případě, že účast zaměstnance ČP na společenské či jiné akci (nesplňující výše uvedené parametry) je schválena jako (tuzemská či zahraniční) pracovní cesta, pak se na ni tato pravidla nevztahují. Pokud nadřízený s účastí zaměstnance ČP na takovéto společenské a další akci souhlasí, avšak nikoliv na bázi pracovní cesty, může zaměstnanec ČP přijmout pozvání v případě, že si uhradí výdaje na cestu a

ubytování a na dobu nepřítomnosti v práci bude čerpat dovolenou nebo bude mít schválenou jinou zákonnou formu nepřítomnosti.

Pravidla pro nabízení pohoštění (včetně účasti na společenských a dalších akcích pořádaných ČP)

Zaměstnanci ČP nesmí nabízet ani slibovat pozvání na pohoštění (nebo na společenské a další akce pořádané ČP) za účelem získání neoprávněné výhody či ovlivnění oficiálního jednání.