

SMLOUVA O POSKYTOVÁNÍ SLUŽBY

Číslo smlouvy Objednatele: CES 2018 / 0023

Číslo smlouvy Poskytovatele: S-MIVA-0089879

Smluvní strany:

Městská část Praha 1

se sídlem: Vodičkova 681/18, 115 68, Praha 1
zastoupená: Ing. Oldřichem Lomeckým, starostou městské části Praha 1
IČ: 00063410
DIČ: CZ00063410
bankovní spojení: Česká spořitelna, pobočka Praha 1
č. účtu 27-2000727399/0800
(dále jen „Zadavatel“)

a

YOUR SYSTEM, spol. s r. o.

Se sídlem: Tůrkova 2319/5b, Praha 4 – Chodov, 149 00
Zastoupený: Ing. Petrem Fialou, jednatelem
IČ: 00174939
DIČ: CZ00174939
bankovní spojení: UniCredit Bank Czech Republic, a.s.
č. účtu 381610004/2700

zapsána v obchodním
rejstříku vedeném Městským soudem v Praze, oddíl C, vložka č. 72.
(dále jen „Poskytovatel“)

(Zadavatel a Poskytovatel dále společně též jako „smluvní strany“)

se níže uvedeného dne, měsíce a roku, v souladu s ustanoveními § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, s přihlédnutím k ust. § 2586 a násl. zákona č. 89/2012 Sb., občanského zákoníku, dohodly na základě usnesení Rady MČ Praha 1 č. UR18_0046 ze dne 9. 1. 2018 a vzájemného konsenzu o všech dále uvedených ustanoveních tak, jak stanoví tato:

SMLOUVA O POSKYTOVÁNÍ SLUŽBY

I.

Preambule

1. Tato smlouva je uzavírána na základě výsledků výběrového řízení dle zákona č. 134/2016 Sb. o zadávání veřejných zakázek pro zadání podlimitní veřejné zakázky s názvem „Správa ICT“ zahájené na základě výzvy k podání nabídek ze dne 11. 12. 2018.
2. Poskytovatel prohlašuje, že se náležitě seznámil se všemi zadávacími podmínkami veřejné zakázky malého rozsahu (dále jen „Zadávací dokumentace“), a které stanovují požadavky na předmět plnění Smlouvy, a že je odborně způsobilý ke splnění všech jeho závazků

podle Smlouvy. Poskytovatel dále prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu plnění, že jsou mu známy veškeré relevantní technické, kvalitativní a jiné podmínky nezbytné k realizaci předmětu plnění, a že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci předmětu plnění za dohodnutou maximální smluvní cenu uvedenou ve Smlouvě. Poskytovatel prohlašuje, že nemůže nastat změna skutečností, které by plnění předmětu plnění dle této smlouvy podstatně ztěžovala. Poskytovatel prohlašuje, že pokud by se v rámci plnění vznikla potřeba jiného úsilí nebo jiných nákladů, než bylo předpokládáno, nemá to vliv na cenu sjednanou v této smlouvě.

3. Pro účely výkladu této smlouvy se pod následujícími pojmy rozumí:

- ↘ **Podpora** - externí správa
- ↘ **IT** - informační technologie
- ↘ **ICT** - informační a komunikační technologie
- ↘ **IS** - informační systém
- ↘ **SW** - software
- ↘ **ASW** - agendový software
- ↘ **ESW** - ekonomický software
- ↘ **LAN** - místní, lokální počítačová síť
- ↘ **SLA** - service level agreement – dohoda o úrovni poskytovaných služeb
- ↘ **HW** – hardware
- ↘ **HelpLine** - komunikační centrum pro podchycení všech požadavků a problémů
- ↘ **HelpDesk** - informační a asistenční centrum, které odstraňuje problémy s počítačem, obdobnými produkty, nebo softwarem
- ↘ **Integrace** - sjednocení, začlenění
- ↘ **Migrace** - převod dat
- ↘ **Update** - aktualizace
- ↘ **Upgrade** - modernizace
- ↘ **Profylaxe** - preventivní kontroly a prohlídky kancelářské a výpočetní techniky
- ↘ **NBÚ** - Národní bezpečnostní úřad
- ↘ **DPH** - daň z přidané hodnoty
- ↘ **maintenance** - podpora, údržba
- ↘ **ČR** - Česká republika
- ↘ **MHMP** - Magistrát hlavního města Prahy
- ↘ **MČ** - Městská část Praha 1
- ↘ **ÚMČ** - Úřad městské části Praha 1
- ↘ **ISVZ** - Informační systém veřejné správy
- ↘ **Patch** - provizorní oprava
- ↘ **Uživatelský interface** - SW (programy) aplikace koncových uživatelů
- ↘ **Konfigurace** – nastavení
- ↘ **Kritický incident** - stav, kdy služba nebo systém či HW Zadavatele, ke kterým se poskytovaná služba vztahuje, není použitelná ve svých základních a klíčových funkcích a současně zásadním způsobem ohrožuje běžný provoz Zadavatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody.
- ↘ **Omezující incident** – stav, kdy služba nebo systém zadavatele, ke kterým se poskytovaná služba vztahuje, je plně funkční, ale vyžaduje nestandardní přístupy a postupy, které pracovníky obtěžují a omezují v jejich činnostech.
- ↘ **Ostatní incident** – nežádoucí stav služby, avšak služba je použitelná ve svých základních a klíčových funkcích a současně zásadním způsobem neohrožuje běžný provoz Zadavatele v jeho klíčových procesech a aktivitách, resp. nezpůsobuje větší finanční nebo jiné kritické škody.

4. V případě jakékoliv nejistoty ohledně výkladu jednotlivých ustanovení Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel a cíle Veřejné zakázky vyjádřený a vyplývající ze Zadávací dokumentace a této Smlouvy.

II.

Předmět smlouvy

1. Účelem Smlouvy je podpora stávajících informačních technologií Zadavatele, za kterou se Zadavatel zavazuje zaplatit Poskytovateli odměnu uvedenou v čl. III odst. 1 této smlouvy.
2. Předmětem plnění podlimitní veřejné zakázky je řádné poskytování následujících služeb:
 - Služba S01 – provoz serverů a datových úložišť
 - Služba S02 – provoz databázové infrastruktury
 - Služba S03 – provoz koncových stanic, notebooků a ostatních přenosných zařízení
 - Služba S04 – zálohování
 - Služba S05 – tiskárny, multifunkční tisková zařízení, periférie
 - Služba S06 – Reporting
 - Účast minimálně jednoho pracovníka Zadavatele, který v rozsahu provozní doby Zadavatele bude plnit funkci koordinátora realizace předmětu veřejné zakázky;
 - Trvalá účast minimálně dvou pracovníků Zadavatele, kteří v rozsahu provozní doby Zadavatele budou plnit funkce realizace předmětu veřejné zakázky;
 - Předání veškeré dokumentace spojené s plněním podle této smlouvy zadavateli nebo jím určené třetí osobě v den ukončení poskytování služby nebo dle pokynů Zadavatele, nejpozději do 5 pracovních dní od ukončení poskytování služby;
 - Návrhy na optimalizaci / zefektivnění ICT zadavatele, vycházející z realizace poskytnutých služeb;
 - Nutná součinnost při realizaci požadavků nad rámec služeb S01 – S05 v rozsahu 40 hodin měsíčně. Nevyčerpané hodiny se nepřevádějí.
3. Bližší způsob a rozsah poskytování služeb je popsán v jednotlivých kvalitativních a kvantitativních parametrech služby (dále jen SLA), které jsou uvedeny v přílohách „Technická specifikace předmětu veřejné zakázky“ a „Popis infrastruktury ICT MČP1“.

III.

Cena plnění a způsob fakturace

1. Celková cena plnění za období od 1. 2. 2018 do 31. 1. 2020 je nabídkovou cenou uchazeče vzešlou z výsledků výběrového řízení u veřejné zakázky „Správa ICT“ a představuje částku.

Celková cena bez DPH činí	3 888 000,-Kč
Zákonné DPH činí	816 480,-Kč
Celková cena včetně DPH činí	4 704 480,-Kč

Tato částka se stanovuje jako nejvýše přípustná a obsahuje veškeré náklady Poskytovatele, včetně ostatních prací spojených s poskytováním plnění a nezbytné míry zisku. Součástí ceny plnění jsou i služby či dodávky, které v zadávací dokumentaci nebo ve smlouvě nejsou výslovně uvedeny, ale Poskytovatel jakožto odborník o nich ví nebo má vědět, že jsou nezbytné pro řádné plnění dle této smlouvy.

2. Cena služby dle čl. III odst. 1 této smlouvy je splatná pravidelným měsíčním paušálem ve výši 162 000,-Kč (slovy jedno sto šedesát dva tisíc korun českých) bez DPH za každý ukončený kalendářní měsíc poskytovaných služeb na základě Zadavatelem odsouhlaseného a podepsaného soupisu poskytnutých služeb a jejich dostupnosti (tzv. Akceptační protokol), který obsahuje zhodnocení kvalitativních parametrů poskytnuté služby za uplynulý měsíc. Akceptační protokol bude podepsán oprávněnými osobami dle čl. VII odst. 6 této smlouvy, vždy nejpozději do 10. dne následujícího kalendářního měsíce. Akceptační protokol bude rovněž přílohou daňového dokladu. Za neukončené měsíce (či počáteční neúplný kalendářní měsíc) se platí alikvotní část měsíčního paušálu uvedeného v tomto odstavci.
3. Průběh odsouhlasení Akceptačního protokolu: Poskytovatel předloží Zadavateli návrh znění Akceptačního protokolu za předcházející kalendářní měsíc nejpozději do pátého pracovního dne následujícího skončení dotčeného kalendářního měsíce. Oprávněná osoba Zadavatele provede vyhodnocení služeb do pěti pracovních dnů od předání Návrhu Akceptačního protokolu. V případě nesouhlasu Zadavatele (oprávněné osoby) s návrhem Akceptačního protokolu jsou oprávněné osoby Zadavatele a Poskytovatele povinny tento rozpor začít řešit nejpozději do dvou pracovních dnů. Nedílnou součástí Návrhu akceptačního protokolu musí být i vyhodnocení SLA v podobě detailního reportu pro každou poskytovanou službu a každého v jejím rámci nahlášeného incidentu, obsahujícího relevantní údaje pro výpočet dostupnosti služby; relevantními údaji se rozumí zejména údaje uvedené v algoritmu výpočtu dostupnosti popsáném v tomto materiálu.
4. Zadavatel neposkytuje dle této smlouvy zálohy.
5. Oprávněně vystavený daňový doklad musí mít veškeré náležitosti daňového dokladu (faktury) dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Dále musí obsahovat i tyto údaje:
 - ↘ pořadové číslo faktury, datum vystavení a datum splatnosti faktury, datum uskutečnění zdanitelného plnění;
 - ↘ identifikaci Poskytovatele podle Obchodního rejstříku, pakliže je v něm zapsán;
 - ↘ označení banky a čísla účtu Poskytovatele dle této smlouvy;
 - ↘ celkovou fakturovanou částku bez DPH, vyčíslení sazby a výše DPH a celkovou cenu vč. DPH;
 - ↘ evidenční údaje akce („název veřejné zakázky malého rozsahu“);
 - ↘ vlastnoruční podpis vystavitele, včetně kontaktního telefonního čísla;
 - ↘ Akceptační protokol.
6. Délka splatnosti daňových dokladů (faktur) je 21 dnů od jejich doručení Zadavateli.
7. V případě, že faktura nebude obsahovat potřebné náležitosti uvedené v předešlém odstavci, nebo bude obsahovat chybné či neúplné údaje (vč. chybně účtované ceny) či nebude připojen oboustranně podepsaný Akceptační protokol se zhodnocením kvalitativních parametrů za uplynulý kalendářní měsíc, je Zadavatel oprávněn ji vrátit Poskytovateli k opravě či doplnění s uvedením důvodu vrácení. Vrácení faktury musí být provedeno do data její splatnosti. Po vrácení faktury (nové či opravené) počíná běžet nová lhůta splatnosti uvedená v čl. III odst. 6 této smlouvy.
8. Zadavatel je oprávněn pozastavit či jednostranně započíst proti pohledávkám Poskytovatele kteroukoli z plateb z důvodu (1) škody způsobené Zadavateli, (2) opakovaného neplnění ze strany Poskytovatele (mimo mechanismy dle SLA a slevy z paušálu dle následujícího odstavce), (3) v případě existence jakýchkoliv oprávněných finančních či jiných nároků Zadavatele vůči Poskytovateli, nebo (4) uplatnění smluvních pokut. V případě, že taková pohledávka neexistuje, bude faktura uhrazena v souladu a ve výši dle předchozích odstavců tohoto článku. Poskytovatel není oprávněn započíst žádnou svou pohledávku proti pohledávce Zadavatele z této smlouvy.
9. V případě, že Zadavatel uplatní slevu za neplnění kvalitativních parametrů poskytovaných služeb stanovenou dle čl. XIII odst. 16 smlouvy, bude sleva uvedena v Akceptačním

protokolu a v případě uplatnění slevy bude Poskytovatel fakturovat cenu dle předchozího článku sníženou o stanovenou slevu.

10. Smluvní strany se dohodly, že stane-li se Poskytovatel nespolehlivým plátcem nebo daňový doklad Poskytovatele bude obsahovat číslo bankovního účtu, na který má být plněno, aniž by bylo uvedeno ve veřejném registru spolehlivých účtů, je Zadavatel oprávněn z finančního plnění uhradit daň z přidané hodnoty přímo místně a věcně příslušnému správci daně Poskytovatele.
11. Fakturovaná částka se považuje uhrazenou okamžikem jejího odepsání z účtu Zadavatele.

IV.

Doba plnění

1. Zahájení poskytování služeb dle této Smlouvy je staveno dnem 1.2.2018 s tím, že služby budou poskytovány od samého počátku doby plnění bez existence tzv. přechodného období.
2. Doba poskytování plnění dle smlouvy vzešlé z výběrového řízení je do 31.1.2020.

V.

Způsob poskytování plnění služby, povinnosti smluvních stran

1. Poskytovatel je povinen poskytnout Zadavateli plnění definované v čl. II. této smlouvy za podmínek sjednaných v této smlouvě, na svou odpovědnost a po sjednanou dobu.
2. Poskytovatel se zavazuje, že bude při poskytování plnění postupovat s odbornou péčí, podle svých nejlepších znalostí a schopností a sledovat a chránit oprávněné zájmy Zadavatele. Poskytovatel se dále zavazuje dodržovat obecně závazné předpisy, technické normy a ustanovení této smlouvy.
3. Poskytovatel je povinen vykonávat své povinnosti podle podmínek této Smlouvy v souladu s legislativním rámcem této Smlouvy a interními předpisy Zadavatele, se kterými bude Poskytovatel seznámen. O seznámení musí být učiněn písemný zápis. Legislativní rámec tvoří:
 - ↘ splnění požadavků legislativy ČR, vztahující se k předmětu plnění této Smlouvy,
 - ↘ splnění metodik vydávaných pro územní samosprávné celky (vydávají centrální a jimi pověřené orgány a Magistrátu hl. města Prahy (MHMP)), se kterými bude Poskytovatel seznámen,
 - ↘ splnění metodik Zadavatele, se kterými bude Poskytovatel seznámen.
4. Poskytovatel je povinen po celou dobu platnosti smlouvy zajistit pro Zadavatele (potažmo i pro veřejnost coby koncové uživatele některých aplikací) dostupnost služeb, a to v souladu s přílohou D01 Technická specifikace předmětu veřejné zakázky a D02 Popis infrastruktury ICT MČ P1. Zejména je povinen provádět plnou instalaci, integraci, řešit vady a kritické stavy IS s jejími dodavateli v jím garantovaných termínech, pomáhat uživatelům na jednotlivých pracovištích Zadavatele a vytvářet a předávat Zadavateli administrátorskou a uživatelskou dokumentaci.
5. Při poskytování služby je Poskytovatel povinen se řídit pravidly a omezeními uvedenými v příloze D04 - Etalon minimální bezpečnosti pro smluvní partnery.
6. Poskytovatel je povinen provádět pravidelné zálohování dat, a to v rozsahu a v intervalech stanovených v příloze D01 Technická specifikace předmětu veřejné zakázky.
7. Poskytovatel má povinnost Zadavateli nabízet řešení, která mu umožní zajistit bezporuchový běh celého informačního systému. Poskytovatel dále zodpovídá za integraci SW, HW a to s ostatním již použitým HW, SW a daty.

8. Poskytovatel je povinen informovat Zadavatele na jeho žádost o průběhu plnění předmětu smlouvy a akceptovat jeho doplňující pokyny a připomínky k plnění předmětu smlouvy. Poskytovatel je však povinen bez zbytečného odkladu písemně upozornit Zadavatele na nevhodnou povahu věci, kterou mu Zadavatel k provedení plnění předal, nebo příkazu (pokynu), který mu Zadavatel dal. To neplatí, nemohl-li nevhodnost zjistit ani při vynaložení potřebné péče.
9. Poskytovatel je povinen v aktuálním stavu udržovat potřebnou dokumentaci spojenou s plněním podle této smlouvy. Dokumentace je uložena v prostředí Zadavatele. Poskytovatel je dále povinen poskytovat Zadavateli informace a dokumenty tak, jak je specifikováno v jednotlivých SLA, a další operativní informace, které jsou nezbytné pro plnění předmětu této Smlouvy.
10. Poskytovatel se zavazuje provádět plnění předmětu této Smlouvy tak, aby nebyla ohrožena realizace těch činností Zadavatele, pro jejichž podporu je předmět této Smlouvy určen.
11. Veškeré odborné práce musí vykonávat pracovníci Poskytovatele mající příslušnou kvalifikaci. Doklad o příslušné kvalifikaci pracovníků je Poskytovatel na požádání Zadavatele povinen doložit. Poskytovatel odpovídá za to, že bude mít pro své zaměstnance poskytující plnění veškerá potřebná školení a platná kvalifikační potvrzení.
12. Použije-li Poskytovatel k plnění podle této smlouvy poddodavatele, musí si vyžádat písemný souhlas Zadavatele, jenž tento souhlas bezdůvodně neodmítne. Za plnění poddodavatelů odpovídá Poskytovatel tak, jakoby plnil sám.
13. Zadavatel je povinen předat a bude předávat Poskytovateli všechny potřebné informace a údaje, které má Zadavatel a které jsou nutné proto, aby Poskytovatel mohl vykonávat služby podle této Smlouvy. Zároveň se zavazuje zodpovídat dotazy Poskytovatele ve vztahu k plnění podle této Smlouvy, a to do dvou pracovních dnů od obdržení dotazu, nedohodnou-li se smluvní strany v konkrétním případě jinak.
14. Zadavatel se zavazuje umožnit přístup pracovníkům Poskytovatele do objektů Zadavatele a ke spravované technice a systémům v rozsahu nezbytném pro plnění předmětu této smlouvy.
15. Poskytovatel se zavazuje, že zajistí, aby jeho pracovníci podílející se na plnění podle této Smlouvy při pobytu na pracovištích Zadavatele dodržovali vnitřní předpisy, pokyny a směrnice Zadavatele, dodržovali předpisy Zadavatele upravující pohyb na pracovištích, pro požární bezpečnost, pro ochranu zdraví při práci a další předpisy, se kterými bude Poskytovatel seznámen, přičemž Poskytovatel zajistí, že o takovém seznámení bude pořízen písemný zápis.
16. Pracovníci Poskytovatele pohybující se na pracovištích Zadavatele budou vždy označeni visačkou se jménem a fotografií.
17. Poskytovatel není oprávněn bez souhlasu Zadavatele, s výjimkou příslušných ustanovení zákona č. 89/2012 Sb. a 90/2012 Sb. týkajících se přeměny společnosti, postoupit svá práva a závazky vyplývající z této Smlouvy na třetí osoby, a to včetně postoupení pohledávky, dluhu, ručení, zástavy i jakéhokoli zajištění závazku.

VI.

Místo plnění

1. Místem plnění Poskytovatele je sídlo Zadavatele a všechna jeho pracoviště v Praze. Služby, u kterých je s ohledem na jejich charakter možné, mohou být poskytovány i vzdáleným přístupem do prostředí Zadavatele z pracoviště Poskytovatele.
2. Pracoviště Zadavatele jsou uvedena v Příloze č D01 smlouvy Technická specifikace předmětu veřejné zakázky.

VII.

Součinnost smluvních stran

1. Smluvní strany se zavazují poskytnout druhé smluvní straně dohodnutou součinnost umožňující řádné plnění této smlouvy.
2. Smluvní strany se zavazují úzce spolupracovat, zejména si poskytovat úplné, pravdivé a včasné informace potřebné k řádnému plnění svých závazků, přičemž v případě změny podstatných okolností, které mají nebo mohou mít vliv na plnění prováděcí smlouvy, jsou povinny o takové změně informovat druhou smluvní stranu nejpozději do tří pracovních dnů po provedení takové změny.
3. V zájmu optimálního plnění této smlouvy jsou smluvní strany povinny plnit řádně a včas své závazky tak, aby nedocházelo k prodlení s jejich plněním. Pokud se některá ze smluvních stran dostane do prodlení s plněním svých závazků, je povinna oznámit bez zbytečného odkladu druhé smluvní straně důvod prodlení a předpokládaný termín a způsob jeho odstranění.
4. Smluvní strany se zavazují plnit své závazky v souladu se všemi příslušnými obecně závaznými legislativními předpisy.
5. Žádná ze smluvních stran není odpovědna za prodlení způsobené prodlením s plněním závazků druhé smluvní strany.
6. Komunikace smluvních stran probíhá na úrovni oprávněných osob a jejich zástupců. Zástupci oprávněných osob přitom oprávněnou osobu zastupují v rámci její působnosti. Za tím účelem se stanovují následující osoby:

Zadavatel	Jméno a příjmení	Kontaktní telefon	Kontakt email
oprávněná osoba			
zástupce oprávněné osoby			
Poskytovatel			
oprávněná osoba			
zástupce oprávněné osoby			

7. Stanovením kontaktních osob a jejich zástupců není dotčena možnost smluvních stran komunikovat prostřednictvím svých statutárních orgánů.
8. Všechny dokumenty mající vztah k plnění této smlouvy, představující vícestranné či jednostranné úkony smluvních stran, například zápisy z jednání, dodatky k zadání, protokoly, výzvy, výpovědi, upozornění, žádosti a jiná oznámení, musí být vyhotoveny písemně a podepsány oprávněnými osobami.
9. Dokumenty uvedené v předchozím odstavci se vždy doručují druhé smluvní straně, a to některým ze způsobů dále uvedených:
 - osobně oproti podpisu
 - doporučeným dopisem či jinou formou registrovaného poštovního styku. V tomto případě se dokumenty považují za doručené dnem jejich převzetí adresátem, nebo v případě, že adresát nebyl zastižen dnem doručení zpět odesílateli a dále dnem, kdy adresát převzetí zásilky odmítl,
 - Prostřednictvím datové schránky nebo elektronickou poštou. V tomto případě se dokumenty považují za doručené okamžikem, kdy odesílatel obdrží od příslušného technického zařízení potvrzení o úspěšném odeslání nebo potvrzení o doručení.
10. V případě doručování dokumentů v elektronické formě smluvní strany zavazují používat

formát „.doc(x)“, nebo „.pdf“. Dokumenty v elektronické formě lze doručovat prostřednictvím elektronické pošty, prostřednictvím datové schránky nebo na dohodnutém datovém médiu.

11. V případě doručování dokumentů v listinné podobě či na datových nosičích se dokumenty doručují na adresy smluvních stran uvedených v záhlaví této smlouvy, není-li stanoveno nebo dohodnuto jinak.
12. Další požadavky na součinnost mohou písemně dohodnout oprávněné osoby smluvních stran pro jednotlivé SLA nebo odpovědné osoby za SLA v rozsahu působnosti SLA.

VIII.

Autorská a vlastnická práva

1. Poskytovatel prohlašuje, že předmět Smlouvy ani jeho části, které jsou/mohou být autorským dílem Poskytovatele, nemají žádné právní vady, že nejsou zatíženy právy třetích osob, a že Poskytovatel je zcela oprávněn vykonávat veškerá majetková práva v celém rozsahu, s autorským dílem disponovat a uzavřít se Zadavatelem smlouvu na celý rozsah předmětu plnění dle Smlouvy.
2. K výstupům Poskytovatele, které budou podléhat ochraně podle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), v platném znění, získává Zadavatel licenci, teritoriálně omezenou územím České republiky, bez omezení množstevního rozsahu. Dnem úplného zaplacení ceny příslušného plnění se licence stává časově omezenou pouze dobou trvání majetkových autorských práv. Cena licence je zahrnuta v ceně služeb. Při ukončení účinnosti prováděcí smlouvy budou tyto výstupy předány Zadavateli pro jeho interní užití bez povinnosti platit jakékoliv poplatky, pokud Zadavatel nebude požadovat jeho podporu (maintenance).

IX.

Ochrana důvěrných informací

1. Smluvní strany se zavazují zachovávat mlčenlivost ohledně skutečností, které se v souvislosti s plněním této Smlouvy dozvěděly, a to v rozsahu sjednaném v tomto článku Smlouvy. Za důvěrné informace jsou považovány jednak veškeré informace bez ohledu na formu jejich zachycení, které nebyly označeny jako veřejné a které se týkají Smlouvy, předmětu Smlouvy v ní sjednaného (zejména informace o právech a povinnostech smluvních stran, jakož i informace o cenách) či porušení zmíněné Smlouvy, dále (zejména, nikoliv však výlučně) obchodní tajemství, informace o činnosti příslušné smluvní strany, struktura, hospodářských výsledcích, know-how), nebo případné informace, pro nakládání s nimiž je stanoven právními předpisy zvláštní režim utajení (osobní údaje, aj.), jednak informace, které byly jako důvěrné výslovně příslušnou smluvní stranou označeny; za důvěrné informace se však nepovažují informace, které se staly veřejně přístupnými, pokud se tak nestalo porušením povinnosti jejich ochrany jednou ze smluvních stran, dále informace získané na základě postupu nezávislého na této smlouvě, pokud je příslušná smluvní strana schopna tuto skutečnost doložit, a konečně informace poskytnuté třetí osobou, která takové informace nezískala porušením povinnosti jejich ochrany některé ze smluvních stran (dále jen jako „Důvěrné informace“).
2. Poskytovatel je povinen Důvěrné informace ochránit proti úniku či neoprávněnému užití. Důvěrné informace mohou být Poskytovatelem využívány výlučně pro přípravu a poskytování předmětu smlouvy dle Smlouvy, není-li ve Smlouvě uvedeno jinak. Poskytovatel se zavazuje zachovávat mlčenlivost o Důvěrných informacích a zavazuje se, že přijme odpovídající opatření k ochraně Důvěrných informací.
3. Poskytovatel se zavazuje, že Důvěrné informace, které v souvislosti s poskytováním předmětu Smlouvy nebo při přípravě poskytování předmětu Smlouvy Poskytovateli poskytne Zadavatel, nebude bez písemného souhlasu Zadavatele žádným způsobem rozmnožovat (kromě potřebných kopií pro poskytnutí předmětu Smlouvy) a kdykoliv je na

požádání vrátí Zadavateli, včetně všech případně vzniklých kopií a nosičů Důvěrných informací, nebo je na základě požadavku této smluvní strany zničí, včetně všech případně vzniklých kopií a nosičů Důvěrných informací.

4. Poskytovatel se zavazuje, že bez písemného souhlasu Zadavatele neposkytne Důvěrné informace v žádné formě třetím osobám. Poskytovatel je povinen zajistit, že jeho případný poddodavatel bude zachovávat mlčenlivost o Důvěrných informacích. Poruší-li poddodavatel Poskytovatele povinnost mlčenlivosti ve vztahu k Důvěrným informacím, považuje se to za porušení povinnosti mlčenlivosti Poskytovatele.
5. Za porušení povinnosti mlčenlivosti se nepovažuje, je-li Poskytovatel, jeho zaměstnanec, spolupracující osoba, zástupce nebo další osoba v obdobném postavení povinen Důvěrnou informací sdělit na základě zákonem stanovené povinnosti.
6. Poskytovatel je povinen uvědomit Zadavatele o porušení povinnosti mlčenlivosti nebo ochrany Důvěrných informací podle Smlouvy bez zbytečného odkladu poté, co se o takovém porušení dozví.
7. Povinnost mlčenlivosti a ochrany Důvěrných informací podle Smlouvy trvá po dobu účinnosti Smlouvy a dále 3 (slovy: tři) roky po jejím ukončení.
8. Vzhledem k veřejnoprávnímu charakteru Zadavatele Poskytovatel výslovně prohlašuje, že je s touto skutečností obeznámen, že žádné ustanovení této Smlouvy nepodléhá z jeho strany obchodnímu tajemství a souhlasí se zveřejněním smluvních podmínek obsažených ve Smlouvě, včetně jejích příloh a případných dodatků Smlouvy za podmínek vyplývajících z příslušných právních předpisů, zejména zák. č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů a zákona č. 340/2015 Sb. o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

X.

Pojištění

1. Poskytovatel se zavazuje, že po celou dobu poskytování svých služeb podle této smlouvy bude pojištěn pro případy škody vyplývající z výkonu svojí podnikatelské činnosti na částku předmětného pojištění alespoň 2.000.000 Kč s max. 10% spoluúčastí. Kopie pojistné smlouvy (či pojistný certifikát) je pak přílohou č. D03 této smlouvy. Poskytovatel je povinen být pojištěn i proti případným odcizením, ztrátám či poškození věcí Zadavatele.

XI.

Odpovědnost za způsobenou škodu, záruka za jakost plnění, vady plnění

1. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu dle platných právních předpisů a Smlouvy.
2. Poskytovatel odpovídá za škodu rovněž v případě, že část plnění poskytuje prostřednictvím poddodavatele. Poskytovateli se zavazuje uhradit Zadavateli či orgánu veřejné moci veškeré finanční částky, které budou Poskytovateli ve správním, soudním či jiném obdobném řízení uloženy jako pokuty či jiné majetkoprávní sankce za Poskytovatelem způsobené porušení právních povinností.
3. Žádná ze smluvních stran není odpovědná za škodu nebo prodlení způsobené okolnostmi vylučujícími odpovědnost ve smyslu Občanského zákoníku. Smluvní strany se zavazují upozornit druhou smluvní stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost a bránící řádnému plnění Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání okolností vylučujících odpovědnost.
4. Poskytovatel přebírá závazek a odpovědnost za jím způsobené vady předmětu smlouvy, jež bude mít v době jeho předání Zadavateli a dále za vady, které se na předmětu Smlouvy

vyskytnou v průběhu záruční doby. Poskytovatel v souvislosti s odpovědností za vady plnění poskytuje Zadavateli záruku, která skončí uplynutím 24 (slovy: dvacet čtyři) měsíců od zahájení plnění, na to, že předmět Smlouvy bude mít vlastnosti stanovené Smlouvou, bude plně funkční a způsobilé pro použití ke smlouvenému účelu, bude odpovídat sjednané funkční a technické specifikaci a parametrům uvedeným ve Smlouvě a bude bez jakýchkoliv nedodělků či vad. Záruka se vztahuje na všechny části plnění, včetně jeho příslušenství a pokrývá všechny součásti plnění předmětu Smlouvy, včetně produktů či činností třetích stran, které byly využity při realizaci plnění dle Smlouvy.

5. Poskytovatel je povinen poskytovat plnění dle Smlouvy v nejvyšší dostupné kvalitě a odpovídá za to, že případné vady plnění poskytnutého dle Smlouvy řádně odstraní, případně nahradí plněním bezvadným, v souladu se Smlouvou a jejími přílohami.
6. Jakékoliv vady plnění předmětu Smlouvy, které vzniknou v záruční době, je Poskytovatel povinen odstranit na své náklady v rámci poskytovaného plnění dle Smlouvy a to způsobem ve Smlouvě uvedeným, zejména v souladu se SLA parametry obsaženými v příloze č. 1 Smlouvy.
7. V případě výskytu incidentu je Poskytovatel povinen zahájit jeho řešení a incident vyřešit ve lhůtách stanovených v příloze D01 této smlouvy Technická specifikace předmětu veřejné zakázky. Úvodem je Poskytovatel povinen ve stanovené době dle přílohy D01 potvrdit příjem hlášení incidentu Zadavateli prostřednictvím HelpDesku Zadavatele, ve kterém validuje navrženou závažnost incidentu (kritický, omezující nebo ostatní) a dle povahy incidentu oznámí, jak bude řešit nebo navrhne způsob jeho řešení (např. také předání k řešení třetím stranám). V případě sporu o tom, zda nahlášený incident je svojí povahou kritický či ostatní, je rozhodující stanovisko oprávněné osoby Zadavatele uvedené v čl. VII. Odst. 6 této smlouvy, která buď povahu incidentu a způsob jeho vyřešení akceptuje nebo navrhne jeho změnu.

XII.

Zánik smlouvy

1. Tato smlouva primárně zaniká primárně splněním, resp. uplynutím předpokládané doby, tj. 31.1.2020. Před uvedeným datem smluvní strany dále mohou ukončit smluvní vztah písemnou dohodou obou smluvních stran. Dále tato smlouva může zaniknout i jednostrannou výpovědí či odstoupením od smlouvy ze strany Zadavatele s výpovědní lhůtou 2 měsíce. Výpovědní lhůta začíná běžet dnem doručení výpovědi Poskytovateli
2. Zadavatel je oprávněn odstoupit od této smlouvy:
 - ↘ v případě, že probíhá insolvenční řízení proti majetku Poskytovatele, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh byl zamítnut proto, že majetek Poskytovatele nepostačuje k úhradě nákladů insolvenčního řízení, nebo byl konkurs zrušen proto, že majetek Poskytovatele byl zcela nepostačující;
 - ↘ v případě podstatného porušení této smlouvy Poskytovatelem, zejména v případě kdy Poskytovatel využil k plnění předmětu této smlouvy poddodavatele v rozporu s nabídkou Poskytovatele v rámci výběrového řízení nebo bez předchozího souhlasu Zadavatele,
3. Zadavatel je také oprávněn odstoupit od této smlouvy v případě, kdy vyjde najevo, že Poskytovatel uvedl v rámci výběrového řízení nepravdivé či zkreslené informace, které by měly zřejmý vliv na výběr Poskytovatele pro uzavření této smlouvy.
4. Smluvní strany jsou oprávněny od této smlouvy dále odstoupit za podmínek stanovených občanským zákoníkem nebo jinými právními předpisy.
5. Odstoupení od smlouvy musí být učiněno písemným oznámením o odstoupení od této smlouvy druhé straně, účinky odstoupení nastávají dnem doručení oznámení druhé straně. V pochybnostech se má za to, že odstoupení bylo doručeno do 10 dnů od jeho odeslání v poštovní zásilce s dodejkou, resp. do 10 dnů od jeho odeslání prostřednictvím

informačního systému datových schránek.

6. Strany se dohodly, že po ukončení smlouvy trvají a zůstávají v platnosti ujednání stran týkající se odpovědnosti za vady, záruk za jakost a záruční lhůty, smluvních pokut, náhrady škody a cenová ujednání obsažená v této smlouvě.
7. Bez ohledu na způsob ukončení smlouvy je Poskytovatel povinen minimálně pět dnů před ukončením smlouvy předat Zadavateli Návrh Protokolu o ukončení projektu zhotovený Poskytovatelem. Součástí tohoto protokolu bude dále aktuální provozní dokumentace, informace potřebné k provozu a správě systému, evidence incidentů předaných prostřednictvím HelpDesku Zadavatele, podpora pracovníků Zadavatele či nového poskytovatele služby po převzetí provozu a správy systému. Za účelem snazšího předání a převzetí služby se Poskytovatel dle této smlouvy rovněž v minimální lhůtě 14 dnů před ukončením služby zavazuje zpřístupnit novému budoucímu poskytovateli (či pověřené osobě zadavatele) nezbytné informace systému jako i zpřístupnit stávající informace k charakteru poskytované služby (v režimu „pro čtení“).

XIII.

Sankce, nárok na slevu při nedodržení SLA služby

1. Pro případ, že Poskytovatel nezačne plnění dle této smlouvy řádně, ve sjednaném rozsahu a v termínu dle čl. IV odst. 1 smlouvy, zavazuje se Zadavateli zaplatit smluvní pokutu ve výši 5.000,--Kč za každý den prodlení.
2. V případě, že Poskytovatel poruší svoji povinnost pravidelného zálohování dat uvedenou v čl. V odst. 6 smlouvy, a v porušení této povinnosti setrvá o více jak 24 hodin zavazuje se Zadavateli zaplatit smluvní pokutu ve výši 50% měsíčního paušálu odpovídající ceně této služby. Právo Zadavatele na náhradu případně vzniklé škody v důsledku neprovedeného zálohování není uhrazením smluvní pokuty dotčeno.
3. Nebude-li Poskytovatel zadavateli poskytovat pravidelný reporting anebo udržovat v aktuálním stavu potřebnou dokumentaci spojenou s plněním podle této smlouvy, nebo nebude-li poskytovat Zadavateli informace a dokumenty tak, jak je specifikováno v jednotlivých SLA, a další operativní informace, které jsou nezbytné pro plnění předmětu této Smlouvy, je povinen Zadavateli zaplatit smluvní pokutu ve výši 5% či 10% (dle char. služby dle SLA) z ceny měsíčního paušálu služby, ke které měla být služba reportingu či údržby poskytnuta.
4. Neposkytne-li Poskytovatel Zadavateli nezbytnou součinnost při realizaci úprav daných platnou legislativou a legislativními změnami či při realizaci nařízení centrálních úřadů a Magistrátu hlavního města Prahy, zavazuje se Zadavateli uhradit smluvní pokutu ve výši 2.000,--Kč za každý den prodlení.
5. Pro případ, že Poskytovatel nezačne řešit nahlášený incident ve stanové lhůtě (resp. ve stanovené lhůtě nebude informace o přijetí nahlášeného incidentu poskytovatelem potvrzena v Helpdesku Zadavatele), zavazuje se Zadavateli uhradit smluvní pokutu 1% z ceny měsíčního paušálu příslušného k dané službě.
6. Pro případ, že Poskytovatel ve stanovených lhůtách od nahlášení incidentu nevyřeší nahlášený incident, zavazuje se Zadavateli uhradit smluvní pokutu ve výši 1.000,--Kč za každou hodinu prodlení v případě kritického incidentu, resp. 500,--Kč za každou hodinu prodlení v případě ostatních incidentů.
7. Poruší-li Poskytovatel kteroukoli povinnost mlčenlivosti uvedenou čl. IX. odst. 1 až čl. IX. odst. 4 smlouvy, zavazuje se Zadavateli uhradit smluvní pokutu ve výši 500.000,--Kč za každý jednotlivý případ porušení povinnosti
8. V případě neplnění závazků Poskytovatele vyplývajících z této smlouvy, u kterých není výše smluvní pokuty samostatně řešena v předchozích bodech, uhradí Poskytovatel Zadavateli smluvní pokutu ve výši 2.000,- Kč za každý případ prodlení.
9. Uplatněné smluvní pokuty se nezapočítávají na náhradu škody, která Zadavateli vznikla

nedodržení ustanovení této smlouvy či platných zákonů ze strany Poskytovatele.

10. Při prodlení Zadavatele s úhradou jakékoli dlužné částky je Poskytovatel oprávněn účtovat Zadavateli úrok z prodlení v zákonné výši, stanovené nařízením vlády č. 351/2013 Sb., ve znění pozdějších předpisů.
11. Smluvní pokuty jsou splatné do 30 dnů od dne obdržení příslušného vyúčtování.
12. Pokud závazek provést dílo zanikne řádným ukončením plnění, nezaniká nárok na smluvní pokutu, která souvisí s dřívějším porušením povinností.
13. Při prodlení Poskytovatele s úhradou sankce proti sjednanému termínu úhrady je Zadavatel oprávněn účtovat úrok z prodlení ve výši 0,05% z dlužné částky za každý, i započatý den prodlení.
14. Sankci (smluvní pokutu, úrok z prodlení) vyúčtuje oprávněná strana straně povinné písemnou formou. Ve vyúčtování musí být uvedeno to ustanovení smlouvy, které k vyúčtování sankce opravňuje a způsob výpočtu celkové výše sankce.
15. Strana povinná se musí k vyúčtování sankce vyjádřit nejpozději do deseti dnů ode dne jeho obdržení, jinak se má za to, že s vyúčtováním souhlasí. Vyjádřením se v tomto případě rozumí písemné stanovisko strany povinné. Nesouhlasí-li strana povinná s vyúčtováním sankce, je povinna písemně ve sjednané lhůtě sdělit oprávněné důvody, pro které vyúčtování sankce neuznává.
16. Nebude-li Poskytovatel splňovat SLA ve výši nad 95 %, vzniká Zadavateli nárok na sankci vůči Poskytovateli ve formě slevy z měsíčního paušálu. Poskytovatel je povinen tuto sankci sám vyčíslit v rámci Návrhu akceptačního protokolu. Zadavatel si vyhrazuje právo na určení způsobu úhrady této sankce, a to včetně formy zápočtu proti kterékoliv splatné pohledávce Poskytovatele vůči Zadavateli. Odstupňovaná výše sankcí, resp. slev v závislosti na dosažené úrovni dostupnosti služeb je uvedena v následující tabulce:

Dostupnost služeb v % v daném kalendářním měsíci (Míra nedodržení SLA)	Sankce jako sleva z měsíčního paušálu
95 % – 93 %	5 % z měsíčního paušálu
92,99 % – 92 %	6 % z měsíčního paušálu
91,99 % – 90 %	10 % z měsíčního paušálu
méně než 89,99 %	20 % z měsíčního paušálu

V případě výskytu okolností zvláštního zřetele hodných v období od počátku poskytování služby do 1 měsíce je Zadavatel na návrh oprávněné osoby Zadavatele uvedené v čl. VII odst. 6 oprávněn neuplatňovat svůj nárok na slevu z měsíčního paušálu při plnění SLA pod 95%. Tato skutečnost, však neopravňuje Poskytovatele k tomu, v uvedeném období nevyvinul maximální snahu k naplnění účelu této smlouvy.

XIV.

Kontrola

1. Zadavatel je oprávněn zmocnit třetí osobu za účelem provádění průběžné kontroly plnění povinností Poskytovatele, včetně kontroly systému řízení služeb Poskytovatele formou zákaznického auditu. Poskytovatel je povinen poskytnout třetí osobě součinnost nezbytnou pro provádění kontroly.
2. Bude-li Zadavatel provádět jakýkoliv audit, atestaci nebo certifikaci, je Poskytovatel povinen poskytnout Zadavateli potřebnou součinnost a dokumentaci. Odpovědnost za atestaci dle legislativy (např. ISVS a další) nese Zadavatel. Poskytovatel je povinen poskytnout součinnost k atestaci a současně poskytovat služby v souladu s těmito parametry tak, aby Zadavatel mohl atestaci úspěšně absolvovat.

3. Poskytovatel je povinen při kontrole poskytnout na vyžádání kontrolnímu orgánu daňovou evidenci v plném rozsahu. Poskytovatel je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů.

XV.

Rozhodné právo, řešení sporů

1. Právní vztahy vyplývající z této smlouvy o dílo se řídí zákony České republiky, zejména zákonem č. 89/2012 Sb., občanským zákoníkem.
2. Smluvní strany se zavazují vyvinout maximální úsilí k smírnému odstranění a vyřešení sporů vzniklých z této smlouvy operativně, a to zejména prostřednictvím oprávněných osob nebo statutárních orgánů. První smírčí jednání se musí uskutečnit do dvou pracovních dnů, nedohodnou-li se smluvní strany jinak.
3. V případě, že spor nebude vyřešen konsensem podle předchozího odstavce, smluvní strany se dohodly řešit spor před soudem. Soudem příslušným pro všechny spory vzniklé z této smlouvy mezi Zadavatelem a Poskytovatelem je obecný soud Zadavatele, v případě právního nástupce Zadavatele nebo osoby, na niž byla převedena práva a povinnosti Zadavatele ze smlouvy obecný soud této osoby.

XVI.

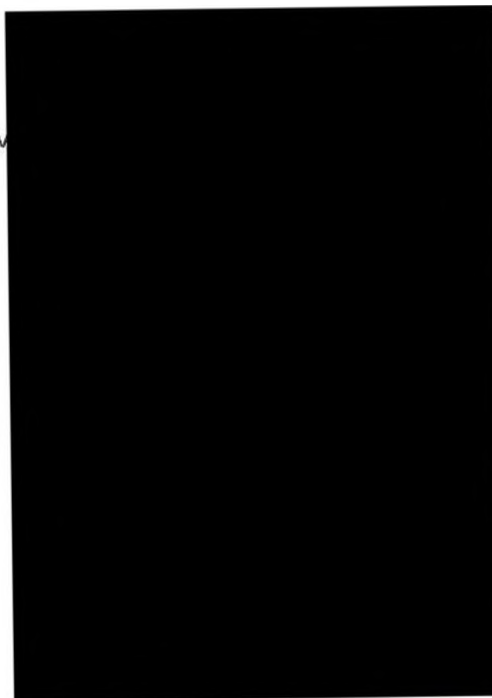
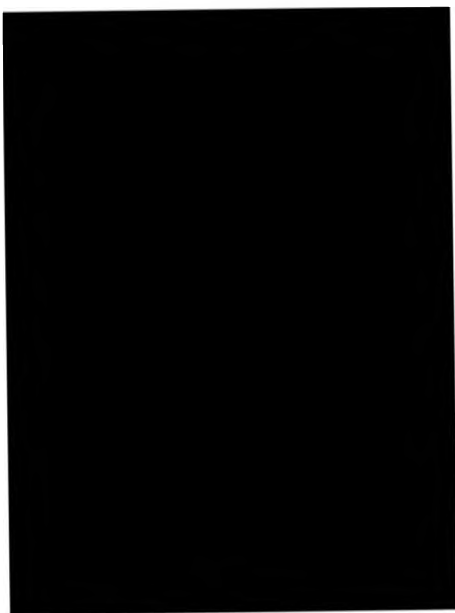
Závěrečná ustanovení

1. Poskytovatel souhlasí se zveřejněním údajů uvedených ve smlouvě v souladu se zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, jako i v souladu se zákonem č. 340/2015 Sb. o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).
2. Poskytovatel souhlasí se zveřejněním této smlouvy včetně všech příloh a případných dodatků.
3. Smluvní strany shodně prohlašují, že z důvodu přijetí nařízení EU, týkajícího se nakládání s osobními údaji, které nabude účinnosti dne 25. 5. 2018 (tzv. GDPR), uzavřou Dodatek k této smlouvě, který bude reflektovat toto nařízení GDPR.
4. Tato Smlouva nabývá platnosti v den podpisu této Smlouvy a účinnosti dnem uveřejnění v registru smluv Ministerstva vnitra ČR, v souladu se zákonem č. 340/2015 Sb. o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), včetně důsledků porušení této povinnosti. Povinnost uveřejnit smlouvu v registru smluv MV ČR náleží městské části Praha 1.
5. Smluvní strany výslovně souhlasí s tím, aby tato smlouva byla uvedena v Centrální evidenci smluv (CES) vedené Zadavatelem, která je veřejně přístupná a obsahuje údaje o smluvních stranách, předmětu Smlouvy, číselné označení této Smlouvy a datum jejího podpisu i v případné evidenci smluv Zadavatele.
6. Veškeré změny či doplnění této Smlouvy lze učinit pouze na základě písemné dohody smluvních stran. Takové dohody musí mít podobu datovaných, číslovaných a oběma smluvními stranami podepsaných dodatků Smlouvy.
7. Tato Smlouva je vyhotovena v čtyřech vyhotoveních, z nichž Zadavatel obdrží dvě vyhotovení a Poskytovatel dvě vyhotovení.
8. Tímto se osvědčuje v souladu s ustanovením § 43 zákona č. 131/2000 Sb., o hlavním městě Praze, v platném znění, že návrh na uzavření této smlouvy byl projednán a schválen Radou městské části Praha 1 dne 9.1.2018 usnesením č. UR18_0046.

Nedílnou součástí této Smlouvy jsou následující přílohy:

Číslo	Příloha
D01	Technická specifikace předmětu veřejné zakázky
D02	Popis infrastruktury ICT MČ P1
D03	Pojistná smlouva či pojistný certifikát
D04	Etalon minimální bezpečnosti pro smluvní partnery

V Praze dne 29 -01- 2018



D01 Technická specifikace předmětu veřejné zakázky
Technická specifikace předmětu veřejné zakázky

A. ÚVOD

Tato příloha popisuje základní specifikaci předmětu veřejné zakázky, kterými jsou služby správy ICT a jejich úrovně plnění, tzv. Service Level Agreement (SLA).

Poskytovatel bere na vědomí, že na datové síti provozuje svoje služby pro všechny systémy a aplikace provozované na ÚMČ P1, které jsou uvedeny v Příloze 4 této Zadávací dokumentace.

B. PROVOZNÍ HODINY ZADAVATELE

Provozní hodiny jsou pro potřeby této veřejné zakázky základem pro výpočet dostupnosti jednotlivých SLA parametrů uvedených v této příloze.

Tabulka 1: Provozní doba Zadavatele

Pondělí	8:00 - 19:00 hod.
Úterý	8:00 - 16:00 hod.
Středa	8:00 - 19:00 hod.
Čtvrtek	8:00 - 16:00 hod.
Pátek	8:00 - 14:00 hod.

C. SEZNAM PRACOVÍŠŤ ZADAVATELE:

Jungmannova 7, Praha 1
 Nové Mlýny 3a, Praha 1
 Palackého 5, Praha 1
 V jámě 12, Praha 1
 Újezd 26, Praha 1
 Žofín, Praha 1
 Jungmannova 3, Praha 1
 Karolíny Světlé 7, Praha 1
 Malostranské nám. 22, Praha 1
 Navrátilova 9, Praha 1
 Staroměstské nám. 1, Praha 1
 Vodičkova 18, Praha 1 - hlavní budova
 Vodičkova 32, Praha 1
 Vodičkova 9, Praha 1
 Štěpánská 24, Praha 1

D. ZPŮSOB VÝPOČTU DOSTUPNOSTI SLA PARAMETRŮ

Výpočet dostupnosti služby se vypočte podle následujícího vztahu:

Dostupnost jednotlivé služby v % = $((\text{Plná provozní doba} - \text{Doba nedostupnosti (DN)}) / \text{Plná provozní doba}) * 100$

U každé poskytované služby (vyjma služby S03) je minimální požadovaná dostupnost v % konkrétně definována. Pokud dojde v rámci běžného měsíce k jejímu nedodržení a současně celková dostupnost služeb klesne pod 95%, je Poskytovateli vyměřena sankce ve výši slevy z měsíčního paušálu. Výši slevy určuje tabulka Tab.2.

Poznámka: Provozní doba je časový interval shodný s úředními hodinami Zadavatele (viz tabulka Tab. 1: Úřední hodiny Zadavatele).

Podmínky poskytování služeb z pohledu řízení jakosti poskytovaných služeb:

- Doba reakce od nahlášení incidentu nesmí překročit 30 minut.
- Poskytovatel služby potvrdí příjem hlášení incidentu Zadavateli notifikací v Help Desku Zadavatele, ve kterém validuje navrženou závažnost incidentu (kritický nebo ostatní) a dle povahy incidentu oznámí, jak bude incident řešit nebo navrhne způsob jeho řešení (např. také předání k řešení třetím stranám).
- Vyhodnocování dostupnosti každé poskytované služby (podle popisu) se bude provádět měsíčně, vždy do stanoveného termínu měsíce následujícího za měsíc právě uplynulý.

- Poskytovatel služby je povinen do pěti pracovních dnů po ukončení kalendářního měsíce předávat Zadavateli detailní report pro každou poskytovanou službu a každý v jejím rámci nahlášený incident, obsahující relevantní údaje pro výpočet dostupnosti služby; relevantními údaji se rozumí zejména údaje uvedené v algoritmu výpočtu dostupnosti popsaném v tomto dokumentu.

Doba nedostupnosti (DN) se měří jako časový interval:

- od okamžiku prokazatelného nahlášení (Tnah1), a to u oprávněných požadavků na řešení závad, poskytovateli
- do okamžiku obnovení dostupnosti alespoň náhradním způsobem (Tobn) a prokazatelného předání této informace zadavateli (e-mailem nebo jiným prokazatelným způsobem).

Plánované doby odstávky (DO) předem dohodnuté se Zadavatelem se do doby nedostupnosti nezapočítávají. Plánovaná odstávka je též doba vytváření datových záloh.

Do doby nedostupnosti se rovněž nezapočítává doba, kdy je systém nedostupný z důvodu nedodržení podmínek na straně zadavatele (DNES) (např. přerušený přívod elektrického proudu, odmítnutí přístupu pracovníkům Poskytovatele k zařízením, zamezení nebo omezení vzdálené správy zařízení, nefunkčnost LAN, síť nebo internetové konektivity), nebo v důsledku vlivů mimo působnost poskytovatele (objektivní vlivy nebo důsledky činnosti zadavatele či třetích stran).

Do doby nedostupnosti se nezapočítává doba do obdržení odpovědi na upřesňující dotaz v případě, kdy incident není popsán dostatečně přesně a poskytovatel vznesl upřesňující dotaz a také doba, kdy poskytovatel čeká na součinnost zadavatele (DSOUČ).

Při výpočtu doby nedostupnosti se nebude zohledňovat počet uživatelů nedostupnosti služby dotčených.

Celkový vzorec pro výpočet nedostupnosti v konkrétní službě:

$$DN = ((Tobn_1 - Tnah_1) - DO_1 - DNES_1 - DSOUČ_1) + \dots$$

$$\dots + ((Tobn_n - Tnah_n) - DO_n - DNES_n - DSOUČ_n),$$

kde n je počet incidentů, při kterých nebyla služba dostupná.

Vypočtená celková doba nedostupnosti dané služby (DN) se vyjádří v procentech vzhledem k celkové provozní době v daném měsíci. Dále se podle následující tabulky určí sleva z měsíčního paušálu za nedodržení stoprocentní dostupnosti služby. (V tabulce je uvedena odstupňovaná výše slev v závislosti na dosažené dostupnosti.)

Tabulka 2: Slevy z měsíčního paušálu na základě dosažené dostupnosti služby

Celková dostupnost služeb v %	Sleva z měsíčního paušálu
94,99 % – 93 %	5 % z měsíčního paušálu
92,99 % – 92 %	6 % z měsíčního paušálu
91,99 % – 90 %	10 % z měsíčního paušálu
méně než 89,99 %	20 % z měsíčního paušálu

Udělování pokut za překročení parametru "Maximální doba pro řešení incidentu (v hod.)"

U každé služby je definována maximální doba pro řešení incidentu (v hodinách), a to jak pro kritický incident, tak pro incidenty ostatního typu.

Dojde-li při řešení incidentu či odstraňování závady k překročení parametru Maximální doba pro řešení incidentu, čas (zaokrouhlený nahoru na celé hodiny), o který byl parametr překročen, je zaznamenán. Poskytovateli je účtována pokuta za každou takto zaznamenanou hodinu prodlení, a to ve výši 1.000 Kč v případě kritického incidentu a ve výši 500 Kč v případě ostatních incidentů.

Stanovení celkové slevy z paušálu pro každou dílčí službu:

Z paušálu příslušného ke každé dílčí službě se v daném měsíci odečtou:

Slevy za nedosažení plné (100%) doby dostupnosti této služby (dle tabulky Tab. 2)

Pokuty vyplývající z nedodržení parametrů uvedených v této příloze.

Poznámka: Veškeré časové hodnoty v této Příloze (maximální doby pro řešení incidentů apod.) znamenají časové intervaly spadající do provozních hodin Zadavatele (viz tabulka Tab. 1: Úřední hodiny Zadavatele).

Stanovení měsíčního paušálu pro každou dílčí službu

Celkový měsíční paušál stanovený ve smlouvě s Poskytovatelem bude rozpočítán na jednotlivé služby podle následujícího rozdělení:

Tabulka 3: Rozdělení měsíčního paušálu mezi jednotlivé služby

Služba (SLA)	Poměrná část v % z celkového paušálu
S01 Provoz serverů a datových úložišť	35
S02 Provoz databázové infrastruktury	30
S03 Provoz koncových stanic, notebooků a ostatních přenosových zařízení	20
S04 Zálohování	10
S05 Tiskárny, multifunkční tisková zařízení, periferie	5
S06 Reporting, údržba dokumentace	0

Podmínky poskytování služeb z pohledu řízení jakosti poskytovaných služeb:

Doba reakce Poskytovatele na požadavek předaný z HelpDesku (tzv. Response-Time) nesmí být delší než 30 minut. Při opakovaném nedodržení (neboli překročení) tohoto časového limitu bude Poskytovateli účtována sankce ve formě slevy ve výši 5% z měsíčního paušálu příslušného k dané službě.

Veškeré informace o incidentech (= požadavky na zásah) budou Poskytovateli zaslány prostřednictvím e-mailu na určenou adresu. Nicméně Poskytovatel má povinnost sledovat HelpDesk, aby nejpozději do 30 minut mohl požadavek převzít a začít jej řešit.

Vyhodnocování dostupnosti každé poskytované služby (podle popisu) se bude provádět měsíčně, vždy do stanoveného termínu měsíce následujícího za měsíc právě uplynulý. Jelikož záznamy o incidentech jsou evidovány v HelpDesku, budou tyto údaje sloužit jakožto podklad pro výpočet celkových dob dostupnosti jednotlivých služeb a pro překročení maximálních dob pro odstranění incidentu u jednotlivých služeb.

Hlášení o incidentu na službu HelpDesk může provést každý autorizovaný uživatel Zadavatele.

V okamžiku, kdy je požadavek na zásah/řešení incidentu předán přes HelpDesk třetí straně (tj. správci dané aplikace či zařízení), končí pro Poskytovatele doba, ze které jsou mu vyčíslovány slevy za případné nesplnění Maximální doby pro řešení incidentu.

E. PARAMETRY JEDNOTLIVÝCH SLUŽEB

Služba S01 „Provoz serverů a datových úložišť“

Produkty - MS Windows, Linux

Popis služby S01

Obsahem služby je zajištění provozu a funkcionality serverů a datových úložišť pro potřeby provozu aplikací zadavatele. Poskytovatel v maximální míře musí využít stávajících prostředků Zadavatele. Součástí služby je součinnost při zajištění odborného HW servisu.

Požadované činnosti služby

01. *Serverová infrastruktura*

- a. Profylaktické činnosti (na týdenní bázi) - čištění nepotřebných souborů, defragmentace disku, kontrola místa na disku – vedení provozního deníku
- b. Správa Active Directory lokálních účtů a skupin (zakládání, rušení, přesouvání, nastavení přístupů a rolí GPO)
- c. Kontrola logů (na denní bázi)
- d. Kontrola výkonnosti a performance monitoring (na měsíční bázi).
- e. Návrh preventivních opatření s cílem předejít možným výpadkům, snížení výkonu v infrastruktuře zadavatele (minimálně kvartálně nebo dle aktuální situace).
- f. Instalace SW (instalace a konfigurace OS, ovladačů a integrace do síťového prostředí)
- g. Správa DNS pomocí softwaru ADDNET
- h. Správa Active Directory včetně podpory a správy uživatelů
- i. Správa domény Windows
- j. Správa DHCP pomocí softwaru ADDNET, případně DHCP clusteru
- k. Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobce včetně analýzy vhodnosti a potřebnosti implementace opravného balíku. Patche instaluje správce aplikace
- l. návrh opatření a postupu implementace opravného balíku ke schválení Zadavateli,
- m. provádění monitoringu provozu serverů
- n. předkládání návrhů na optimalizaci Windows infrastruktury (na kvartální bázi),
- o. instalace a provedení změn dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna 1x měsíčně),
- p. implementace schválených požadavků na změnu konfigurace OS.
- q. přístup správců pouze v provozních hodinách zadavatele. Přístup mimo provozní hodiny musí být nahlášen zadavateli
- r. Vytváření nových virtuálních serverů a součinnost při testování nových aplikací a systémů

02. *Správa diskového pole*

- a. Monitoring provozu (kontrola logů, obsazenost disků, výpadky)
- b. Změny v nastavení a konfiguraci
- c. Výkonnostní management (tvorba a analýza statistik)
- d. Správa HW (monitoring HW událostí) a systémové části zařízení
- e. Součinnost při řešení výpadků, zajištění náhradního provozu a zajištění oprav formou výměny HW s dodavatelem HW podpory
- f. Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobce (na měsíční bázi) včetně analýzy vhodnosti a potřebnosti implementace opravného balíku,
- g. návrh opatření a postupu implementace opravného balíku ke schválení Zadavateli,

03. *Řízení a správa infrastruktury pomocí systému Microsoft System Center Configuration Manager (SCCM)*

- a. Distribuce a řízení aktualizací
- b. Sestavy (collection) uživatelů a počítačů
- c. Správa systému na základě rolí
- d. Distribuce a nasazení klientů
- e. Sledování klientů a jejich nastavení
- f. Sledování instalace software a aktualizací
- g. Poskytovat sestavy dle požadavků zadavatele

04. *Vytváření a deployment OS koncových zařízení pomocí Microsoft Deployment Toolkit (WDS)*

a. Správa instalační sady pro koncová zařízení dle podkladů zadavatele

05. Správa virtualizační platformy (VMWare, Hyper-V)

- a. Správa a konfigurace stávajícího prostředí
- b. Instalace nových virtuálních strojů
- c. Správa snapshotů
- d. Kontrola logů (na denní bázi)
- e. Kontrola výkonnosti a performance monitoring (na týdenní bázi)

06. Spolupráce a součinnost s dodavateli SW aplikací (viz Příloha 4 této Zadávací dokumentace.)

Požadavky na službu:

- a. restart systému, vizuální kontrola systému na vyžádání
- b. vložení medií do požadovaných zařízení provozovaného systému
- c. správa profilů, zakládání uživatelů a skupin
- d. řízení batch-jobů
- e. umožnění dodavatelům aplikací vzdálený přístup do systému podle jejich požadavků – schvaluje MČP1
- f. povinnost dodržovat pravidla definovaná dodavatelem aplikace pro provoz systému
- g. povinnost spolupracovat při objasňování případných problémů v provozu aplikace v maximálním rozsahu 1 člověkodne za kalendářní měsíc
- h. Součinnost při podpoře provozu aplikací.
- i. Součinnost s dodavatelem poskytovaných služeb Zadavateli (např. připojení k Internetu)

07. Realizace přemístění techniky v rámci prostor Zadavatele.

08. Součinnost s ostatními dodavateli Zadavatele.

09. Spolupráce se zadavatelem při strategii rozvoje,

10. Součinnost v rámci procesů „Projektového řízení“ souvisejících s návrhem změn v infrastruktuře (společně s dodavateli technologií).

11. Správa a aktualizace provozní dokumentace

vedení provozního deníku (dokumentace všech činností), měsíční report obsazenosti diskových polí, apod.

12. Účast na jednání provozních a pracovních týmů Zadavatele (4x měsíčně)

Dostupnost služby a podpora uživatelů (% za měsíc)

95 % pro virtuální i fyzické servery

Řešení incidentů

Doba řešení incidentu = počítá se provozní doba Zadavatele

Kritický incident*	do 4 hodin od nahlášení
Omezující incident*	do 14 hodin od nahlášení
Ostatní incidenty*	do 24 hodin od nahlášení

*) Kritický incident - do 4 hodin od nahlášení (v Helpdesku priorita „kritická“ a „vysoká“) stav, kdy služba nebo systém zadavatele, ke kterým se poskytovaná služba vztahuje, není použitelná ve svých základních a klíčových funkcích a současně zásadním způsobem ohrožuje běžný provoz zadavatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody

*) Omezující incident – do 14 hodin od nahlášení (v Helpdesku priorita „střední“) stav, kdy služba nebo systém zadavatele, ke kterým se poskytovaná služba vztahuje, je plně funkční, ale vyžaduje nestandardní přístupy a postupy, které pracovníky obtěžují a omezují v jejich činnostech.

*) Ostatní incidenty - do 24 hodin od nahlášení (v Helpdesku priorita „nízká“) stav, kdy služba nebo systém zadavatele, ke kterým se poskytovaná služba vztahuje, je plně funkční, nebrání práci uživatele, ale vyžaduje např. instalaci nové služby, apod.

Plánované výpadky

Pravidelná profylaxe fyzických serverů bude prováděna každý čtvrtek 16:00 – 19:00 dle předem stanoveného a Zadavatelem schváleného plánu.

Mimo plánované výpadky je možno provést další výpadky služeb pouze se souhlasem odpovědného zástupce Zadavatele.

Omezení služby

Opravy HW budou vyjmuty z výpočtu dostupnosti SLA.

Náhrada a výměna HW nebo jen komponent HW se provádí ze skladu zadavatele. Podpora HW není součástí služby. Potřebné opravy HW ve specializovaných servisních centrech se budou řešit ve spolupráci se Zadavatelem a na náklady Zadavatele

Pro součinnost a spolupráci s dodavateli kritických aplikací platí následující:

Pokud poskytovatel zjistí závadu HW či nefunkčnost nějaké aplikace, začne neprodleně pracovat na jejím odstranění. Současně s tím vyrozumí o vzniklé situaci správce dané aplikace (v roli tzv. třetí strany). V případě potřeby poskytne součinnost k odstranění závady.



Služba S02 „Provoz databázové infrastruktury“

Produkty - MS SQL, Oracle

Popis služby S02

Obsahem služby je zajištění provozu a funkcionality databázové vrstvy infrastruktury

Požadované činnosti služby

01. Instalace a konfigurace

- a. instalace a konfigurace Automating Storage Management (ASM)
- b. instalace a konfigurace databázového Oracle SW
- c. instalace a konfigurace nových databází
- d. konfigurace parametrů databázových instancí
- e. konfigurace Oracle Net
- f. instalace Oracle klientů

02. Zálohování a obnova

- a. návrh zálohovací strategie
- b. zálohování databází pomocí nástroje Recovery Manager (RMAN)
- c. obnova databází po havárii
- d. export a import databází
- e. pravidelná obnova provozních databází na testovacím serveru

03. Správa a monitoring databázových prostředí

- a. návrh, správa a optimalizace databázové architektury
- b. správa uživatelských databázových schémat
- c. správa přístupových práv
- d. konfigurace monitoringu databázových prostředí
- e. kontrola databázových logů
- f. kontrola chodu databázových instancí a monitoring jejich zatížení
- g. ladění výkonu databázových instancí
- h. vytváření a správa dokumentace

04. Správa clusterového řešení

- a. správa Oracle Clusterware
- b. správa OCR a voting disků
- c. monitoring a správa RAC
- d. kontrola cluster ready services a cluster synchronization services
- e. správa ASM

05. Správa jednotlivých databází

- a. Správa uživatelských účtů
- b. Zabezpečování spolehlivého a bezpečného chodu databázových systémů
- c. Monitorování tabulkových prostorů
- d. Analýza zámků u problematických SQL dotazů
- e. Správa instancí a databází v RAC
- f. Kontrola a správa SQL Net
- g. Kontrola běhu databázových procesů
- h. Monitoring a správa alokace paměti v SGA
- i. Dohled nad diskovými ASM grupami
- j. Kontrola databázových instancí pomocí nativních pohledů Oracle
- k. Kontrola audit files, ASM a alert logů, disků, zatížení (top), vyčištění starých listener a OEM logů
- l. Vyhledání nejzatíženějších sql dotazů a jejich optimalizace
- m. Profylaxe databází
- n. Součinnost s aplikačními dodavateli
- o. Řešení specifických uživatelských požadavků
- p. Aktualizace dokumentace

06. Aktualizace, řešení problémů

- a. stahování a aplikace patchů (opravných záplat) dle potřeby
- b. občerstvení testovacích databází

- c. řešení problémů vzniklých při provozu databázových instancí
- d. zakládání service request (SR) v rámci podpory Oracle - My Oracle Support
- e. součinnost DBA při instalaci aplikací
- f. konzultační činnost ve vztahu ke správě a rozvoji databázového prostředí

- 07. *Součinnost s ostatními dodavateli Zadavatele.*
- 08. *Spolupráce se zadavatelem při strategii rozvoje,*
- 09. *Součinnost v rámci procesů „Projektového řízení“ souvisejících s návrhem změn v infrastruktuře (společně s dodavateli technologií).*
- 10. *Správa a aktualizace provozní dokumentace*
- 11. *Účast na jednání provozních a pracovních týmů Zadavatele (2x měsíčně)*

Dostupnost služby a podpora uživatelů (% za měsíc)
95 % pro databáze

Řešení incidentů
Doba řešení incidentu = počítá se provozní doba Zadavatele

Kritický incident*	do 4 hodin od nahlášení
Omezující incident*	do 14 hodin od nahlášení
Ostatní incidenty*	do 24 hodin od nahlášení

*) Kritický incident - do 4 hodin od nahlášení (v Helpdesku priorita „kritická“ a „vysoká“) stav, kdy služba nebo systém zadavatele, ke kterým se poskytovaná služba vztahuje, není použitelná ve svých základních a klíčových funkcích a současně zásadním způsobem ohrožuje běžný provoz zadavatele v jeho klíčových procesech a aktivitách, případně způsobuje větší finanční nebo jiné kritické škody

*) Omezující incident – do 14 hodin od nahlášení (v Helpdesku priorita „střední“), stav, kdy služba nebo systém zadavatele, ke kterým se poskytovaná služba vztahuje, je plně funkční, ale vyžaduje nestandardní přístupy a postupy, které pracovníky obtěžují a omezují v jejich činnostech.

*) Ostatní incidenty - do 24 hodin od nahlášení (v Helpdesku priorita „nízká“) stav, kdy služba nebo systém zadavatele, ke kterým se poskytovaná služba vztahuje, je plně funkční, nebrání práci uživatele, ale vyžaduje např. instalaci nové služby, apod.

Plánované výpadky
Pravidelná profylaxe fyzických serverů bude prováděna každý čtvrtek 16:00 – 19:00 dle předem stanoveného a Zadavatelem schváleného plánu.
Mimo plánované výpadky je možno provést další výpadky služeb pouze se souhlasem odpovědného zástupce Zadavatele.

Omezení služby
Pro součinnost a spolupráci s dodavateli kritických aplikací platí následující:
Pokud poskytovatel zjistí závadu HW či nefunkčnost nějaké aplikace, začne neprodleně pracovat na jejím odstranění. Současně s tím vyrozumí o vzniklé situaci správce dané aplikace (v roli tzv. třetí strany). V případě potřeby poskytne součinnost k odstranění závady.



Služba S03 „Provoz koncových stanic, notebooků a ostatních přenosných zařízení“

Produkty – Specifikace SW – viz tabulka

Popis služby S03

Poskytovatel zajistí správu stávajících a případně nově pořizovaných koncových stanic a NTB a to včetně všech dalších přenosných zařízení (tabletů) a mobilních telefonů, maximální počet spravovaných koncových zařízení je [redacted] (Aktuální seznam zařízení je uveden v Příloze č.4 Popis infrastruktury)

Seznam standardního SW, který bude instalován a spravován na koncových stanicích nebo notebookech, je uveden v následující tabulce. Verze jednotlivých SW budou upřesněny Zadavatelem při zahájení projektu dle platných licenčních ujednání. Podle pracovišť se liší instalované SW. V tabulce uvedený seznam je typický seznam pro typickou koncovou stanicí.

Název aplikace	Popis

Požadované činnosti služby

Obsahem služby je zajištění provozu a funkcionality všech koncových stanic (počítačů), notebooků, mobilních telefonů a ostatních přenosných zařízení (tabletů).

01. Instalace a konfigurace zařízení u všech uživatelů (nastavení přístupů k aplikacím, konfigurace tiskáren, připojení do počítačové sítě, ovladače pro externí zařízení (např. čtečka karet RŽP)
02. Instalace a správa standardních aplikací dle podkladů Zadavatele.
03. Stěhování koncových stanic a NTB v rámci prostor Zadavatele v rozsahu max 15 kusů koncových stanic měsíčně
04. Výměna a instalace nových koncových stanic a NTB v případě poruchy
05. Instalace nových zařízení, stěhování a výměna (bod 1, 3, 4) probíhá podle metodických pokynů Zadavatele – protokoly o předání a instalaci
06. Zajištění potřebných aktualizací „standardního SW“ ve spolupráci se Zadavatelem viz tabulka výše
07. Správa uživatelských účtů
08. Provedení změn v nastavení koncové stanice a její konfiguraci, v případě potřeby zajištění kompletní zálohy zařízení
09. Součinnost při řešení výpadků zařízení, zajištění náhradního zařízení, upgrade a opravy formou výměny HW komponent nebo HW se provádí ze skladu Zadavatele,
10. Opravy HW ve specializovaných servisních centrech se budou řešit ve spolupráci se Zadavatelem a na náklady Zadavatele
11. Nastavení podporovaných služeb na mobilní telefony (např. antivirová ochrana, pošta, úkoly, kalendář včetně synchronizace, připojení na wifi síť, speciální nastavování iPhone apod.)
 - a. základní nastavení mobilu (jas, zabezpečení...)
 - b. instalace externích aplikací
 - c. pomoc při vytváření/obnovení googlu účtu
12. Součinnost s ostatními dodavateli Zadavatele.
13. Spolupráce se zadavatelem při strategii rozvoje,
14. Součinnost v rámci procesů „Projektového řízení“ souvisejících s návrhem změn v infrastruktuře (společně s dodavateli technologií).
15. Správa a aktualizace provozní dokumentace
16. Účast na jednání provozních a pracovních týmů Zadavatele (4x měsíčně)

Dostupnost služby a podpora uživatelů (% za měsíc)
95 % pro databáze

Řešení incidentů

Doba řešení incidentu = počítá se provozní doba Zadavatele

Poznámka: Důležité je v okamžiku reakce správně určit závažnost nalezeného incidentu (= míru jeho kritičnosti) a s odpovídající naléhavostí jej předat k dalšímu řešení.

Kritický incident* do 2 hodin od nahlášení
Omezující incident* do 4 hodin od nahlášení
Ostatní incidenty* do 20 hodin od nahlášení

*) Kritický incident - do 2 hodin od nahlášení (v Helpdesku priorita „kritická“) stav, kdy zařízení zadavatele není použitelné, ohrožuje běžný provoz a může způsobit větší finanční nebo jiné kritické škody. V případě incidentu vydat náhradní zařízení ze skladu - to poskytne Zadavatel. Poskytovatel bude mít do 2 hodin poté připravené funkční a provozuschopné odpovídající koncové zařízení.

Tento stav nastane, pokud jej vyhodnotí služba na HelpDesku jako velmi důležitý pro klíčové zaměstnance úřadu.

*) Omezující incident – do 4 hodin od nahlášení (v Helpdesku priorita „vysoká“), stav, kdy zařízení zadavatele, je plně funkční, ale vyžaduje nestandardní přístupy a postupy, které pracovníky obtěžují a omezují v jejich činnostech.

*) Ostatní incidenty - do 20 hodin od nahlášení (v Helpdesku priorita „střední“ a „nízká“) stav, kdy zařízení zadavatele, je plně funkční, nebrání práci uživatele, ale vyžaduje např. instalaci nové služby, apod.

Plánované výpadky

Případná profylaxe jednotlivých pracovních stanic, notebooků a přenosných zařízení je možná pouze dle předem stanoveného a Zadavatelem schváleného plánu.

Omezení služby

Celkový upgrade či obměna koncových stanic není součástí služby podpory.



Služba S04 „Zálohování“

Produkty – IBM Tivoli storage manager

Popis služby S04

Obsahem služby je zajištění zálohování serverů a aplikací určených Zadavatelem. Záloha se provádí na média určená a předaná Zadavatelem a jejich bezpečné uložení dle požadavků Zadavatele.

Požadované činnosti služby

1. Pravidelné zálohování každý pracovní den po ukončení úředních hodin.
2. Pravidelná kontrola výsledků zálohování. Zaslání reportu s popisem výsledků provedeného zálohování Zadavateli každý den ráno na vybraný email.
3. Správa zálohovacího systému IBM TSM dle aktuálního zálohovacího plánu vytvořeného Poskytovatelem a schváleného Zadavatelem.
4. Záloha musí umožnit obnovit data 30 dní zpětně
5. Pravidelná profylaxe, kontrola čitelnosti dat včetně testování obnovy systémů a dat ze záloh (nejméně 1x za 3 měsíce), vytvoření protokolu o provedené profylaxi
6. Provádění záloh/obnov/archivace serverů agendových i ekonomických, dalších serverů a počítačů podle požadavků Zadavatele, včetně nových serverů, které mohou být doplněny v době trvání smlouvy
7. Zajištění spouštění čistící pásky a kontrola stavu pásek a případné informování o nutnosti dokoupit další pásky
8. Spolupráce na řešení zjištěných nedostatků (např. síťová infrastruktura, duplicita zálohovaných dat)
9. Součinnost s ostatními dodavateli Zadavatele.
10. Spolupráce se zadavatelem při strategii rozvoje,
11. Součinnost v rámci procesů „Projektového řízení“ souvisejících s návrhem změn v infrastruktuře (společně s dodavateli technologií).
12. Správa a aktualizace provozní dokumentace
13. Účast na jednání provozních a pracovních týmů Zadavatele (2x měsíčně)

Dostupnost služby a podpora uživatelů (% za měsíc)

Dostupnost služby nebude v tomto případě určována, případné nedostatky v dodávání budou řešeny jednorázovou pokutou za neprovedení služby

Řešení incidentů

Doba řešení incidentu = počítá se provozní doba Zadavatele

8 hodin pro odstranění incidentu – neproběhla záloha. V případě příchodu další – v pořadí již druhé - zprávy (reportu) o neprovedení zálohování (tj. další den ráno) - neboli zálohování se neprovedlo 2 dny po sobě - bude směrem na Poskytovatele uplatněna jednorázová pokuta a to ve výši 50% paušálu příslušejícího této službě.

Pokud bude při ranní kontrole zjištěno, že zálohování neproběhlo, potom Poskytovatel provede „náhradní“ zálohování – to ovšem pouze za okolností, pokud mu to umožní momentální denní provoz Informačních systémů.

Plánovaná profylaxe

Pravidelná profylaxe pouze dle schváleného plánu Zadavatelem.

Ukončení procesu zálohování bude vždy nejpozději do 7. hodiny ranní.

Omezení služby

Zadavatel poskytne dostatečné množství zálohovacích medií.



Služba S05 „Tiskárny, multifunkční tisková zařízení, periferie“

Popis služby S05

Poskytovatel zajistí správu tiskáren, multifunkčních tiskáren a periférií uvedených v Příloze č.4 Popis infrastruktury

Požadované činnosti služby

1. Instalace a konfigurace v rozsahu maximálně 15 ks za měsíc (T, S, MF).
2. HW a SW správa, řešení výpadků a zajištění upgrade a nastavení zařízení (T, MF, S)
3. Doplnění tonerů (T, MF, CVS) podle metodického pokynu Zadavatele
4. Doplnění spotřebního materiálu do vyvolávacího systému v sídle úřadu
5. Realizace přemístění techniky (T, MF, S) v rámci prostoru Zadavatele
6. Předání Zadavatelí popisů (návodů), jak nainstalovat dané zařízení do prostředí úřadu MČP1, a to v editovatelném stavu, udržování těchto návodů v aktuálním stavu.

T - tiskárny

MF - multifunkce

S - štítkové tiskárny

CVS - tiskárny centrálního vyvolávacího systému

Dostupnost služby a podpora uživatelů (% za měsíc)

75 %

Řešení incidentů

Doba řešení incidentu = počítá se provozní doba Zadavatele

Provedení servisního zásahu včetně eventuální výměny vadného zařízení pro malé tiskárny, skenery a multifunkční tisková zařízení: do 4 hodin.

Výměnou se rozumí náhrada nefunkčního zařízení za funkční zařízení od zadavatele ze skladu zadavatele v prostorách Vodičkova 18, Praha 1.

Kritický incident* do 2 hodin od nahlášení

Omezující incident* do 4 hodin od nahlášení

Ostatní incidenty* do 20 hodin od nahlášení

*) Kritický incident - do 2 hodin od nahlášení (v Helpdesku priorita „kritická“) stav, který vyhodnotí služba na HelpDesku jako velmi důležitý pro klíčové zaměstnance úřadu.

*) Omezující incident – do 4 hodin od nahlášení (v Helpdesku priorita „vysoká“), stav, kdy zařízení je funkční, ale vyžaduje nestandardní přístupy a postupy, které pracovníky obtěžují a omezují v jejich činnostech.

*) Ostatní incidenty - do 20 hodin od nahlášení (v Helpdesku priorita střední a „nízká“) Stav zařízení je plně funkční, nebrání práci uživatele, ale vyžaduje např. vyčištění, apod.

Omezení služby

Předmětem této služby není spotřební materiál a náklady na opravu zařízení.

Služba S06 „Reporting“

Popis služby S06

Poskytovatel v rámci této služby zajistí

1. pro každou výše uvedeno službu vytvoření reportu pro Zadavatele
2. vytvoření a údržbu nezbytné technické dokumentace – (pokud to u dané služby přichází v úvahu) v souladu s požadavky specifikovanými v dále uvedených tabulkách.

Požadované činnosti služby

A - Reporting ze služby S01 „Provoz serverů a datových úložišť a S02 „Provoz databázové infrastruktury“

Obsahem služby je vytvoření pravidelného měsíčního reportu, který obsahuje následující údaje:

- a) relevantní detailní záznamy o evidenci a řešení všech požadavků, které byly v daném období (kalendářní měsíc) na službu S01 a S02 Zadavatelem sjednaným způsobem uplatněny, se zřetelným vyznačením, zda byla dodržena stanovená doba pro odstranění všech incidentů.
- b) vypočtenou hodnotu dostupnosti poskytnuté služby za právě uplynulé sledované období (kalendářní měsíc),
- c) z detailních záznamů podle bodu a) výše: relevantní agregované časové údaje s popisem jejich obsahu, ze kterých může Zadavatel jejich pouhým dosazením do (výše publikovaného) stanoveného vzorce pro výpočet dostupnosti provést kontrolu vypočtené hodnoty dostupnosti.

Termín a forma dodání reportu

Poskytovatel služby je povinen dodat Zadavateli report ve formátu MS .xlsx do 5-ti kalendářních dnů měsíce následujícího po právě ukončeném.

Podmínky nesplnění služby

1. Nedodržení požadovaného obsahu reportu,
2. Uvedení nesprávných údajů v reportu (zejména identifikace splnění a nesplnění časových limitů pro odstranění kritických a ostatních incidentů, nesoulad deklarované hodnoty splnění vyhodnocované služby a výsledku kontrolního přepočtu Zadavatelem na základě dodaných agregovaných dílčích hodnot pro výpočet dostupnosti služby),
3. nesplnění termínu a formy dodání reportu.

Sankce za nesplnění služby

V případě nesplnění služby snižuje Zadavatel Poskytovateli služby měsíční paušál příslušný k dané službě S01 a S02 o 10 %.

B - Reporting ze služby S03 „Provoz koncových stanic, notebooků a ostatních přenosných zařízení“

Obsahem služby je vytvoření pravidelného měsíčního reportu, který obsahuje následující údaje:

- a) relevantní detailní záznamy o evidenci a řešení všech požadavků, které byly v daném období (kalendářní měsíc) na službu S03 Zadavatelem sjednaným způsobem uplatněny, se zřetelným vyznačením, zda byla dodržena stanovená doba pro odstranění všech incidentů.
- b) vypočtenou hodnotu dostupnosti poskytnuté služby za právě uplynulé sledované období (kalendářní měsíc),
- c) z detailních záznamů podle bodu a) výše: relevantní agregované časové údaje s popisem jejich obsahu, ze kterých může Zadavatel jejich pouhým dosazením do (výše publikovaného) stanoveného vzorce pro výpočet dostupnosti provést kontrolu vypočtené hodnoty dostupnosti.

Termín a forma dodání reportu

Poskytovatel služby je povinen dodat Zadavateli report ve formátu MS .xlsx do 5-ti kalendářních dnů měsíce následujícího po právě ukončeném.

Podmínky nesplnění služby

1. Nedodržení požadovaného obsahu reportu,
2. Uvedení nesprávných údajů v reportu (zejména identifikace splnění a nesplnění časových limitů pro odstranění kritických a ostatních incidentů, nesoulad deklarované hodnoty splnění vyhodnocované služby a výsledku kontrolního přepočtu Zadavatelem na základě dodaných agregovaných dílčích hodnot pro výpočet dostupnosti služby),
3. nesplnění termínu a formy dodání reportu.

Sankce za nesplnění služby

V případě nesplnění služby snižuje Zadavatel Poskytovateli služby měsíční paušál příslušný k dané službě S03 o 10 %.

C - Reporting ze služby S04 „Zálohování“

Obsahem služby je:

1. Předávání reportu Poskytovateli o provedeném zálohování, který obsahuje minimálně následující údaje:
 - a) datum zálohování,
 - b) co bylo zálohováno,
 - c) relevantní identifikace zálohy,
 - d) popis výsledků provedeného zálohování,
 - e) kde je záloha uložena,
 - f) kdo je za provedení zálohování odpovědný
 - g) údaje o provedení kontroly čitelnosti zálohy a odpovědná osoba za provedení kontroly
2. Vytváření protokolu o provedené profylaxi procesu zálohování, který obsahuje relevantní údaje, zejména
 - a) datum provedení profylaxe,
 - b) co bylo předmětem profylaxe,
 - c) relevantní okolnosti profylaxe,
 - d) odpovědná osoba,
 - e) datum další profylaxe.

Termín a forma dodání reportu

Poskytovatel služby je povinen dodat Zadavateli reporty podle specifikace v popisu služby:

- Report o provedeném zálohování: každý den ráno
Forma: elektronický soubor ve formátu html, xlsx, docx, pdf stanoveném Zadavatelem
- Report o provedené profylaxi: vždy do 2 kalendářních dnů po provedené profylaxi;
Forma: elektronický soubor ve formátu html, xlsx, docx, pdf stanoveném Zadavatelem

Podmínky nesplnění služby

1. Nedodržení požadovaného obsahu reportu,
2. Uvedení nesprávných údajů v reportu
3. nesplnění termínu a formy dodání reportu.

Sankce za nesplnění služby

V případě nesplnění služby snižuje Zadavatel Poskytovateli služby měsíční paušál příslušný k dané službě S04 o 5 %.

C - Reporting ze služby S05 „Tiskárny, multifunkční tisková zařízení, periferie“

Obsahem služby je vytvoření pravidelného měsíčního reportu, který obsahuje následující údaje:

1. relevantní detailní záznamy o evidenci a řešení všech požadavků, které byly v daném období (kalendářní měsíc) na službu S05 Zadavatelem sjednaným způsobem uplatněny, se zřetelným vyznačením, zda byla dodržena stanovená doba pro odstranění incidentů
2. vypočtenou hodnotu dostupnosti poskytované služby za právě uplynulé sledované období (kalendářní měsíc),
3. z detailních záznamů podle bodu 1) výše: relevantní agregované časové údaje s popisem jejich obsahu, ze kterých může Zadavatel jejich pouhým dosazením do (výše publikovaného) stanoveného vzorce pro výpočet dostupnosti provést kontrolu vypočtené hodnoty dostupnosti.

Termín a forma dodání reportu

Poskytovatel služby je povinen dodat Zadavateli report ve formátu MS .xlsx do 5-ti kalendářních dnů měsíce následujícího po právě ukončeném.

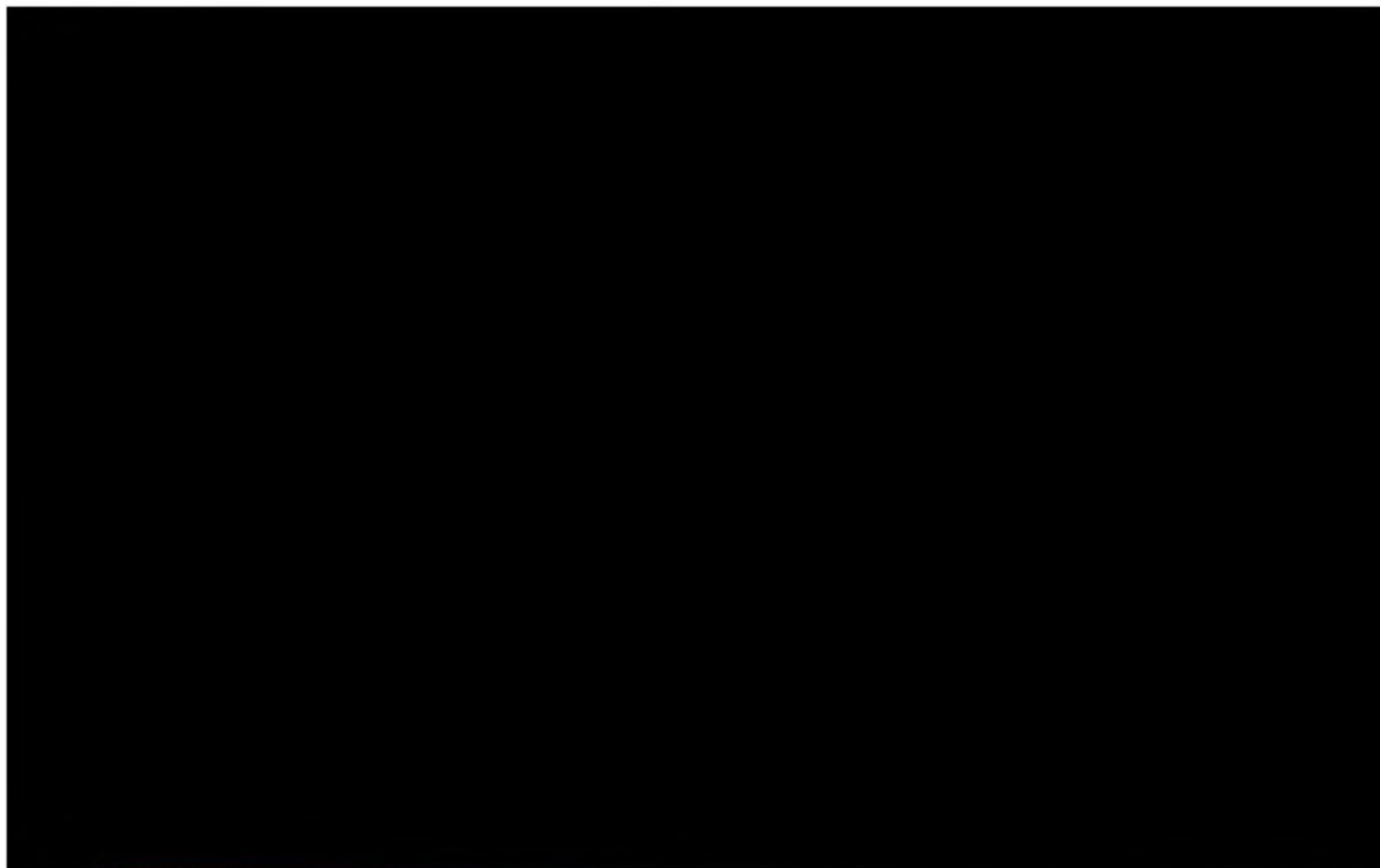
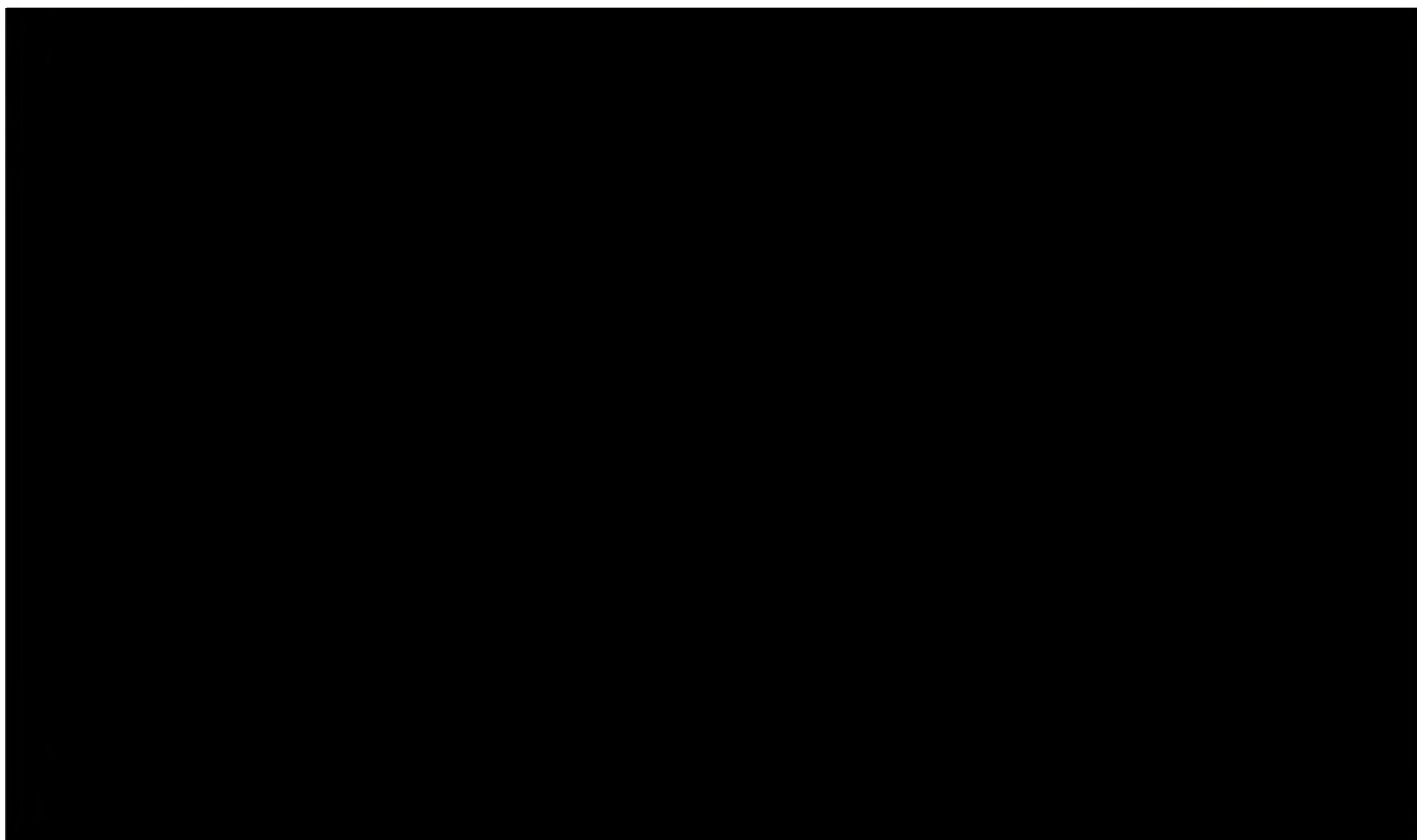
Podmínky nesplnění služby

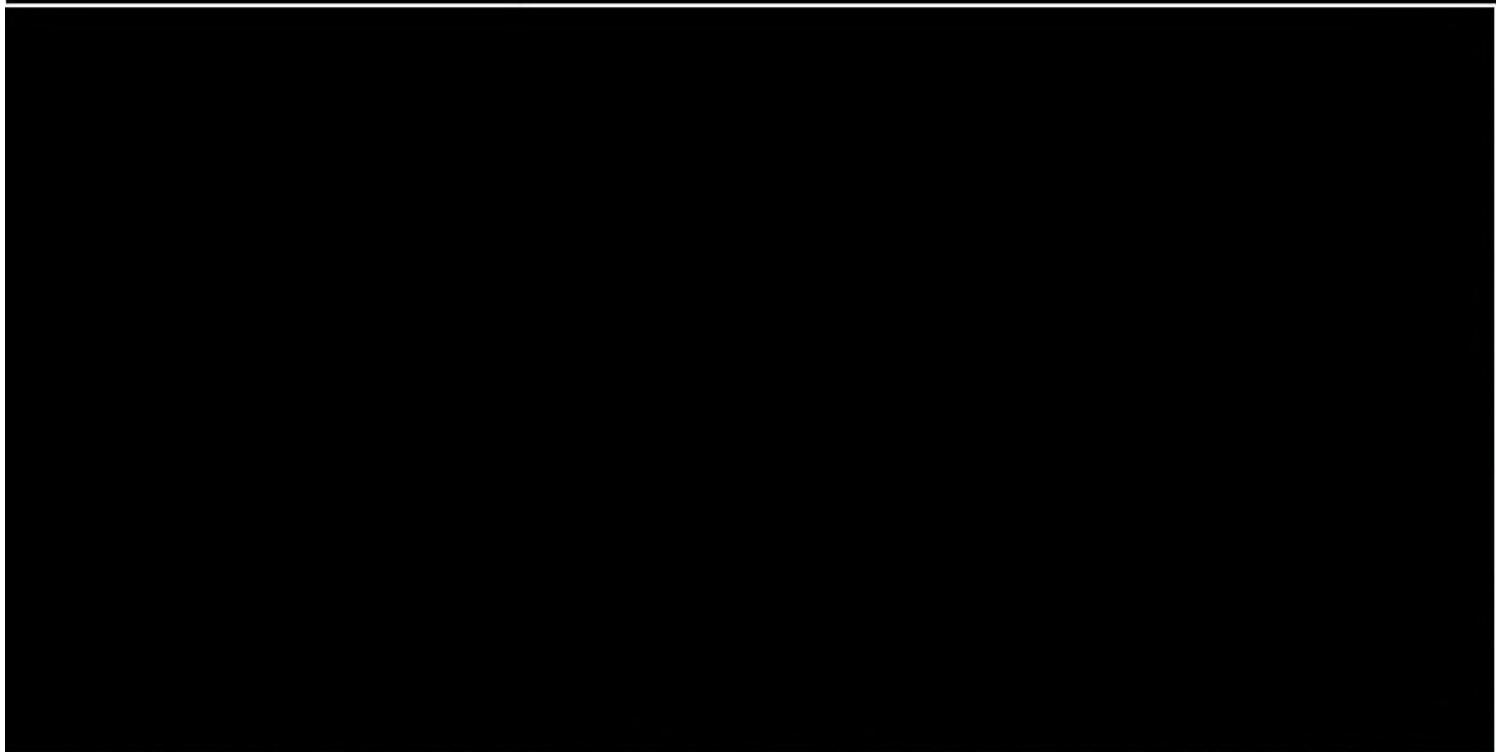
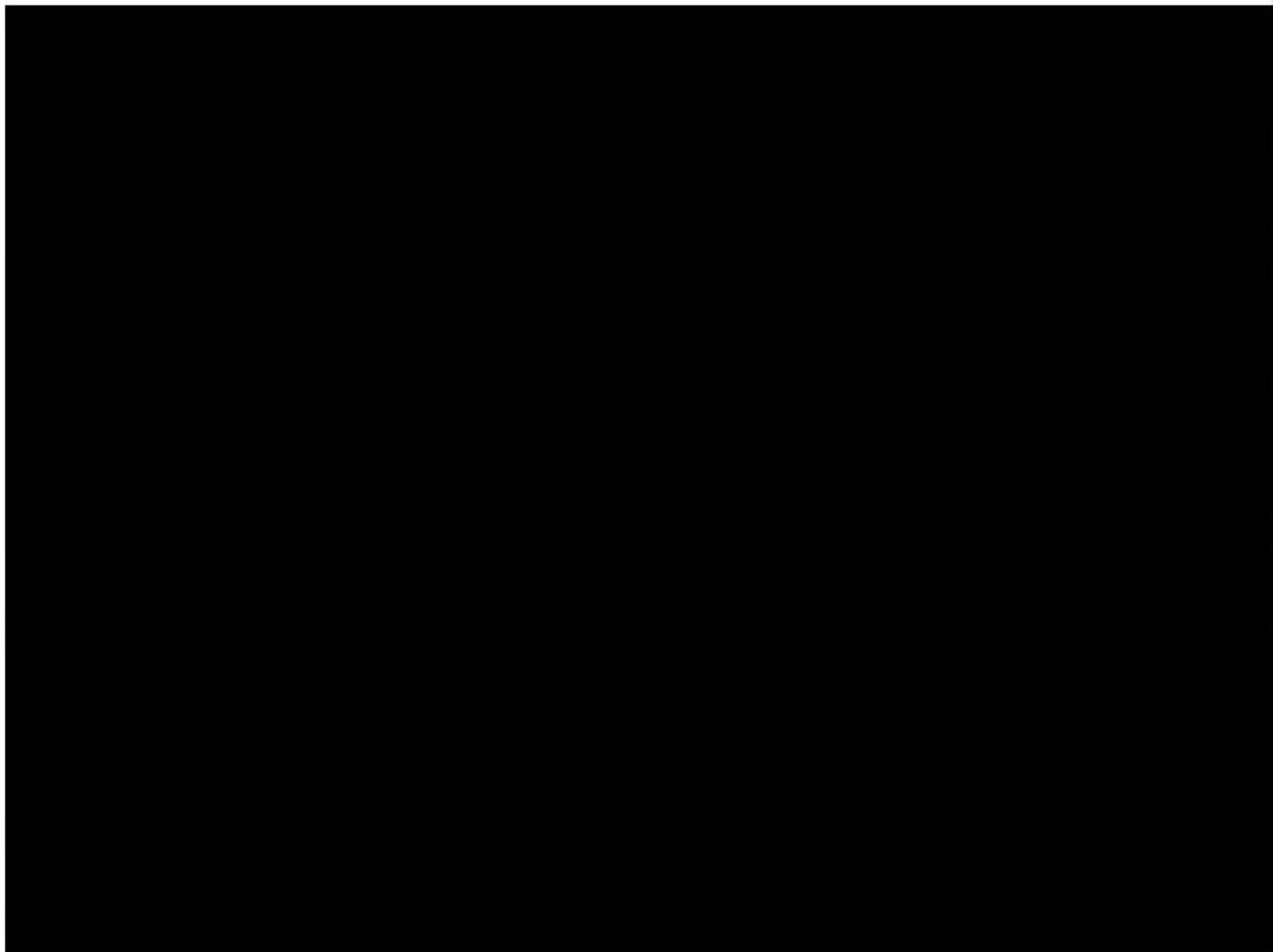
1. Nedodržení požadovaného obsahu reportu,
2. Uvedení nesprávných údajů v reportu (zejména identifikace splnění a nesplnění časových limitů pro odstranění kritických a ostatních incidentů, nesoulad deklarované hodnoty splnění vyhodnocované služby a výsledku kontrolního přepočtu Zadavatelem na základě dodaných agregovaných dílčích hodnot pro výpočet dostupnosti služby),
3. nesplnění termínu a formy dodání reportu.

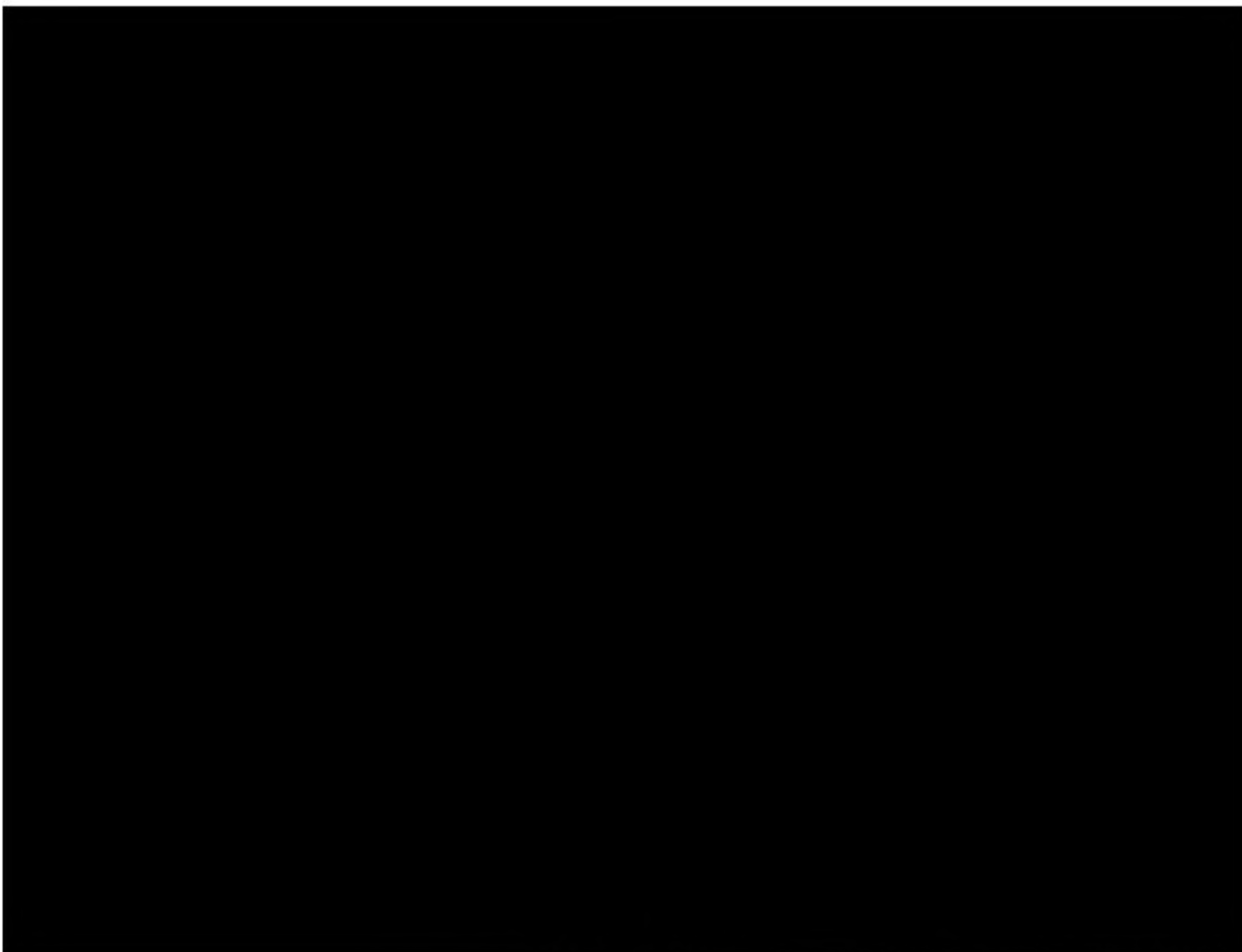
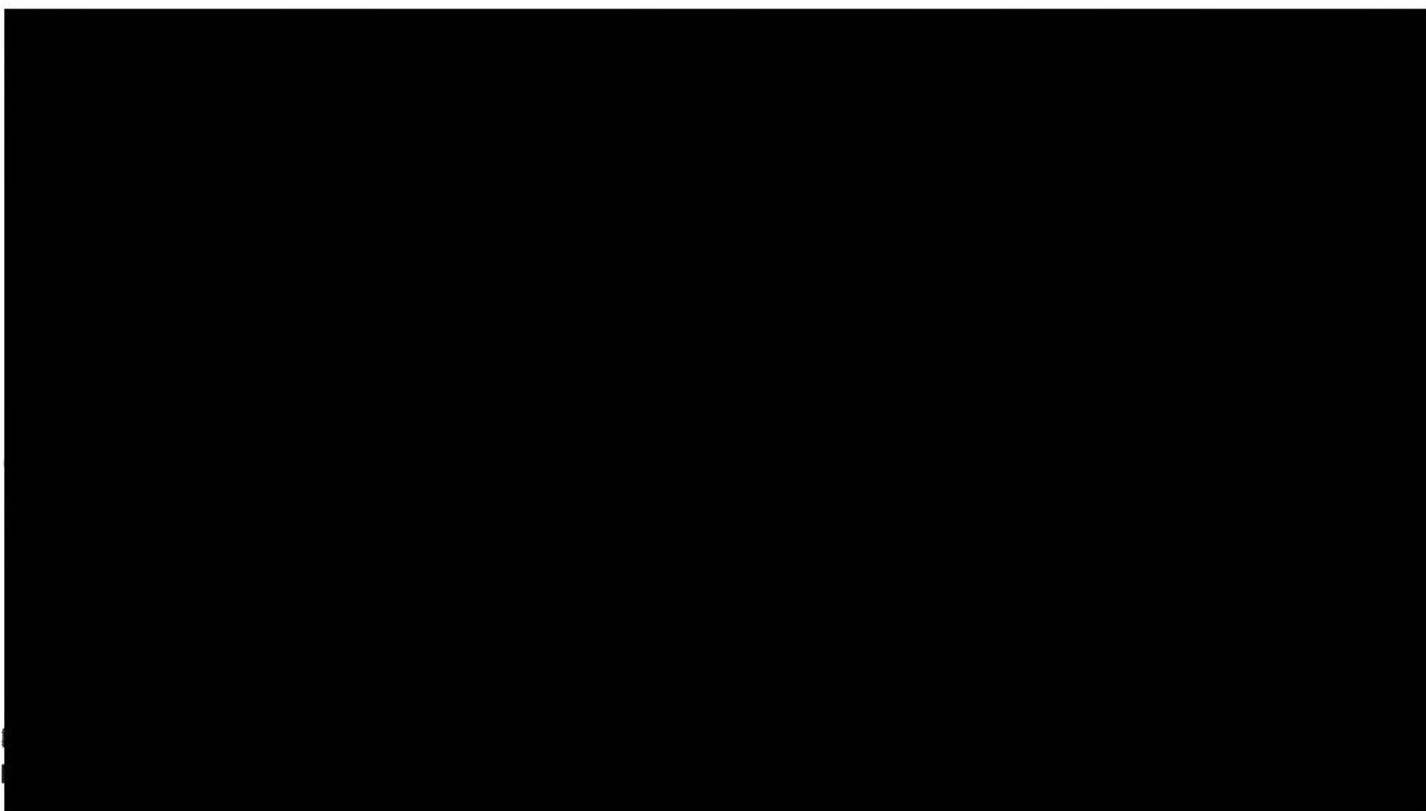
Sankce za nesplnění služby

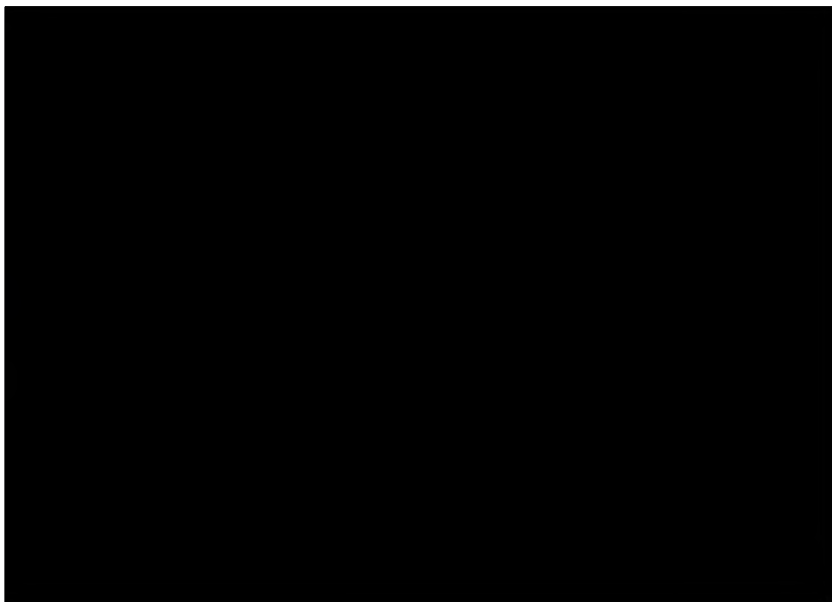
V případě nesplnění služby snižuje Zadavatel Poskytovateli služby měsíční paušál příslušný k dané službě S05 o 5 %.

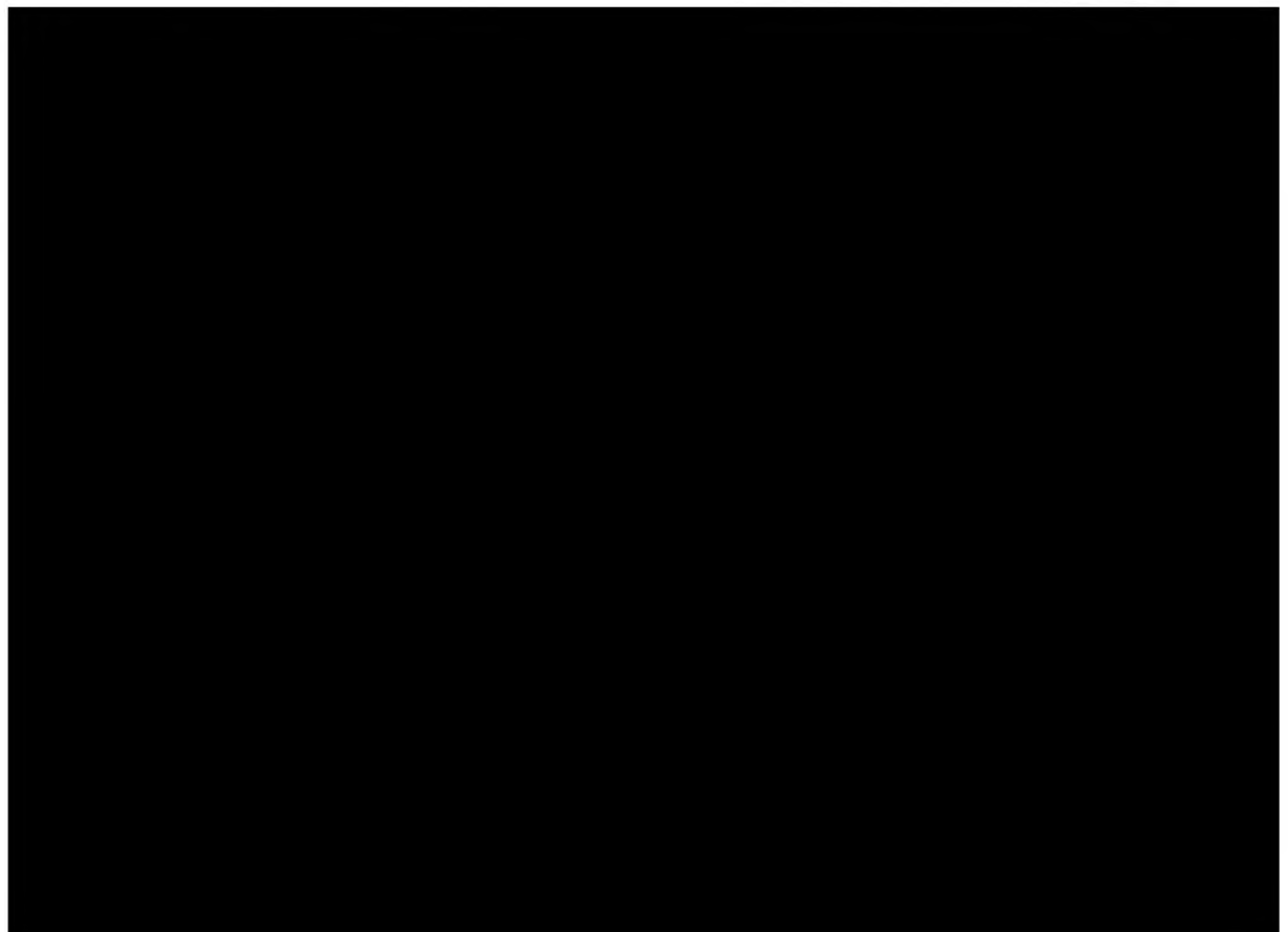
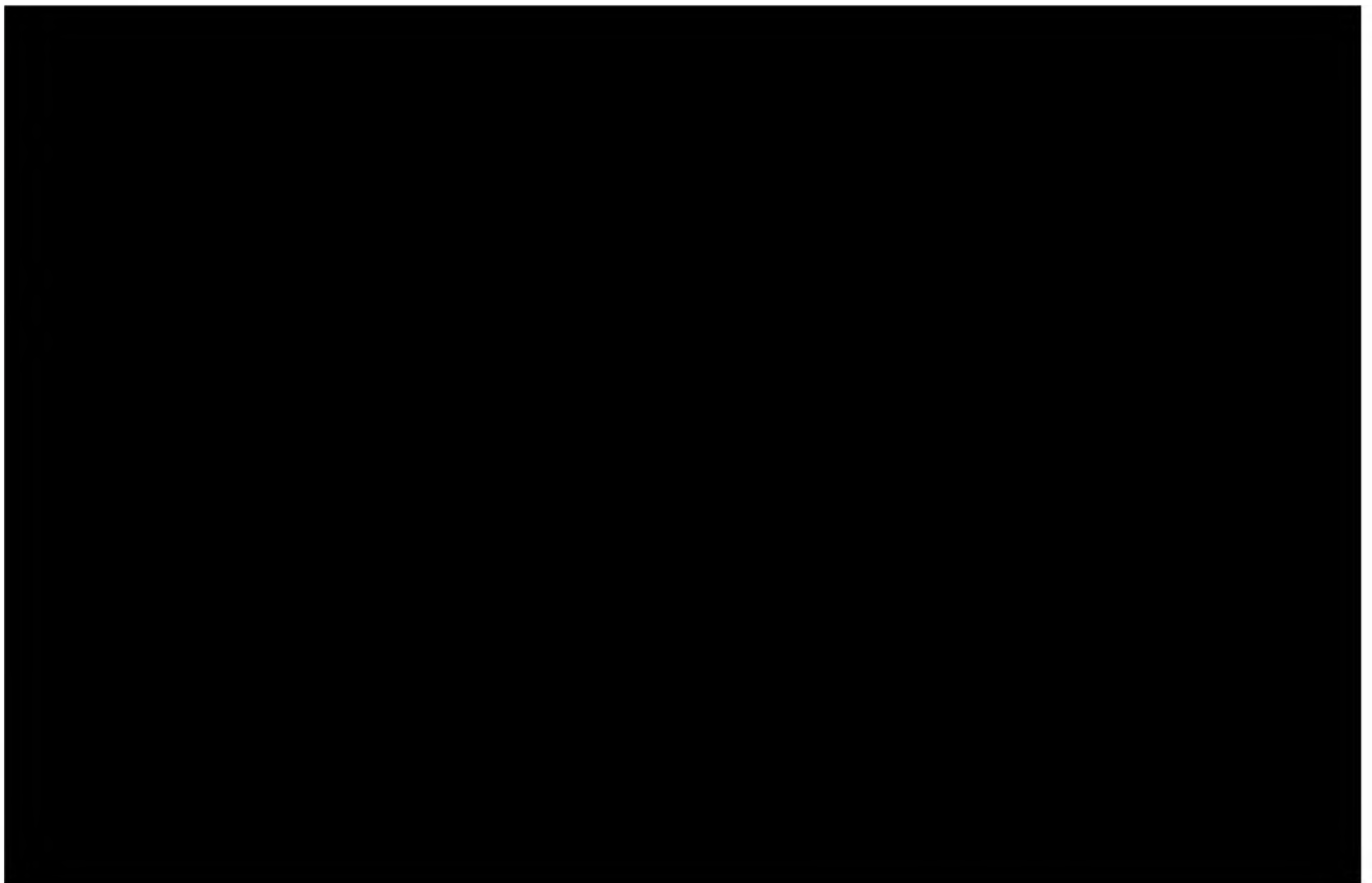
D02 Popis infrastruktury ICT MČ P1

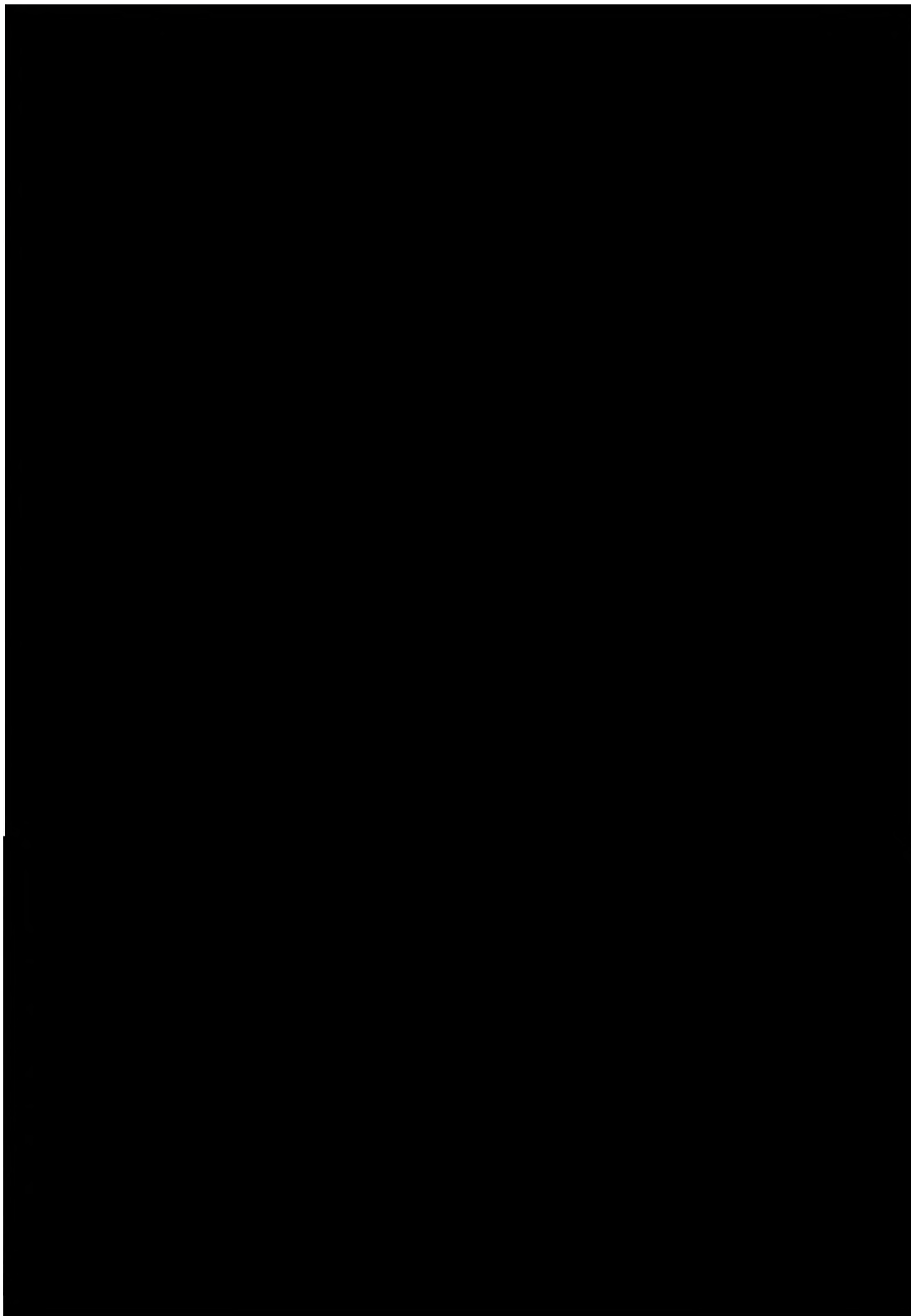


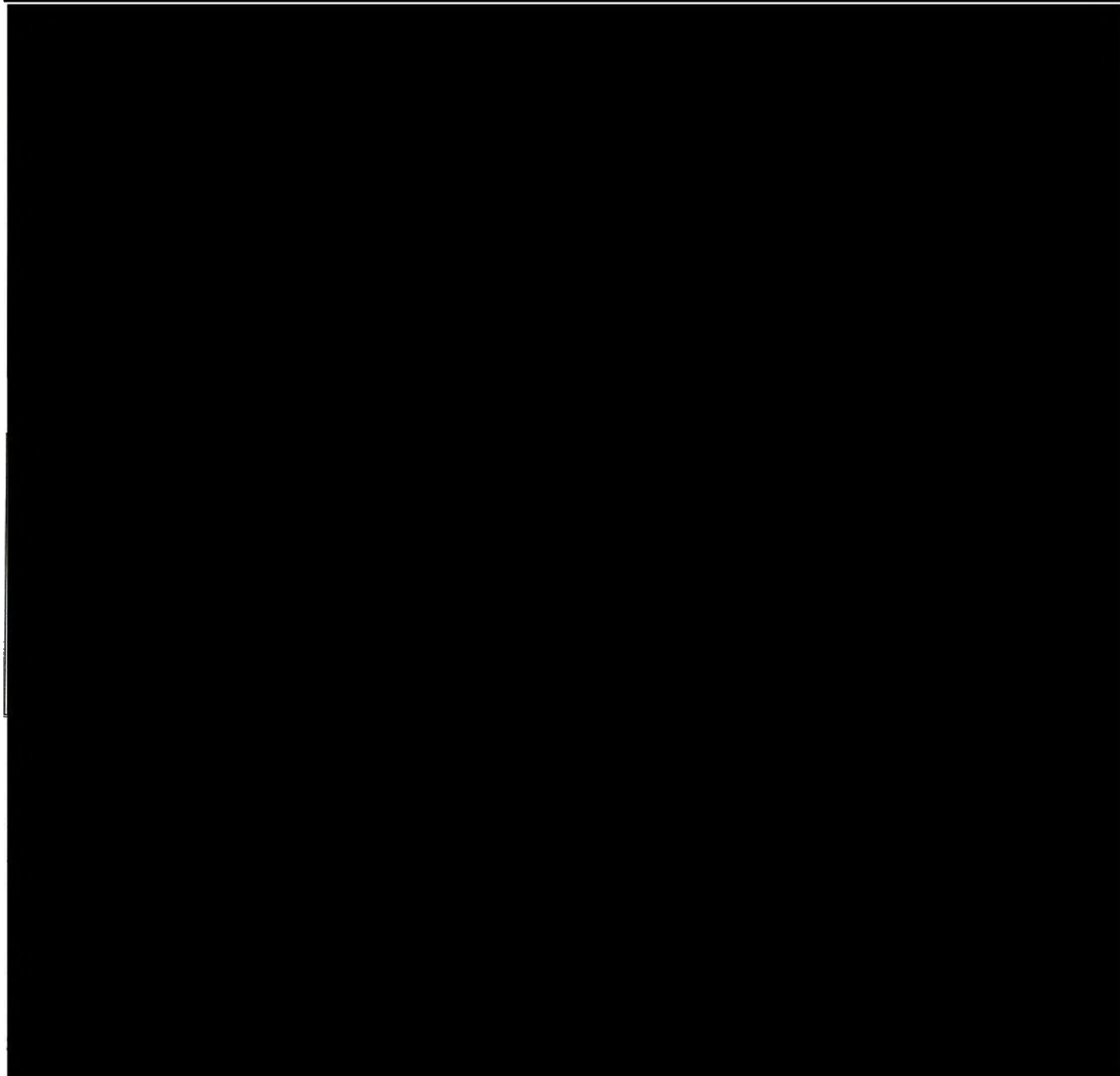
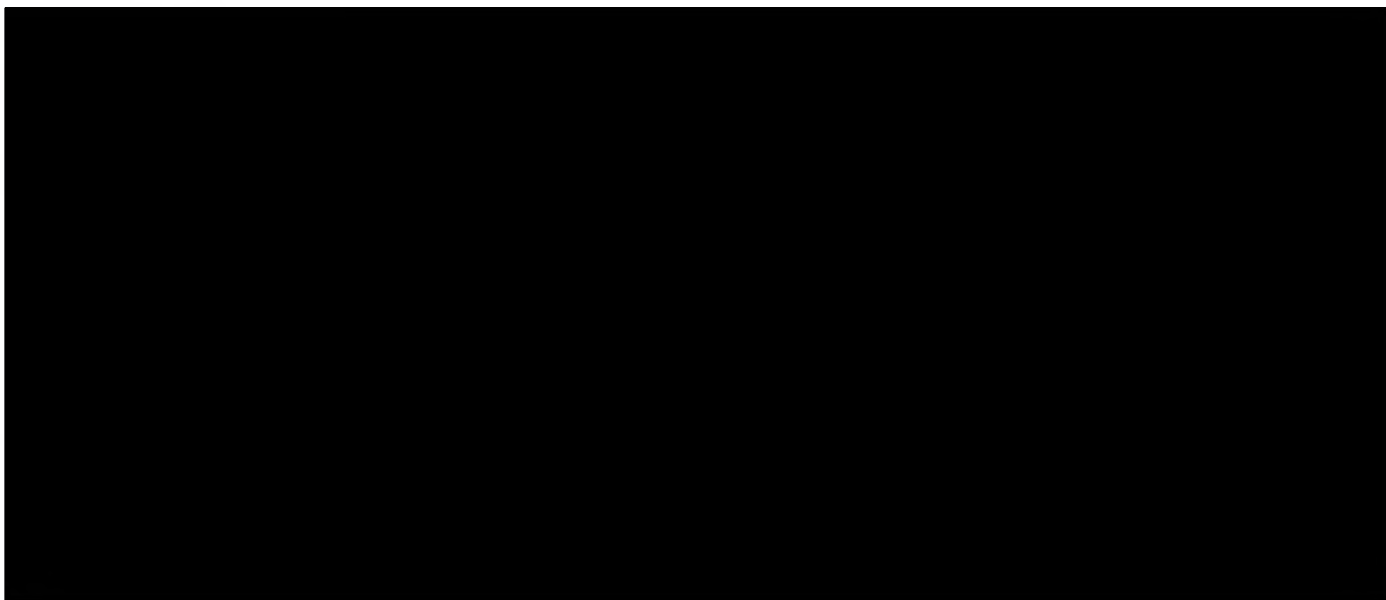


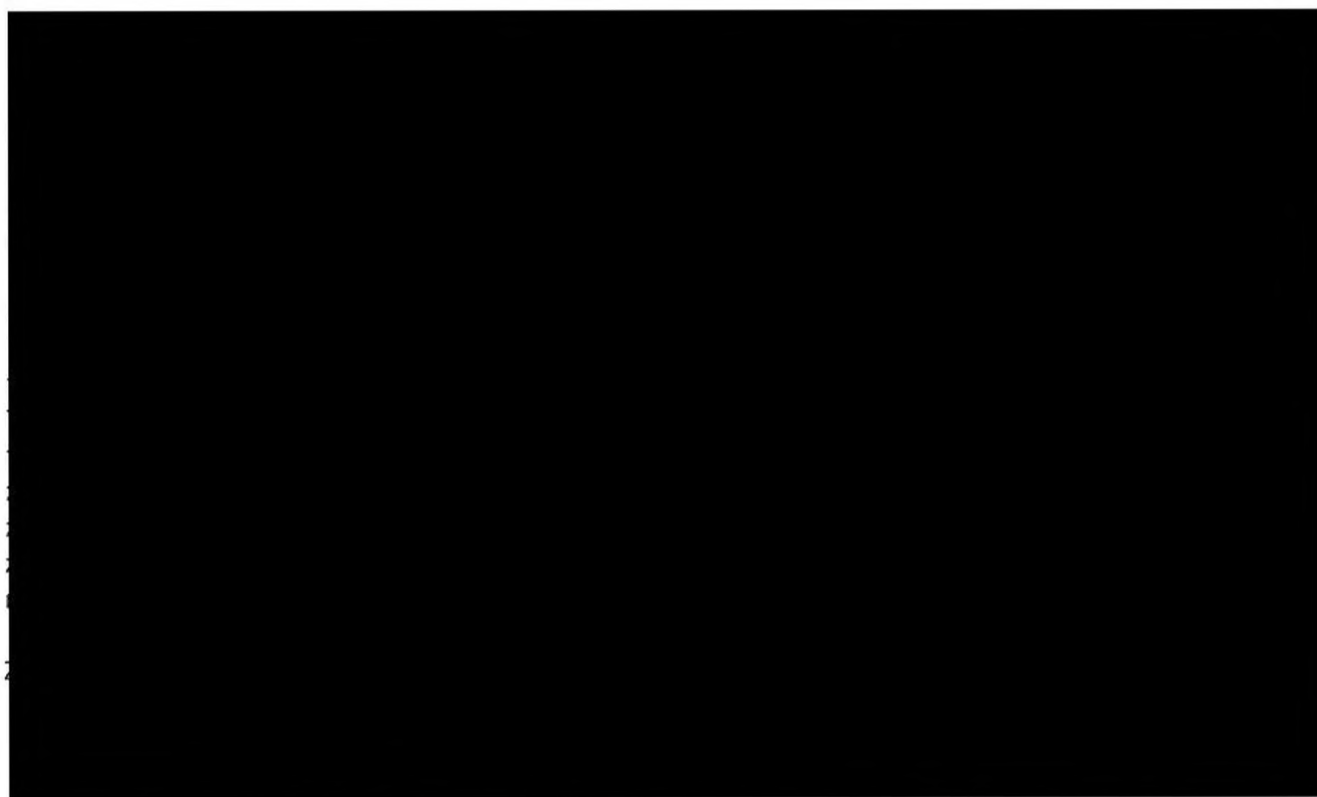
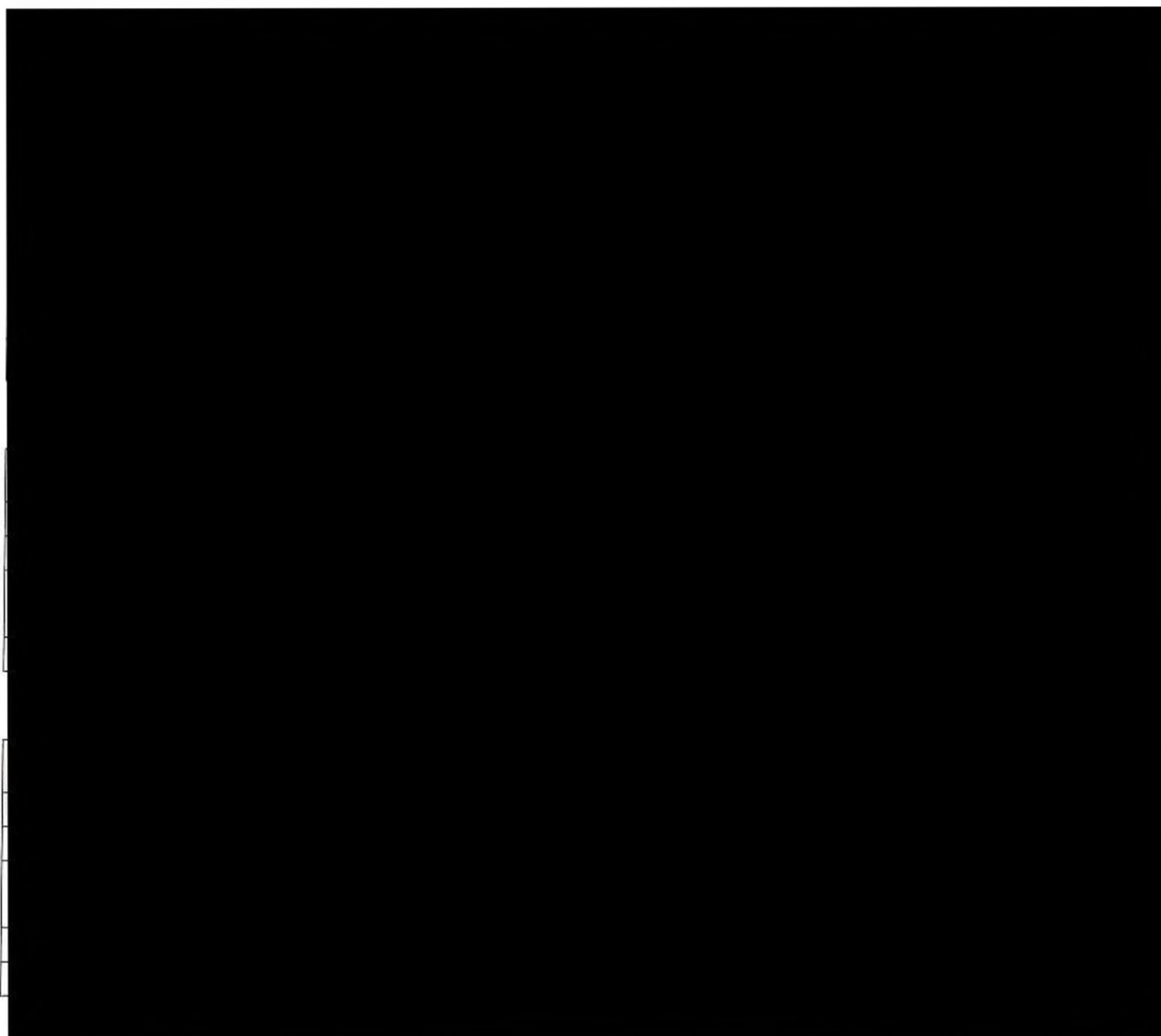


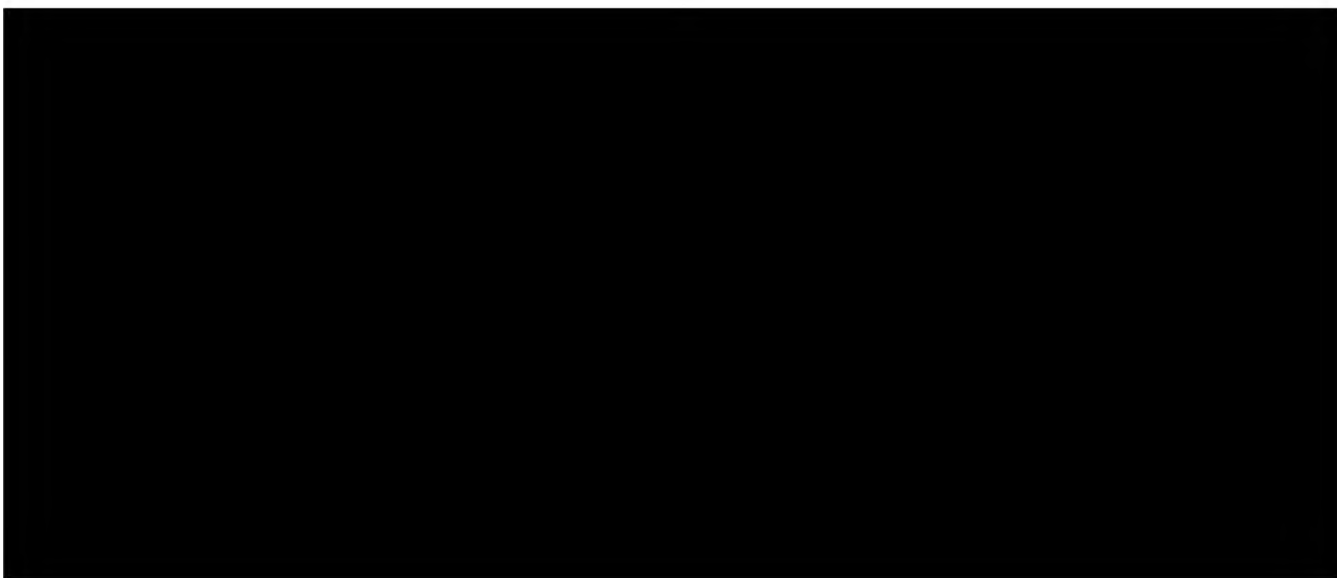
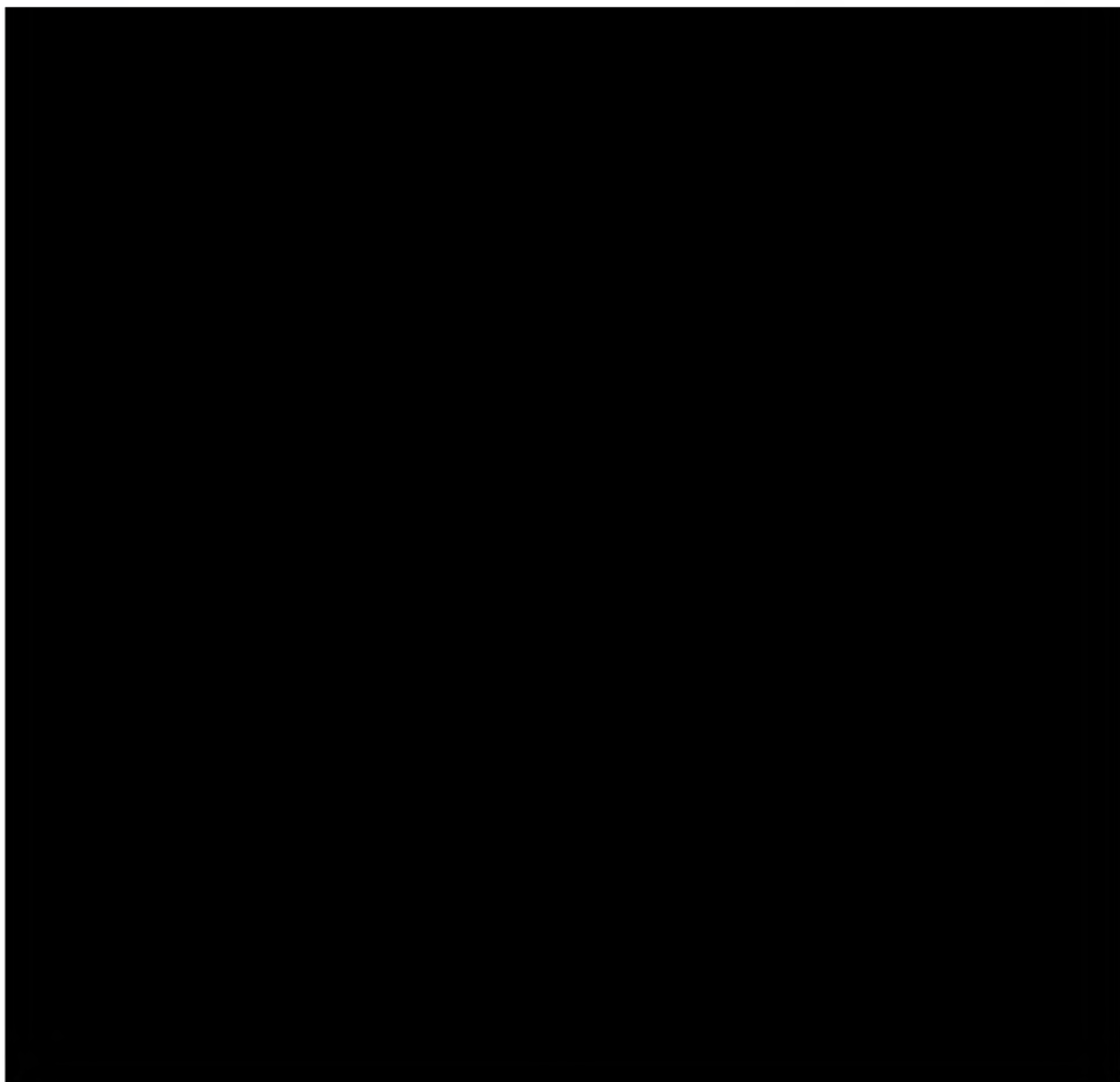


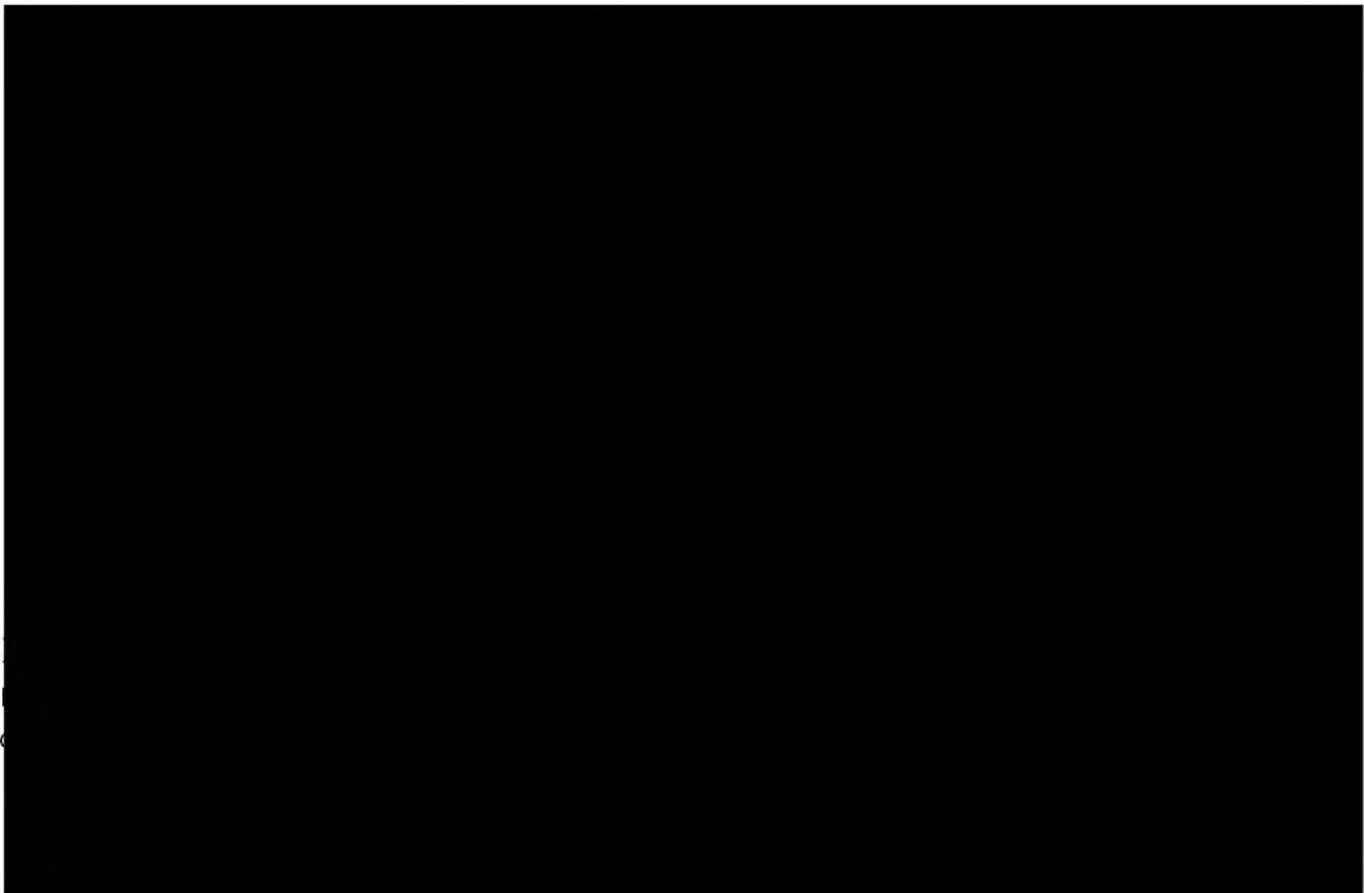
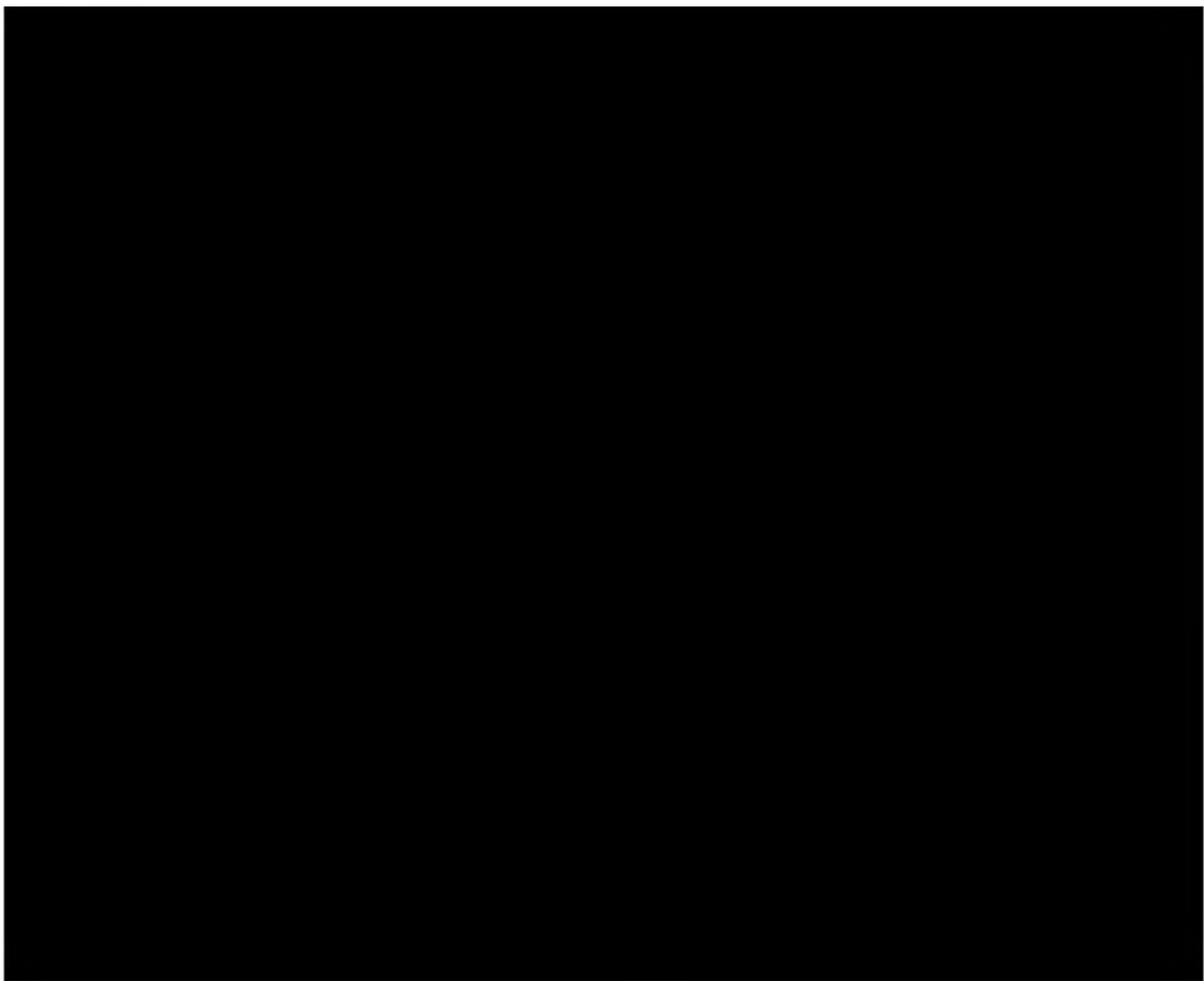


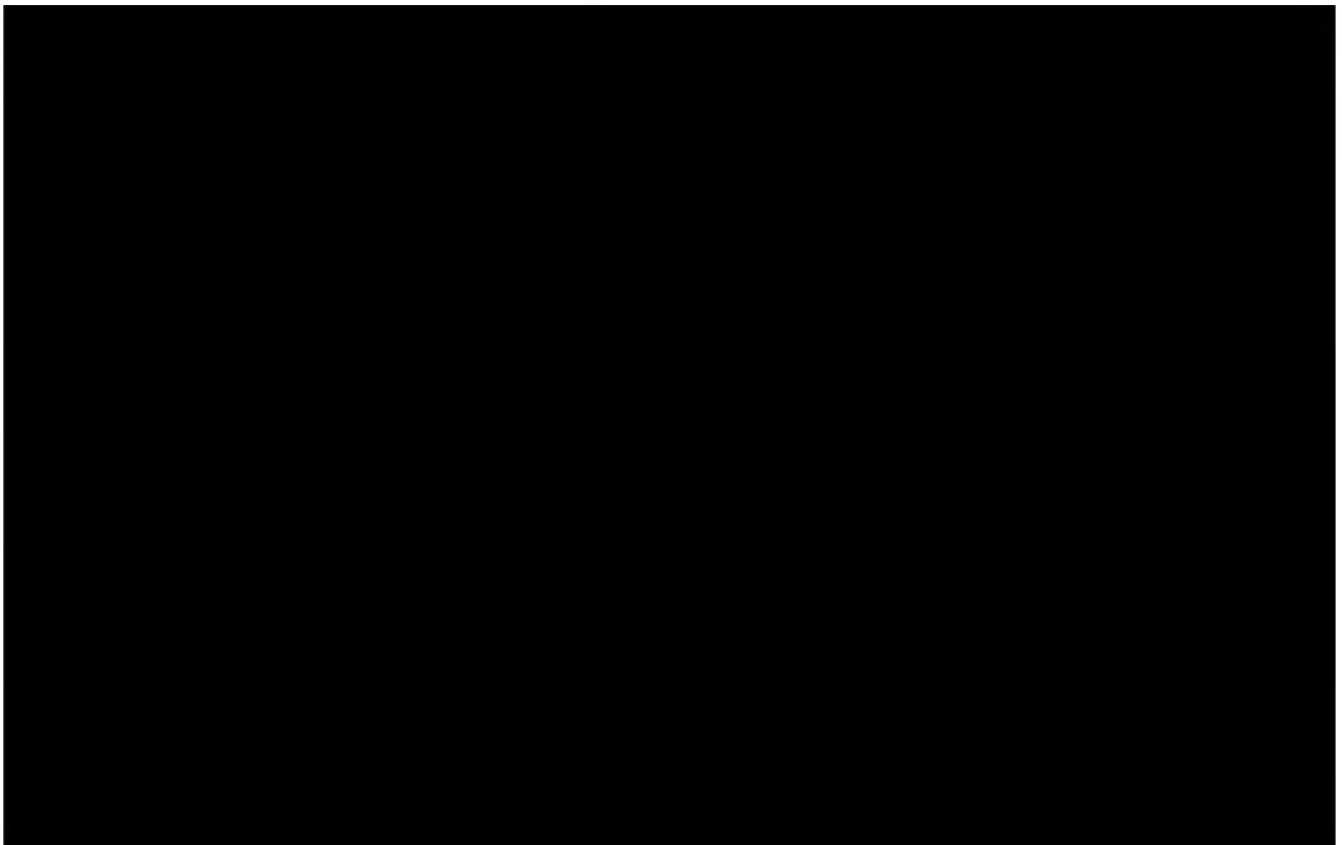
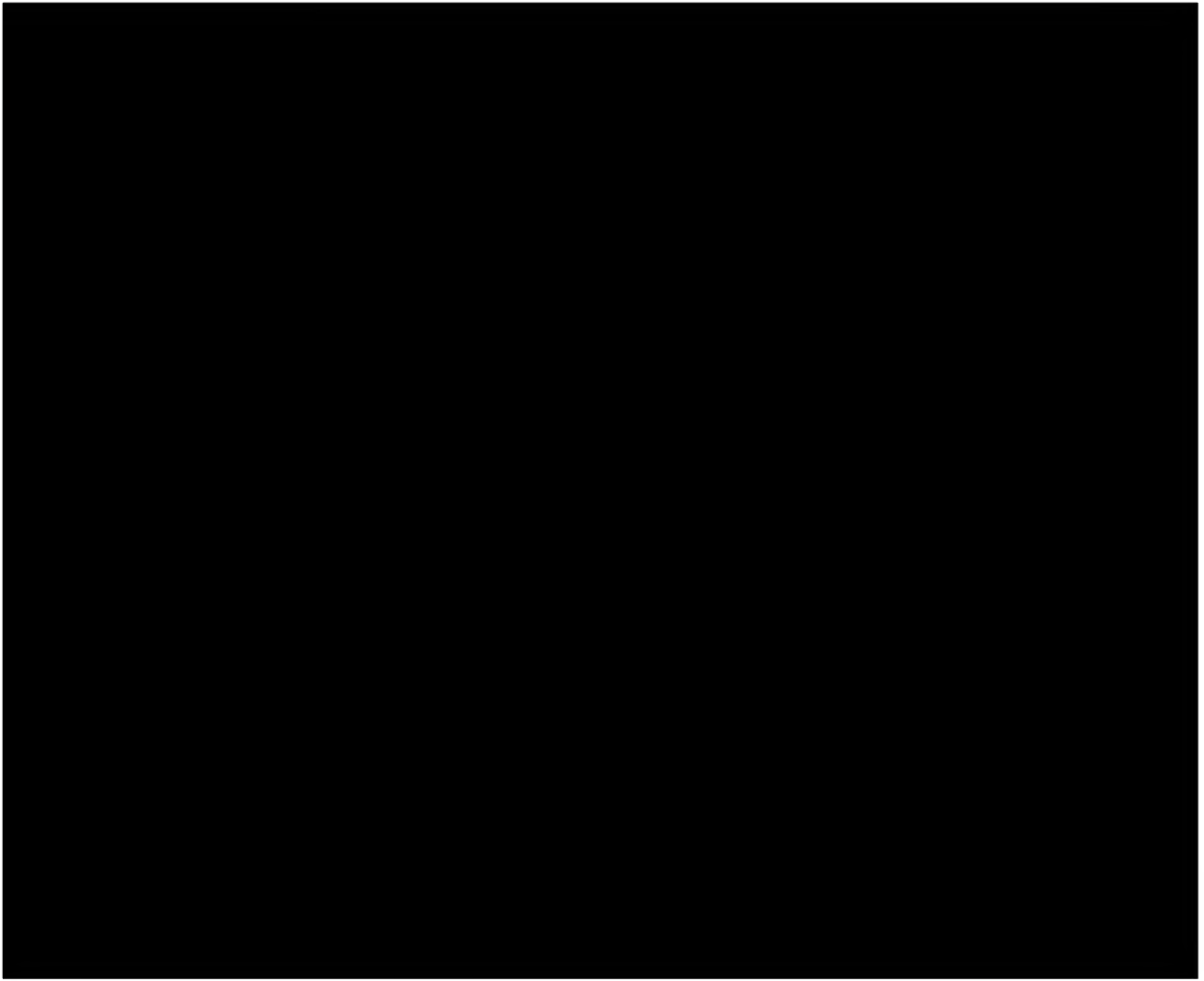


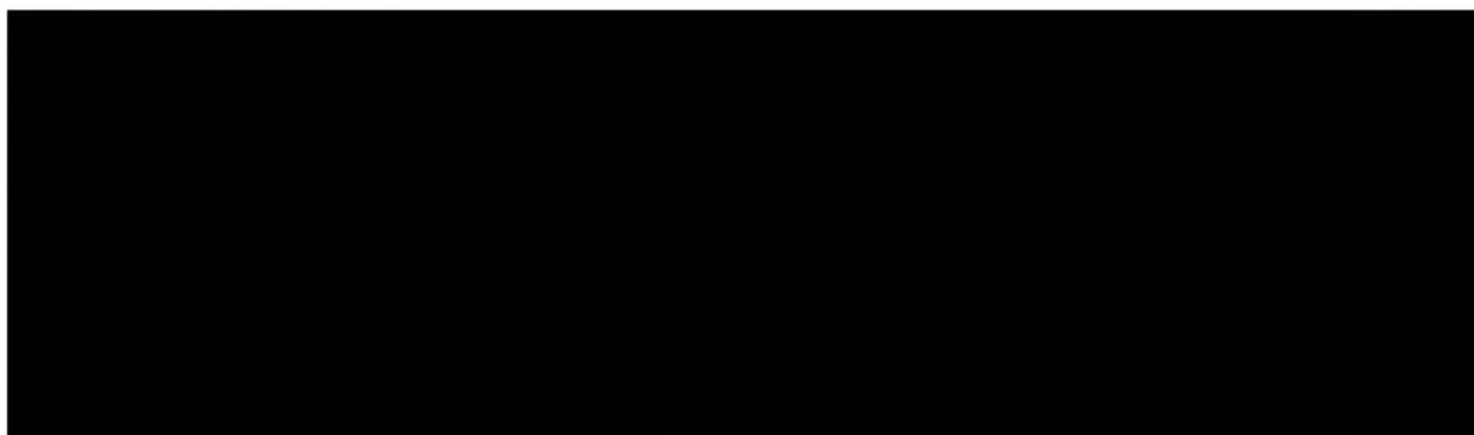
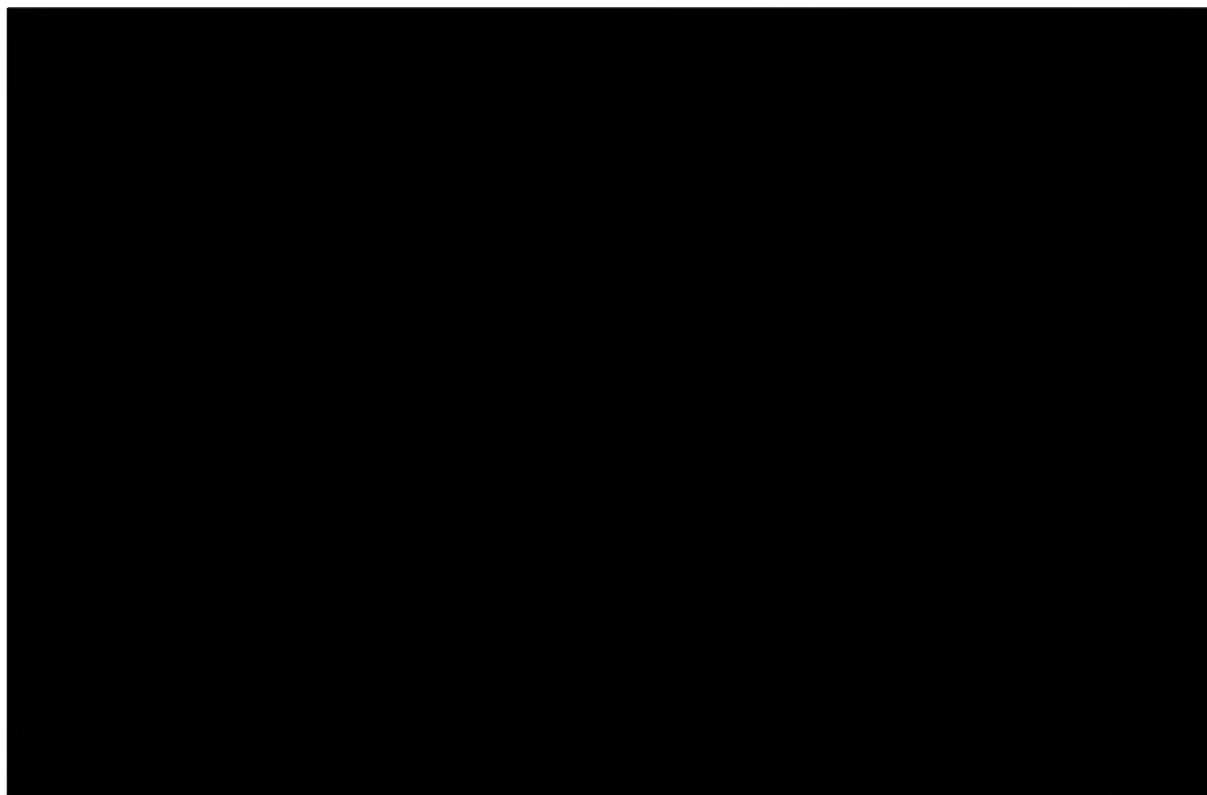
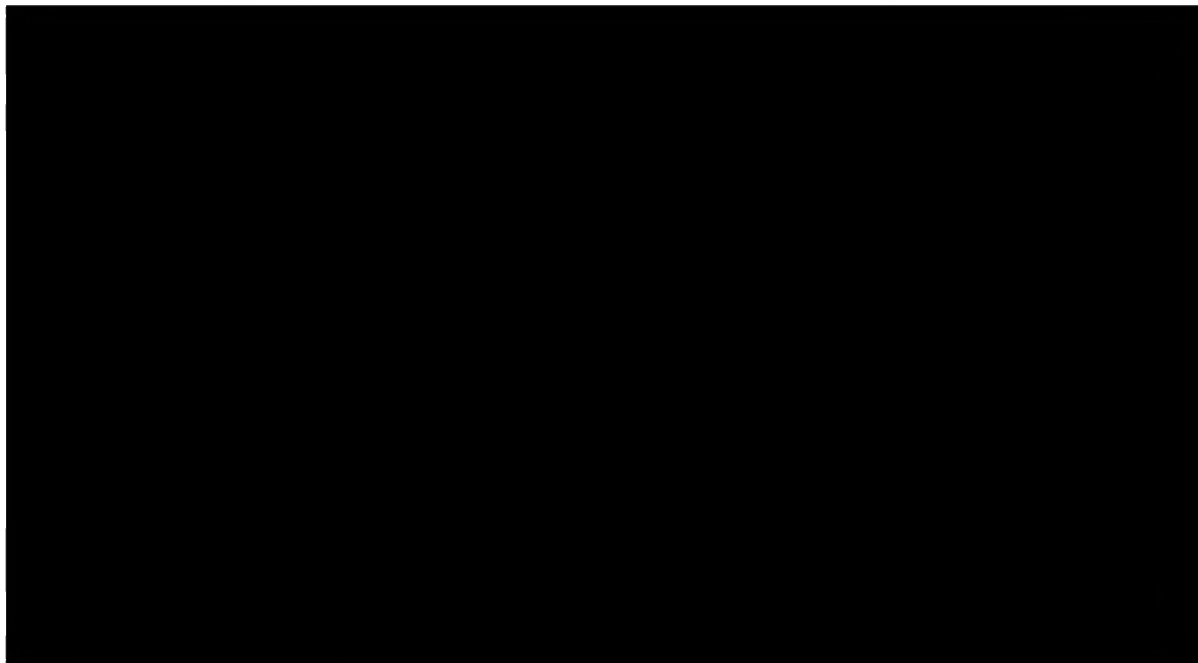


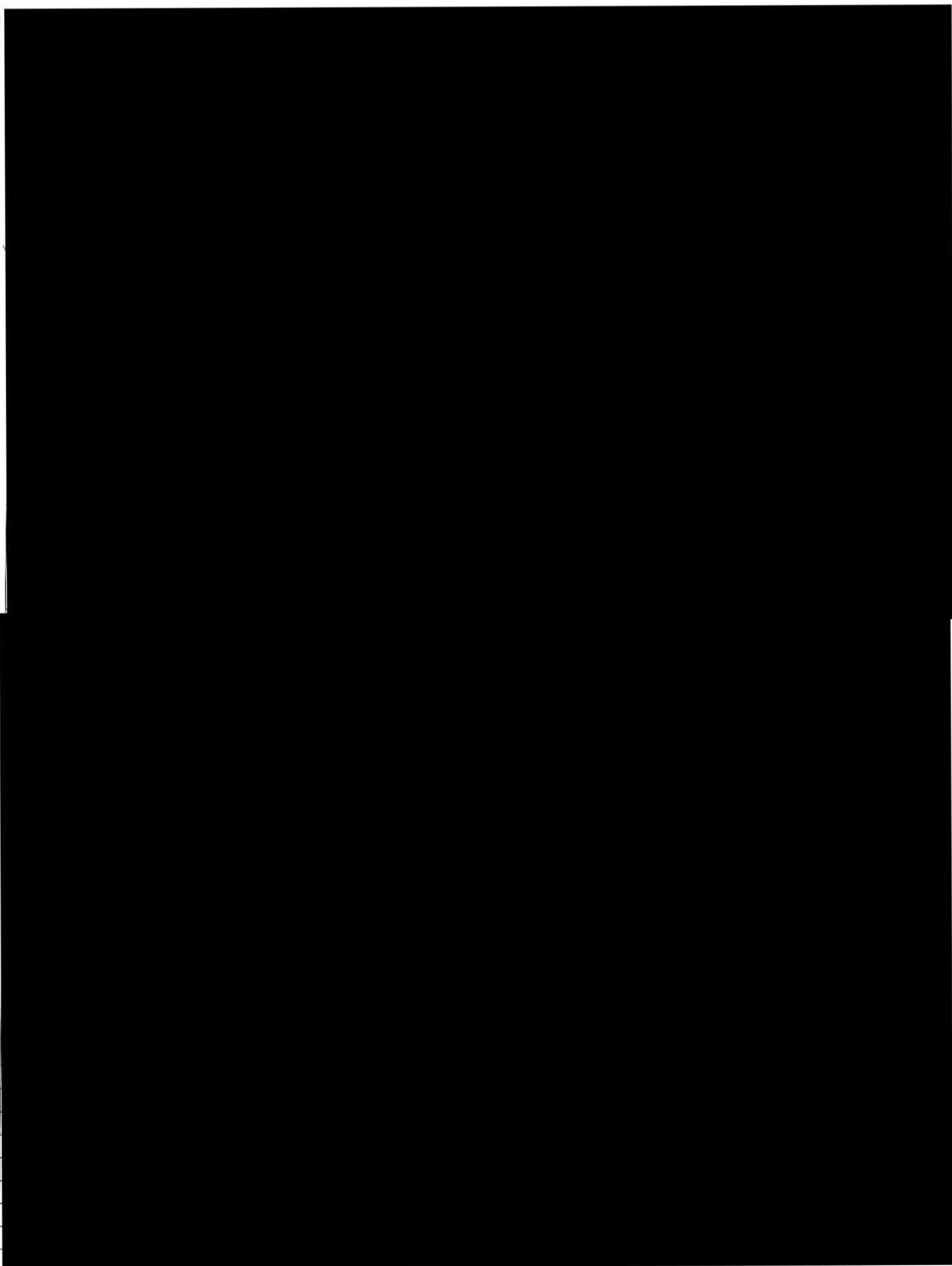


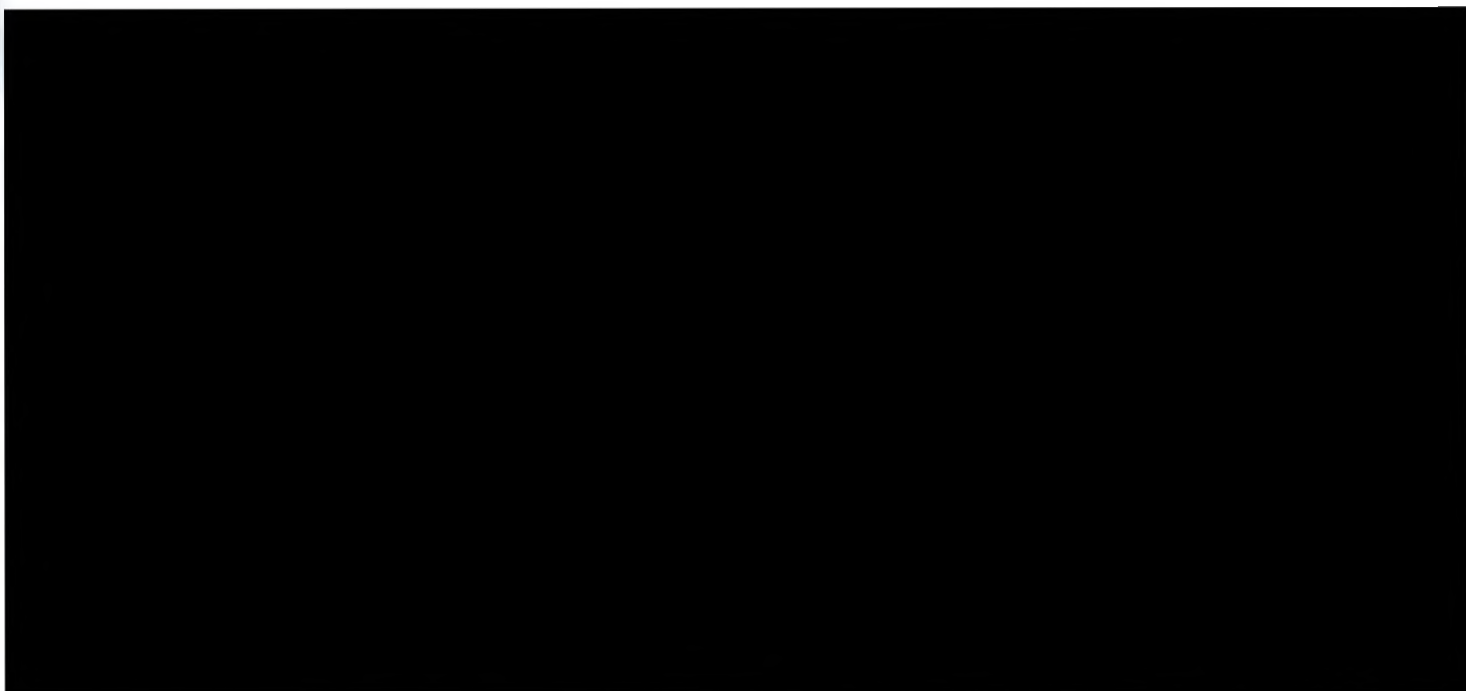


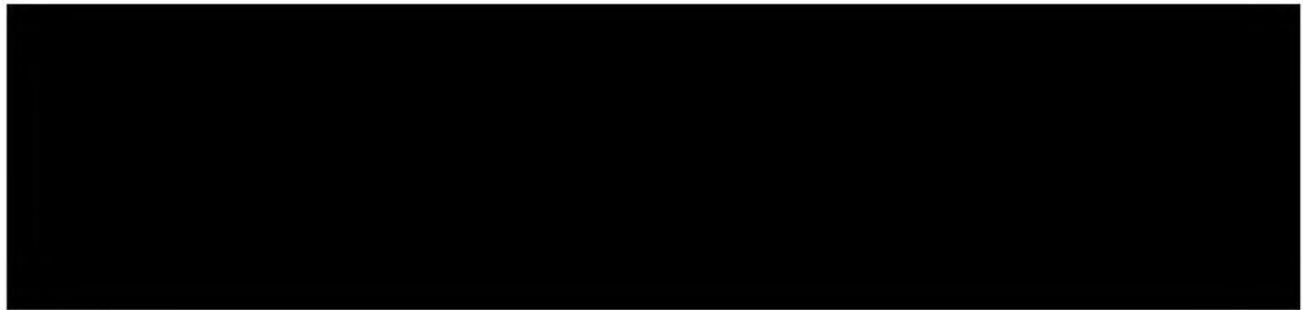
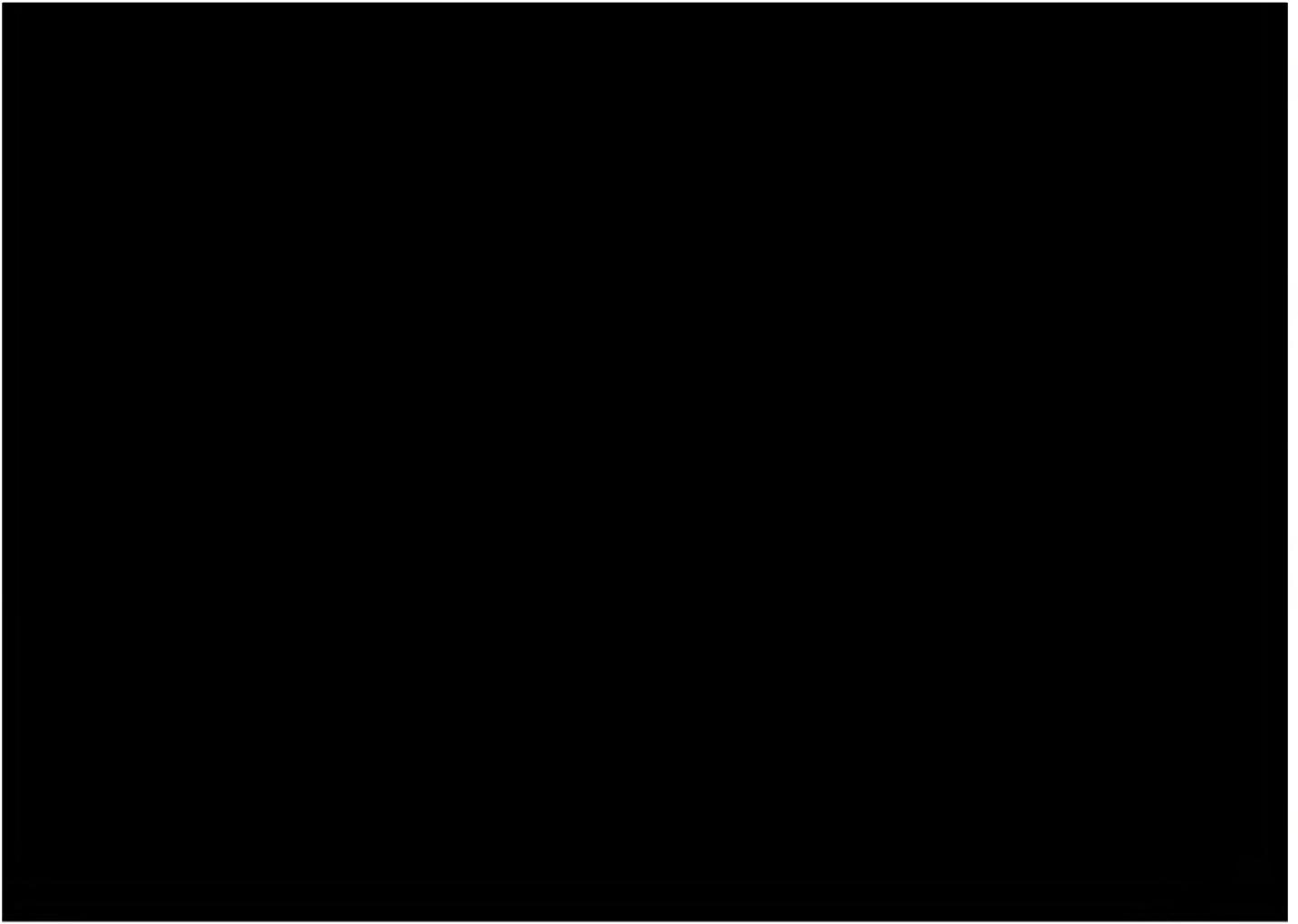












D03 Pojistná smlouva či pojistný certifikát

Kopie pojistného certifikátu je předkládána na následující straně.



MARSH

MARSH, s.r.o.
Vinohradská 2828/151
130 00 Praha 3

IČ: 45306541
Tel: 221 418 111
Fax: 221 418 150

POJISTNÝ CERTIFIKÁT č. 1051/2017

Pojištěný subjekt: **YOUR SYSTEM, spol. s r.o.**
Türkova 2319/5b, 149 00 Praha 4
IČ: 00 17 49 39

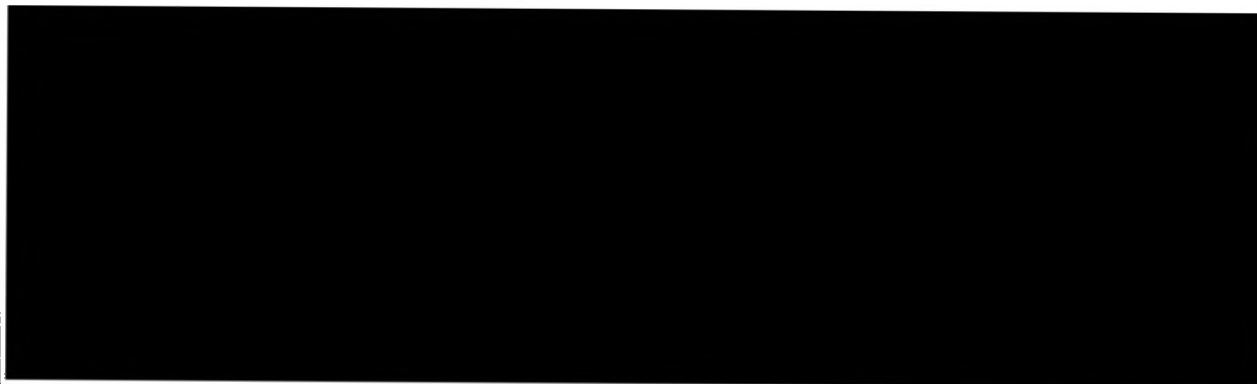
Pojistitel: **Česká pojišťovna, a.s.**

Pojistná smlouva č.: **899-18811-15**

Osvědčujeme tímto, že pojištěný subjekt uzavřel od 2.6.2016 prostřednictvím společnosti MARSH, s.r.o. pojistnou smlouvu výše uvedeného čísla, která kryje odpovědnost pojištěného za škodu v souladu s právními předpisy, která může nastat v souvislosti s činností pojištěného s tím, že pojištěný za škodu odpovídá a tato škoda je výsledkem jeho činnosti. Toto pojištění kryje odpovědnost za škody na věcech a škody vzniklé ze zranění osob nebo smrti. Územní rozsah je Česká republika, pojistné období od 2.6.2017 do 1.6.2018, pojistná částka 10.000.000,-Kč, pro odpovědnost za věci užívané a převzaté je pojištěn limit ve výši 5.000.000,-Kč.

Současně je pojištěna **profesní odpovědnost pro činnost Poskytování software**, a to na pojistnou částku 10.000.000,-Kč.

Platnost tohoto certifikátu končí se zánikem pojistné smlouvy, nejpozději však 1.6.2018.



D04 Etalon minimální bezpečnosti pro smluvní partnery

1 Účel a cíle

Etalon minimální bezpečnosti informací pro dodavatele MČ Praha 1 tvoří soubor pravidel a postupů, které stanovují požadovanou minimální úroveň bezpečnosti informací.

Dodržování pravidel uvedených v dokumentu je povinné pro všechny partnery spolupracující na smluvní bázi s MČ Praha 1, pro všechny jejich zaměstnance či osoby spolupracující se smluvními partnery.

Používané i nově zaváděné informační systémy v rámci MČ Praha 1 musí být upraveny, vyvíjeny nebo vybírány tak, aby splňovaly zásady bezpečnosti informací v souladu s tímto dokumentem a se základním dokumentem pro bezpečnost informací MČ Praha 1, tj. Politikou bezpečnosti informací MČ Praha 1.

Cílem etalonu minimální bezpečnosti informací pro smluvní partnery obecně je:

- a) Specifikovat základní pravidla a požadavky bezpečnosti informací MČ Praha 1 pro smluvní partnery;
- b) Předcházet porušování platných právních předpisů ČR;
- c) Zamezit, příp. minimalizovat možnost finanční, majetkové a nemajetkové újmy MČ Praha 1;
- d) Zabránit neautorizovanému přístupu k informacím MČ Praha 1;
- e) Umožnit řízení bezpečnosti informací MČ Praha 1 ve vztahu s dodavateli;
- f) Zajistit dostupnost informací pro oprávněné uživatele a procesy;
- g) Zabránit neautorizované modifikaci nebo zneužití dat a informací;
- h) Definovat základní pravidla bezpečnosti v oblasti vývoje a dodávek prostřední IT;
- i) Umožnit monitorování a vyhodnocování stavu bezpečnosti.

Výklad použitých zkratk:

BP	bezpečnostní politika informačního systému veřejné správy
ICT	informační a komunikační technologie (Information and Communication Technology)
IS	informační systém (obecně)
ISVS	informační systém veřejné správy (viz § 3 odst. 1 zák. č. 365/2000 Sb.)
MČ Praha1	Městská část Praha 1
ÚMČ Praha 1	Úřad městské části Praha 1
SŘBI / ISMS	systém řízení bezpečnosti informací, ustanovený na základě požadavků IEC 27001
MBI	Manažer bezpečnosti informací ÚMČ Praha 1
Zákon o ISVS	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, v platném znění
HelpDesk	primární, centrální bod pro kontakt se všemi uživateli IS/ICT a informačních služeb za účelem hlášení chyb, nedostatků i námětů pro rozvoj řešení
NTB	notebook

2 Bezpečnost informací

Bezpečností informací se rozumí zajištění třech hlavních aspektů – důvěrnosti, dostupnosti a integrity informací v duchu požadavků a doporučení norem řady ISO/IEC 27000.

K zajištění výše uvedených aspektů bezpečnosti informací musí dodavatel použít a řídit vhodná bezpečnostní opatření, zahrnující jak technické, tak organizační opatření, zohledňující rozsah hrozeb související s předmětem dodávky.

3 Obecné povinnosti

Mezi odpovědnosti smluvních partnerů patří zejména:

- a) Dodržování platných právních předpisů ČR k zajištění bezpečnosti informací;
- b) Využívání informačních systémů MČ Praha 1 a jejich komponent tak, jak vyplývá z provozní a bezpečnostní dokumentace těchto systémů;
- c) Používání informačních aktiv a ostatních aktiv MČ Praha 1 pouze v souladu s určeným rozsahem přístupových oprávnění a pouze ke schváleným účelům;
- d) Zajištění ochrany autentizačních údajů (login, heslo, identifikační předmět) k informačním systémům a zařízením MČ Praha 1, které mu byly svěřené, příp. těch, ke kterým má přístup při naplňování smluvního vztahu;
- e) Odpovědnost za každý přístup k informačním aktivům a dalším aktivům, provedený prostřednictvím jejich autentizačních údajů;
- f) Respektování a dodržování všech bezpečnostních opatření, pravidel a procedur, stanovených vlastníkem informací, tj. MČ Praha 1;
- g) Odpovědnost za dostatečné proškolení svých zaměstnanců a pracovníků svých subdodavatelů v oblasti zajištění bezpečnosti informací MČ Praha 1;
- h) Vyhodnocování rizik vůči bezpečnosti informací MČ Praha 1 v rozsahu smluvního vztahu a samostatně přijímání potřebných opatření k jejich ošetření;
- i) V případě vzniku bezpečnostního incidentu přijetí nezbytných opatření k eliminaci dopadů tohoto incidentu a neprodlené informování MČ Praha 1.

3.1 Poskytování informací třetím stranám

- a) Smluvní partneři jsou povinni dodržovat mlčenlivost o skutečnostech, které se dozvěděli při výkonu své činnosti na základě uzavřené smlouvy s MČ Praha 1.
- b) Každé případné veřejné použití neveřejných informací MČ Praha 1 musí být schváleno vedoucím Odboru informatiky MČ Praha 1.

4 Bezpečnost HW, SW a komunikací

Smluvní partneři MČ Praha 1 musí chránit aktiva MČ Praha 1, která používají při své práci nebo naplňování smluvního vztahu a zabránit podle svých nejlepších možností a schopností jejich poškození, zneužití a/nebo odcizení.

4.1 HW (pracovní stanice, ...)

Při práci na koncových pracovištích musí být splněny nejméně následující bezpečnostní pravidla:

- a) Použití koncového zařízení (počítače) musí být umožněno pouze oprávněné osobě;
- b) Je zakázáno připojovat soukromé počítače do vnitřní sítě MČ Praha 1 bez vědomí oprávněného pracovníka Odboru informatiky ÚMČ Praha 1;
- c) Koncová zařízení (pracovní stanice, NTB) nesmí být ponechána bez dozoru zapnuté a s přihlášeným uživatelem (k aplikaci, IS); za minimální opatření se považuje „uzamčení“ pracovní stanice;

- d) Počítače smluvního partnera, které mají být připojeny do vnitřní sítě ÚMČ Praha 1, musí mít aktivní ochranu před škodlivými kódy (antivirový program) v aktuální verzi databázi;
- e) Smluvní partner je povinen chránit vybavení ÚMČ Praha 1, udržovat bezpečné pracovní prostředí; v blízkosti prostředků informačních technologií je zakázáno jíst, pít a kouřit;
- f) V případě ukončení práce se zařízením je smluvní partner povinen provést odhlášení od systému.

4.2 Využívání prostředků a internetu

- a) Systémy MČ Praha 1, vztahující se k počítačové síti, internetu, intranetu, počítačové vybavení, program, operačních systémů a médií pro ukládání dat, ..., jsou ve vlastnictví MČ Praha 1. Tyto systémy mohou být používány pouze pro pracovní účely tak, aby to sloužilo zájmům MČ Praha 1;
- b) Smluvní partneři mají povoleno používání internetového připojení do a z vnitřní sítě MČ Praha 1 pouze za účelem plnění pracovních záležitostí v rozsahu smluvního vztahu. Způsob připojení a autentizace musí být předem dohodnuta s Odborem informatiky ÚMČ Praha 1;
- c) Obecně platí povinnost, že smluvní partner předem oznamuje datum a čas přihlášení k vnitřnímu prostředí a následně ukončení práce ve vnitřním prostředí systémů MČ Praha 1.

5 Bezpečnost IS / IT systémů

U vyvíjených nebo dodávaných informačních systémů, jejich HW/SW komponent, musí být zajištěna níže uvedená pravidla:

5.1 Aplikace

- a) Aplikace musí být vytvářeny tak, aby byl vždy vyžadován autorizovaný přístup uživatelů (identifikační a autentizační údaje); a musí být zaznamenávána činnost uživatele v aplikaci / systému;
- b) Uživatel aplikace musí být nucen si své přístupové heslo pravidelně měnit;
- c) Aplikace musí být vytvořena tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po několika neúspěšných pokusech o přihlášení musí být další zadávání hesla dočasně omezeno nebo činnost ukončena;
- d) Pokud je při přihlašování do aplikace některá část přihlašovacích údajů chybná, nesmí být přihlašovatel poskytnuta informace, kde je chyba v přihlašovacích údajích;
- e) V případě, že je povolen přístup do aplikace, v níž iniciační (vstupní) heslo určuje administrátor, musí aplikace vynutit změnu tohoto iniciačního hesla při prvním přihlášení uživatele;
- f) Všichni uživatelé musí při své činnosti používat jedinečný identifikátor tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti;
- g) Smluvní partner může používat jeden přihlašovací identifikátor pro několik svých zaměstnanců, přičemž smluvní partner odpovídá za veškeré úkony provedené v aplikaci či informačním systému pracovníkem přihlášeným s tímto identifikátorem;
- h) Systém správy hesel musí být podpořen efektivním a interaktivním vybavením, které prosazuje a vynucuje požadovanou kvalitu hesel.

5.2 Řízení přístupu k informačním systémům

- a) Před umožněním přístupu musí proběhnout identifikace a autorizace každého uživatele;
- b) Informační systém (příp. aplikace) by měl po určité době nečinnosti uživatele (doporučená doba <15> minut) daného uživatele odhlásit;

- c) Po stanoveném počtu neúspěšných autentizačních pokusů (dle politiky řízení přístupů <3>) se musí ukončit přihlašovací procedura;
- d) V případě neúspěšné autentizace nesmí systém poskytnout uživateli informace o tom, která část autentizace je chybná;
- e) U každého uživatele systému musí být možné identifikovat, jaká přístupová práva má přidělena;
- f) Pro každý prostředek systému musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, zápis, editace, ...);
- g) Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo celé skupině uživatelů.

5.3 Monitorování používání systému a přístupu k systému

V informačním systému (případně v jeho jednotlivých součástech) musí být pořizovány auditní záznamy obsahující minimálně:

- a) Identifikační údaje uživatele, resp. osoby provádějící úkony;
- b) Datum a čas přihlášení a odhlášení;
- c) Identifikaci místa, odkud se uživatel (resp. osoba) přihlašoval (dle možností);
- d) Záznamy o přístupu k systému, a to jak úspěšném i neúspěšném.

6 Bezpečnost informací a dat

6.1 Kontrola správnosti dat

Data vstupující do systémů musí být kontrolována tak, aby byla zajištěna jejich maximální správnost. V aplikaci se musí evidovat identifikátor uživatele nebo procesu, který pořízení nebo změnu dat provedl.

Pro kontrolu dat je nezbytné aplikovat opatření:

- a) Vstupní formální kontrola (neplatné znaky, rozsah, přetečení, kompletnost, souvislosti,...);
- b) Kontrola vnitřního zpracování dat (dle problematiky);
- c) Kontrola správnosti běhu programů;
- d) Kontrola integrity dat;
- e) Kontrola obsahu generovaných dat.

Opatření musí zahrnovat popis postupu při zjištění chyby v datech.

Pokud bude usouzeno, že vytvářený informační systém nebo aplikace by měla podporovat (využívat) kryptografické prostředky pro zajištění integrity dat, je nezbytné, aby aplikované prostředky byly podporovány mezinárodně uznávanými standardy a byly dodrženy právní předpisy České republiky.

6.2 Data / informace předávané smluvním partnerům

Jedná se o informace předávané MČ Praha 1 smluvnímu partnerovi na jakémkoliv nosiči a v jakékoliv formě, zejména listiny a dokumenty, CD ROM, Flash disky, pevné disky, nebo zaslané emailem.

Dále se jedná o jakékoliv informace a data MČ Praha 1, s kterými se smluvní partner seznámí nebo k nim má přístup na základě realizace činností prováděných v rámci smluvního vztahu.

Smluvní partner musí s informacemi nakládat v souladu s ustanovením tohoto dokumentu, pokud není smlouvou stanoveno jinak.

- a) Předání, resp. poskytnutí nebo přístup k informacím (datům) musí být vymezeno ve smlouvě (struktura dat, způsob předání/ poskytování, způsoby ochrany, ...) a musí probíhat řízením a bezpečným způsobem;
- b) Uchovávání a případné zpracovávání dat u smluvního partnera musí být prováděno tak, aby byla zajištěna jejich ochrana dle pravidel stanovených MČ Praha 1 před neoprávněným přístupem a aby bylo znemožněno jejich zneužití;
- c) Zodpovědnost za ochranu informací (dat) má smluvní partner;
- d) Informace (data), která již nejsou potřeba pro účely vymezené smluvním vztahem, musí být smluvním partnerem bezpečně zlikvidována, včetně jejich nosičů. Pro likvidaci nosičů obsahující neveřejné informace MČ Praha 1 musí být zvolena metoda, zaručující, že takto zlikvidované informace (data) nelze běžně dostupnými prostředky obnovit (např. skartovače, SW skartovače dat, ...); provedení likvidace doloží protokolem o jejich zlikvidování;
- e) Každé nové předání informací (dat) nebo zřízení dálkového přístupu k informačnímu systému nebo databázi na smluvním základě musí být konzultováno s manažerem bezpečnosti informací MČ Praha 1, příp. s bezpečnostním správcem systému MČ Praha 1;
- f) Smluvní partner si nesmí sám „stahovat“ (získávat) žádná data z informačních systémů MČ Praha 1, vytváření souborů dat musí provádět zaměstnanec ÚMČ, která následně vytvořená data smí poskytnout, resp. předat smluvnímu partnerovi.

7 Bezpečnost dodávek a služeb

7.1 Vývoj software a informačních systémů

Vývoj SW a informačních systémů musí probíhat:

- a) S využitím legálního software;
- b) Na testovacím prostředí odděleném od prostředí produkčního; za vytvoření testovacího prostředí a jeho bezpečnost odpovídá smluvní partner;
- c) Na testovacích datech, která nejsou převzata z provozní databáze; za testovací data je odpovědný smluvní partner. Pokud je nutné použít data z provozní databáze, je nutné je předem anonymizovat. Za bezpečnost testovacích dat odpovídá smluvní partner;
- d) Tak, že migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém prostředí a formalizovaném a doložitelném odsouhlasení těchto testů. Přístup smluvního partnera (dodavatele) do informačních systémů – podmínky:
 - a) Vzdálený přístup dodavatele může být povolen pouze do vývojového a testovacího prostředí za podmínek stanovených Odborem informatiky ÚMČ Praha. Případné výjimky musí být projednány a schváleny manažerem bezpečnosti informací MČ Praha 1, příp. bezpečnostním správcem systému;
 - b) Lokální přístup dodavatele do provozního prostředí (příp. k aktivům MČ Praha 1) musí být povolen manažerem bezpečnosti informací MČ Praha 1 v odůvodněných případech a musí probíhat v režimu dohledu ze strany Odboru informatiky ÚMČ Praha 1 nebo oprávněného (stanoveného) pracovníka ÚMČ Praha 1, ale vždy na základě žádosti dodavatele a po schválení Odborem informatiky ÚMČ Praha 1;
 - c) Přístup dodavatele do informačního systému MČ Praha 1 (testovacího i provozního prostředí) může být použit pouze pro realizaci činností zadaných oprávněným pracovníkem Odboru informatiky ÚMČ Praha 1 v rámci smluvního vztahu.
 - d) Vzdálený přístup k informačnímu systému MČ Praha 1 musí být chráněn kryptografickými prostředky;
 - e) Součástí dodávky informačního systému, příp. jeho částí, musí být mimo jiné:

- definice a dokumentování postupů pro spuštění a ukončení chodu IS a jeho částí,
- definice a dokumentování postupů pro obnovu činnosti IS po havárii,
- definice a dokumentování postupů pro ošetření mimořádných stavů technických i programových částí IS,
- definice a dokumentování záznamů o provozu IS (logy), včetně případného dálkového přístupu k těmto záznamům, jejich formy a způsobu ukládání,
- zajištění a dokumentování způsobu ochrany záznamů o provozu IS,
- zajištění podpory ze strany dodavatele při řešení bezpečnostních incidentů,
- definice a dokumentování postupů pro zálohování dat IS a pro obnovu dat ze záloh, včetně postupů testování použitelnosti záloh, pokud je tato funkcionality součástí systému.

7.2 Dodávky software

- a) Dodávka software (SW) musí být řádně smluvně zajištěna, průběžně kontrolována a dokumentována;
- b) U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený SW, nebo SW podléhající licenční nebo registrační politice;
- c) Dodávka licenčního SW musí zahrnovat jasná pravidla pro vydávání a používání licencí, včetně jejich evidence.
- d) Každý nový SW musí být otestován, než bude akceptován a zařazen do produkčního prostředí daného systému MČ Praha 1; za provedení testů je odpovědný dodavatel daného SW.

7.3 Dodávky hardware

- a) Dodávky hardware (HW) musí být řádně smluvně zajištěna, průběžně kontrolována a dokumentována;
- b) O každé dodávce musí existovat, kromě účetních dokladů, také předávací protokol o řádném dodání a instalaci HW; podepsaný dodavatelem a za odběratele oprávněným pracovníkem Odboru informatiky ÚMČ Praha 1;
- c) Způsob předání dodávaného HW a jeho otestování závisí na konkrétním produktu a podmínkách smluvním vztahu s dodavatelem;
- d) Každé nové HW zařízení musí být otestováno, než bude akceptováno a zařazeno do produkčního prostředí; za provedení testů je odpovědný dodavatel daného hardware.

7.4 Dodávky služeb a ostatní služby

- a) Dodávka služeb musí být řádně smluvně zajištěna, průběžně kontrolována a dokumentována ze strany dodavatele i zadavatele;
- b) Způsob předání výstupů služby závisí na konkrétní službě a na smluvních podmínkách dohodnutých ve smlouvě; vždy musí existovat předávací a akceptační protokol o řádném poskytnutí služby;
- c) Pracovníci smluvních partnerů, zajišťující servis IT technologií (HW / SW / IS), jsou na základě smlouvy oprávněni se pohybovat i na neveřejných místech ÚMČ Praha 1; a to vždy a pouze s vědomím oprávněného pracovníka Odboru informatiky ÚMČ Praha 1;
- d) Pracovníci smluvních partnerů, zajišťující ostatní služby (např. úklid, ostrahu, ...) jsou na základě smlouvy oprávněni pohybovat se na neveřejných místech ÚMČ Praha 1. Při svém pohybu musí dbát příslušných bezpečnostních pravidel, nemají zpravidla přístup k informačním aktivům MČ Praha 1.

7.5 Dokumentace dodávky SW, HW a služeb

- a) Nedílnou součástí každé dodávky SW, HW nebo služeb je příslušná projektová, provozní a bezpečnostní dokumentace vztahující se k předmětu dodávky;

- b) Chybějící, neúplná a/nebo neaktuální dokumentace je důvodem k reklamaci dodávky a může být i důvodem k neakceptaci dodávky z důvodů nenaplnění požadavků ze strany dodavatele;
- c) Dokumentace musí být předána formálním způsobem a podrobena akceptačnímu řízení ze strany zadavatele, tj. MČ Praha 1;
- d) Dodavatel je povinen všechny změny v konfiguraci IS/IT v průběhu dodávky zadokumentovat a v případě již zpracované dokumentace musí provést její aktualizaci v potřebném rozsahu.

7.6 Akceptace dodávky

- a) Každý dodaný SW, HW a služba musí být plně a v potřebné míře otestována, zda splňuje očekávané a smluvně definované parametry; a zda jeho používání nepředstavuje neočekávaná bezpečnostní nebo provozní rizika;
- b) V případě informačního systému, před jeho uvedením do rutinního provozu, musí být formálně akceptován z hlediska provozního příslušným pracovníkem Odboru informatika a z hlediska bezpečnosti informací MBI ÚMČ Praha 1.

7.7 Outsourcing

- a) Outsourcing musí být řádně smluvně zajištěn, průběžně monitorován a dokumentován;
- b) Externí zpracovávání neveřejných informací MČ Praha 1 a přístup k aktivům MČ Praha 1 musí být smluvně ošetřeno tak, aby byla zajištěna úroveň ochrany informací MČ Praha 1 ve všech aspektech informační bezpečnosti dle požadavků MČ Praha 1 a platných právních předpisů ČR.

8 Fyzická bezpečnost

Cílem fyzické bezpečnosti v oblasti IT je chránit prostředí, ve kterém se nacházejí aktiva MČ Praha 1, zabránit náhodnému nebo cílenému neautorizovanému přístupu, poškození nebo narušení aktiv MČ Praha 1.

Prostory ÚMČ Praha 1 jsou rozčleněny na oblasti veřejnosti přístupné a oblasti neveřejné (např. serverovny, prostory s HW aktivy, ...).

- a) V neveřejných prostorech není dovolen pohyb cizích osob, tzn. včetně pracovníků smluvních partnerů (= neautorizovaných osob) bez doprovodu oprávněného pracovníka ÚMČ Praha 1;
- b) Cizí osoby (= neautorizované osoby) nesmějí být ponechány v neveřejných prostorech ÚMČ Praha 1 bez dozoru, pokud tato skutečnost není ošetřena smlouvou.

9 Personální bezpečnost

Cílem personální bezpečnosti v oblasti IT je vytvoření potřebného bezpečnostního povědomí zaměstnanců dodavatele, příp. subdodavatelů, smluvních partnerů MČ Praha 1 v oblasti zajištění ochrany a bezpečnosti aktiv MČ Praha 1 s cílem předcházet, příp. zabránit neautorizovanému přístupu, narušení důvěrnosti a integrity aktiv MČ Praha 1.

- a) Smluvní partner je odpovědný za veškeré aktivity osob provádějící činnosti na základě uzavřeného smluvního mezi smluvním partnerem a MČ Praha 1;
- b) Smluvní partner zajistí, že veškeré činnosti dle smluvního vztahu, budou prováděny kompetentními osobami, s příslušnou odbornou kvalifikací a bezpečnostními zárukami;

- c) Smluvní partner provede a doložitelně dokumentuje rozsah a obsah proškolení osob podílejících se na realizaci smluvního vztahu v oblasti zajištění bezpečnosti informací MČ Praha 1;
- d) Rozsah a obsah proškolení vychází jednak z požadavků tohoto dokumentu, dále z platné Politiky bezpečnosti informací MČ Praha 1 a dalších upřesnění manažera bezpečnosti informací k danému smluvnímu vztahu.