

Příloha č.1, část (A): Převzetí podpory

Tato příloha specifikuje kontext a parametry převzetí systému IDM od současného provozovatele.

1.1. Zkratky a pojmy

Zkratka	Vysvětlení
AD	Microsoft Active directory, tj. technologický prvek v IT infrastruktuře
Celoměstská identita	identita založená v IDM s platností pro systémy MHMP, MČ i MO
Dílo	souhrnné označení pro celou dodávku v rámci této veřejné zakázky
DMZ	demilitarizovaná zóna, veřejně přístupná část IT sítě
FO	fyzická osoba
HW	hardware
IDM	Identity management, tj. systém pro správu identit uživatelů
MČ	Městské části hlavního města Prahy
Městské organizace (MO)	příspěvkové organizace zřizované hlavním městem Praha
MHMP	Magistrát hlavního města Prahy
Objednatel	Hlavní město Praha, Mariánské náměstí 2, Praha 1, 110 00
Osoba	reprezentace fyzické osoby v systému prostřednictvím sady atributů
PO	právní osoba
Poskytovatel	uchazeč, se kterým bude podepsán smluvní vztah dle této veřejné zakázky na dodávku Díla
Privilegované účty	uživatelské účty s nadstandardní sadou oprávnění, např. administrátorské
Role	určuje rozsah povolených činností uživatele v informačním systému
Service Desk	nástroj Zadavatele k evidenci tiketů
SLA	Service level agreement, tj. nastavení úrovně parametrů služby
SSO	Single sign-on, tj. princip jednotného přihlašování napříč informačními systémy
SW	software
Systém	pokud není v kontextu uvedeno jinak, jedná se o systém IDM, který je předmětem této veřejné zakázky
Technické účty	uživatelské účty, které nejsou svázané s jednou osobou, ale slouží pro zajištění funkčnosti systému nebo integrace mezi systémy
Technický garant	garanta systému technického rázu, zodpovědného za chod systému a kontakt s jeho dodavatelem
Uživatel	osoba, která má přístup k systémům v doméně MHMP a v doménách dalších MO“

1.2. Celkový rozsah etapy Převzetí podpory k novému Poskytovateli

Poskytovatel převezme stávající systém IDM a všechny jeho součásti, včetně dokumentace, softwarového vybavení, datové základny a konfigurace.

Objednatel požaduje po Poskytovateli následující rozsah činností v rámci této etapy:

Činnost	Výstup	
1	Provedení inventarizace veškerých technických komponent systému a poskytnuté dokumentace, vč. seznámení se zdrojovými kódy systému a konfiguračních částí.	Přehled zjištěného ve formě inventarizace komponent a převzaté dokumentace.
2	Vypracování analýzy stavu otevřených problémů (evidovaných v Service Desku) souvisejících s provozem IDM.	Seznam se stručným popisem stavu všech otevřených provozních problémů (pokud takové v době plnění budou otevřeny).
3	Vypracování analýzy stavu otevřených koncepčních problémů souvisejících s rozvojem a architekturou IDM.	Seznam se stručným popisem stavu všech otevřených koncepčních problémů.
4	Vypracování analýzy stavu a provedení revize implementovaných procesů, včetně analýzy rozhraní na integrované systémy, v rámci IDM.	Seznam se stručným popisem stavu všech aktuálně implementovaných procesů a rozhraní v rámci systému IDM.
5	Provedení revize a aktualizace dokumentace skutečného provedení.	Revidovaná provozní dokumentace.
6	Příprava realizačního Plánu Upgrade	Vytvoření realizačního Plánu upgrade, s popisem realizačních kroků, náročnosti, součinností a harmonogramu.
7	Příprava Provozní příručky	Vytvořená Provozní příručka.
8	Vytvoření protokolu o převzetí	Protokol o provedení činností a převzetí.

Podpis protokolu o provedení činností a převzetí je rozhodný okamžik, kdy se z předávaných dílčích komponent systému předcházejícího poskytovatele, včetně všech jeho součástí, stává jediný funkční celek dále provozovaný pod souhrnným označením IDM.

1.3. Činnost - Provedení inventarizace veškerých technických komponent systému a poskytnuté dokumentace, vč. seznámení se zdrojovými kódy systému a konfiguračních částí.

V Příloze č. 1, část (E) Smlouvy je specifikován stávající stav a rozsah nasazení systému IDM v prostředí Objednatele, ze kterého může Poskytovatel vycházet. Zadavatel předá Poskytovateli veškerá práva k systému k umožnění ověření reálného stavu systémů. V rámci této činnosti je požadováno po Poskytovateli provedení analýzy současného reálného stavu nasazení IDM, jeho všech technických komponent, poskytnuté dokumentace, zdrojového kódu systému a konfiguračních částí. Souhrnně bude analýza zahrnovat:

- vlastní softwarové části platformy MidPoint,
- případné dodělané podpůrné komponenty, potřebné pro integrace okolních systémů,
- virtuální servery a případné infrastrukturní prvky,
- dokumentaci:
 - Původní technická analýza nasazení
 - Dokumentace skutečného provedení – MHMP a Městská policie
 - Provozní dokumentace
 - Administrátorská dokumentace
 - Uživatelská dokumentace
 - Bezpečnostní příručka
- zdrojové kódy všech technických komponent,
- konfigurační soubory, nutné pro běh systému

Cílem této činnosti je, aby Poskytovatel získal jednoznačný přehled o rozsahu a stavu nasazení a používání systému IDM.

Výstupem této činnosti je dokument obsahující přehled zjištěného ve formě detailního přehledu komponent a převzaté dokumentace.

1.4. Činnost - Vypracování analýzy stavu otevřených problémů (evidovaných v servicedesk) souvisejících s provozem IDM.

V rámci této činnosti je požadováno po Poskytovateli provedení analýzy všech otevřených záznamů (ticketů) v rámci současně používaného systému pro hlášení problémů a dotazů Service Desk. Přístup k tomuto systému bude Objednatelem Poskytovateli zřízen na začátku etapy tranzice.

Cílem této činnosti je, aby Poskyvatel získal přehled o případných provozních problémech, či delší dobu nevyřešených otázkách systému IDM.

Výstupem této činnosti je dokument obsahující seznam se stručným popisem stavu všech otevřených provozních problémů IDM (pokud takové v době plnění budou otevřeny).

1.5. Vypracování analýzy stavu otevřených koncepčních problémů souvisejících s rozvojem a architekturou IDM.

V rámci této činnosti je požadováno po Poskytovateli provedení sběru a analýzy v oblasti koncepčních, strategických a architektonických problémů systému IDM. Systém je již několik let v produkčním provozu. Řada původně zamýšlených úprav a rozšíření nebyla ve výsledku implementována. Některé napojené okolní systémy jsou napojeny jen jednoduchým způsobem s cílem rozšíření a další podobné oblasti.

Poskyvatel analyzuje poskytnuté podklady a provede pohovory s relevantními zástupci Objednatele (zejména věcný garant, technický garant, odbor bezpečnosti a odbor rozvoje informačních systémů) s cílem identifikovat tyto oblasti a popsat jejich zamýšlenou formu.

Cílem této činnosti je, aby Poskyvatel získal představu o aktuálních potřebách změny, resp. rozvoje systému IDM do budoucna.

Výstupem této činnosti je seznam se stručným popisem aktuálního a cílového stavu všech otevřených koncepčních problémů IDM.

1.6. Vypracování analýzy stavu a provedení revize implementovaných procesů, včetně analýzy rozhraní na integrované systémy, v rámci IDM

V rámci této činnosti je požadováno po Poskytovateli provedení analýzy implementovaných procesů v rámci systému IDM, tj. např. proces obnovy hesla, přidělení nové role, synchronizace rolí s doménou a další. U každého takového procesu získat představu o jeho formě, zda je využíván, jestli plní zamýšlenou funkci a zda fakticky funguje.

Poskyvatel také provede, dle poskytnuté dokumentace a faktického stavu, analýzu všech existujících (funkčních i rozpracovaných) rozhraní systému IDM na ostatní integrované systémy.

Cílem této činnosti je, aby Poskyvatel získal přehled o implementovaných (a v jaké formě) procesech, které systém IDM obsluhuje a jak jsou používány, včetně jejich závislostí na okolní systémy. Poskyvatel také získá přehled o úrovni implementovaných rozhraní.

Výstupem této činnosti je dokument obsahující seznam se stručným popisem stavu všech aktuálně implementovaných procesů v rámci systému IDM. Dokument bude také obsahovat seznam a stav všech implementovaných rozhraní.

1.7. Provedení revize a aktualizace dokumentace skutečného provedení

V rámci této činnosti je požadováno po Poskytovateli provedení seznámení s dostupnou Objednatelem předanou dokumentací k IDM a jeho částí. V návaznosti na výstupy činností viz výše následné provedení aktualizace dokumentu dokumentace skutečného provedení IDM, kterým Objednatel disponuje a který nezohledňuje aktuální stav. Objednatel požaduje, aby architektura systému byla v rámci standardu Objednatele vypracována a předložena v SW nástroji Enterprise architekt.

Cílem této činnosti je, aby Poskyvatel získal přehled o dostupné dokumentaci, její struktuře, obsahu a úplnosti. Zároveň, aby dokumentace skutečného provedení byla aktualizována na zjištěný faktický stav.

Výstupem této činnosti je aktualizovaný dokument dokumentace skutečného provedení IDM, který zohledňuje skutečný zjištěný stav z činností výše a zakreslená architektura řešení v SW nástroji Enterprise architekt.

1.8. Příprava rámcového realizačního Plánu Upgrade

V rámci této činnosti Poskytovatel popíše realizační kroky, které je nutné udělat v souvislosti s Upgrade stávající verze produktu midPoint na aktuální verzi. Tento upgrade bude řešen v rámci změnového řízení, ale s ohledem na náročnost přípravy této činnosti na straně Zadavatele, je nutné zajistit součinnost na straně Zadavatele co nejdříve.

Cílem je mít rámcový plán a harmonogram všech nutných realizačních kroků, jejich popis a požadavky na součinnost.

Výstupem je dokument, který bude obsahovat výše definované požadavky.

1.9. Příprava Provozní příručky

V rámci této činnosti Poskytovatel vypracuje a předloží ke schválení Provozní příručku, která nastaví rozsah prováděných činností, jejich četnost, SLA a další podmínky provozu IDM. Bude také obsahovat organizační strukturu, odpovědnosti, procesy, role a komunikaci na projektu. Jednotlivě budou popsány ITIL procesy a jejich zajištění a nastavení - změnové řízení, řízení nových verzí, řízení incidentů, řízení problémů, řízení konfigurací, řízení rizik, apod.

Cílem této činnosti je mít nastavené řízení projektu po převzetí.

Výstupem je dokument Provozní příručka, který bude řídicím dokumentem projektu v oblasti zajištění provozních a servisních činností.

1.10. Vytvoření protokolu o převzetí

V rámci této činnosti je požadováno po Poskytovateli vytvoření protokolu o převzetí, který bude obsahovat soupis všech výstupů činností v rámci etapy Převzetí podpory. U každé činnosti bude stručně uvedeno, jaké práce byly vykonány a jaký výstup je přebírán.

Cílem této činnosti je, aby Poskytovatel i Objednatel disponovali jednotným pohledem na předávaný/přebíraný systém IDM a jeho technické i netechnické části a jejich faktický stav.

Výstupem této činnosti je protokol o převzetí, obsahující, jaké práce byly vykonány a jaký výstup je přebírán.

Příloha č.1, část (B): Dílo

Tato příloha obsahuje technickou specifikaci na 5 změnových požadavků, které Zadavatel může požadovat implementovat do současné verze:

Etapa 1:	Integrace žádostí o roli v Systému prostřednictvím nadstavby Marbes
Etapa 2:	Aplikace SelfService pro městské části – aplikace pro správu hesel
Etapa 3:	Integrace více faktorové autentizace
Etapa 4:	Integrace aplikace Zahraniční služební cesty
Etapa 5:	Úprava systému pro robustní kontrolu duplicit identit

Po podpisu Smlouvy budou u každého změnového požadavku realizovány následující etapy:

- finalizace analýzy a návrhu řešení, návrh akceptačních testů,
- vývoj a implementace,
- testování,
- školení,
- dokumentace – aktualizace všech typů dokumentace,
- akceptace.

Zadavatel požaduje pro každý změnový požadavek od Uchazeče uvést do nabídky:

- popis navrhovaného řešení,
- harmonogram realizace,
- požadavky na součinnost,
- cenu za dílo jako fixní a nepřekročitelnou.

Etapa 1: Integrace žádostí o roli v Systému prostřednictvím nadstavby Marbes

Výchozí koncepční předpoklady integrace aplikace Nadstavby s řešením IDM:

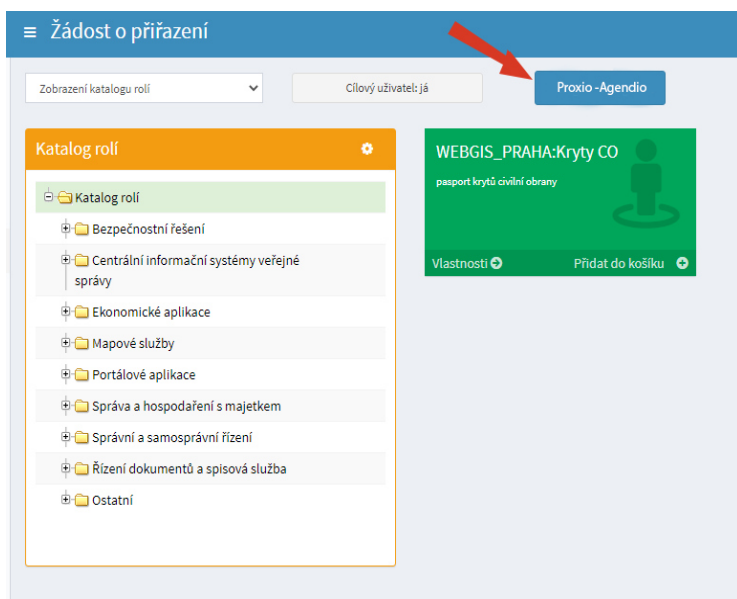
- Nadstavba není v tomto případě propojená s EOS, takže nemá přehled přiřazených rolí pro přístup do Proxio Agendia, ten udržuje IDM.
- Nadstavba umožní uživateli sestavit roli z pracovních náplní, případně dalších parametrů a předá o tom informace IDM (náplně, parametry, příslušné profily).
- IDM roli zaeviduje a po schválení (v případě Zadavatele) předá profily EOS (založí přístup).
- Přidělenou roli lze pak z IDM:
 - zobrazit v Nadstavbě (kontrola),
 - upravit v Nadstavbě a následně zrušit původní roli a založit novou (upravenou),
 - zrušit bez náhrady (bez využití Nadstavby).

Zobrazení v Nadstavbě (pro kontrolu nebo úpravu) umožní uložit informace a parametry, které IDM do Nadstavby předá.

1.1 Work-flow přidání oprávnění

1.1.1 Žádost o roli/e (centrální řešení)

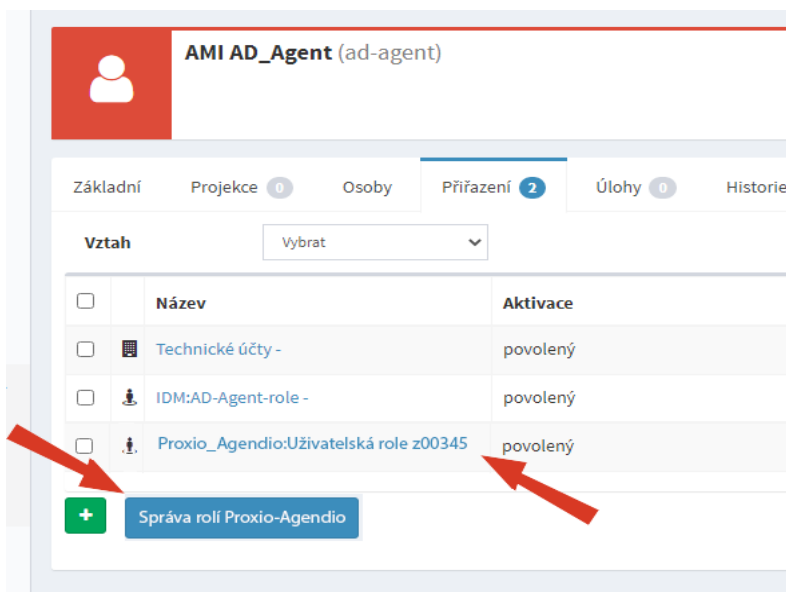
- Žádost o přístup do Proxio Agendia bude standardně započata v service desku (dále jen SD), viz. stávající uživatelská dokumentace IdM.
- Z SD bude žadatel o oprávnění, tedy vedoucí pracovník nebo ředitel (dále jen „žadatel“) standardně přesměrován do IdM (viz. stávající uživatelská dokumentace IdM).
- V košíku bude doplněno nové tlačítko pro výběr uživatele pro správu rolí v Proxio Agendio (viz.
- Odkaz do Nadstavby). Odkaz otevírá okno s výpisem podřízených zaměstnanců, pro které je oprávněn žádat o roli. Jedná se o standardní okno z menu Uživatelé -> Seznam uživatelů.



Odkaz do Nadstavby

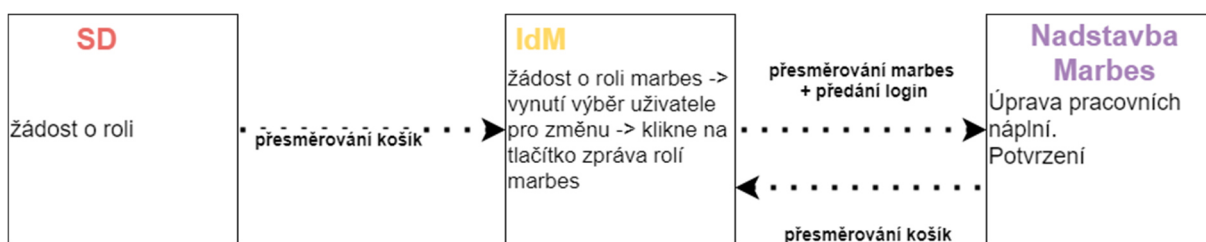
V rámci nabídky řešíme odkaz do Nadstavby formou tlačítka. Pokud se během realizace ukáže, že pracnost přípravy odkazu do Nadstavby pomocí položky v Katalogu aplikací je stejná jako příprava a interpretace prostřednictvím tlačítka, budeme preferovat řešení pomocí Katalogu aplikací.

- Po výběru konkrétního uživatele je třeba vybrat v záložce „Přiřazení“ tlačítko „Spravovat Proxio-Agendio“. Žadatel bude přesměrován do Nadstavby s vybraným uživatelem. Přesměrování probíhá v rámci původního okna prohlížeče.



Přidání role

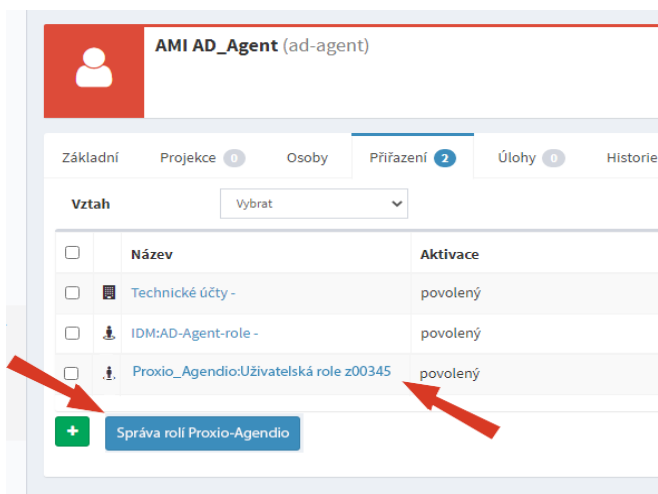
- Nadstavba zobrazí aktuálně přiřazené role uživatele(ů) a nabídne možnost změny.
- Po výběru odpovídající role a potvrzení je uživatel navrácen do nákupního košíku v IdM.



- Po potvrzení bude žádost standardně zpracována – např. schvalování, po schválení budou v systému Proxio Agendio přiděleny příslušné profily a v záložce „Přiřazení“ je doplněna odpovídající role.

1.1.2 Žádost o roli/e (hostované řešení)

- V menu IdM Uživatelé je třeba vybrat uživatele, kterému chceme roli přiřadit.
- Po výběru konkrétního uživatele je třeba vybrat v záložce „Přiřazení“ tlačítko „Spravovat Proxio-Agendio“. Žadatel bude přesměrován do Nadstavby s vybraným uživatelem. Přesměrování probíhá v rámci původního okna prohlížeče.



Přidání role

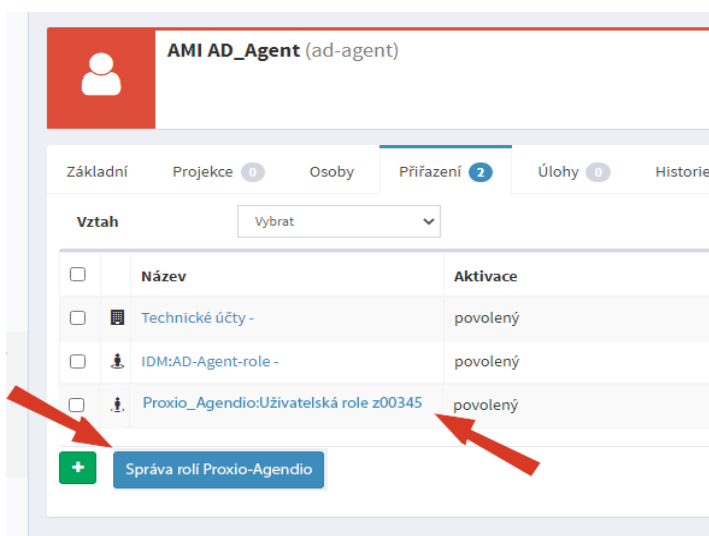
- Nadstavba zobrazí aktuálně přiřazené role uživatele(ů) a nabídne možnost změny.
- Po potvrzení bude žádost standardně zpracována, v systému Proxio Agendio budou přiděleny příslušné profily a v záložce „Přiřazení“ je doplněna odpovídající role.

1.2 Odebrání/úprava role/í

1.2.1 Odebrání role/í (centrální řešení)

Návrh počítá s následujícím řešením:

- Žádost o přístup do Proxio Agendio bude standardně započata v SD (viz. stávající uživatelská dokumentace IdM).
- Z SD bude žadatel o oprávnění standardně přesměrován do IdM (viz. uživatelská dokumentace IdM).
- Po výběru konkrétního uživatele v záložce „Přiřazení“ může žadatel odebrat roli Proxio Agendio, čímž dojde ke zrušení přístupu. Úpravu role lze realizovat pomocí tlačítka „Spravovat Proxio-Agendio“. Žadatel bude přesměrován do Nadstavby s vybraným uživatelem. Přesměrování probíhá v rámci původního okna prohlížeče. Při volbě smazání následuje poslední krok.



Odebrání role

- Nadstavba zobrazí aktuálně přiřazené role uživatele(ů) a nabídne možnost změny.
- Po odstranění/změně odpovídající role a potvrzení je uživatel navrácen do nákupního košíku v IdM.
- Po potvrzení bude žádost standardně zpracována – např. schvalování, po schválení budou v systému Proxio Agendio odebrány příslušné profily a v záložce „Přiřazení“ je odstraněna odpovídající role.

1.2.2 Odebrání role/í (hostované řešení)

- V menu IdM Uživatelé je třeba vybrat uživatele, kterému chceme roli odebrat.
- Po výběru konkrétního uživatele v záložce „Přiřazení“ může žadatel odebrat roli Proxio Agendio, čímž dojde ke zrušení přístupu. Úpravu role lze realizovat pomocí tlačítka „Spravovat Proxio-Agendio“. Žadatel bude přesměrován do Nadstavby s vybraným uživatelem. Přesměrování probíhá v rámci původního okna prohlížeče. Při volbě smazání následuje poslední krok.

AMI AD_Agent (ad-agent)

Základní Projekce 0 Osoby **Přiřazení 2** Úlohy 0 Historie

Vztah Vybrat

<input type="checkbox"/>	Název	Aktivace
<input type="checkbox"/>	Technické účty -	povolený
<input type="checkbox"/>	IDM:AD-Agent-role -	povolený
<input type="checkbox"/>	Proxio_Agendio:Uživatelská role z00345	povolený

+ Správa rolí Proxio-Agendio

Odebrání role

- Nadstavba zobrazí aktuálně přiřazené role uživatele(ů) a nabídne možnost změny.
- Po potvrzení bude žádost standardně zpracována a v systému Proxio Agendio, budou odebrány příslušné profily a v záložce „Přiřazení“ je odstraněna odpovídající role.

1.3 Změny v IdM rozhraní

1.3.1 Košík (centrální řešení)

V seznamu systémů se nebude vyskytovat systém Proxio Agendio ani jeho moduly, místo toho na obrazovce košíku bude tlačítko „Proxio-Agendio“.

☰ Žádost o přiřazení

Zobrazení katalogu rolí Cílový uživatel: já Proxio - Agendio

Katalog rolí

- Katalog rolí
 - Bezpečnostní řešení
 - Centrální informační systémy veřejné správy
 - Ekonomické aplikace
 - Mapové služby
 - Portálové aplikace
 - Správa a hospodaření s majetkem
 - Správní a samosprávní řízení
 - Řízení dokumentů a spisová služba
 - Ostatní

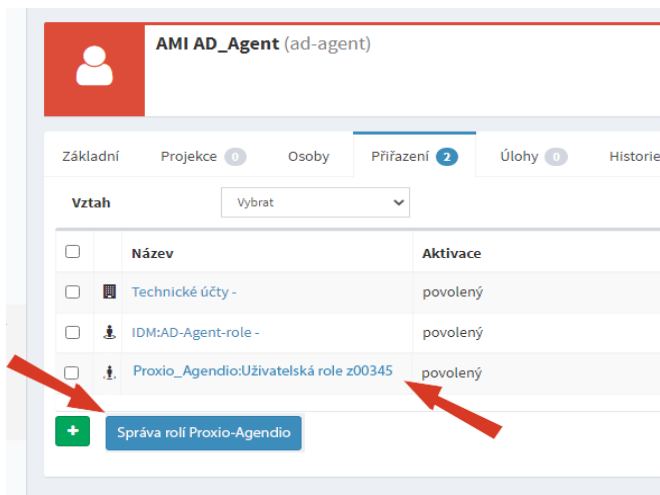
WEBGIS_PRAHA:Kryty CO
pasport krytů civilní obrany

Vlastnosti + Přidat do košíku +

1.3.2 Profil uživatele – záložka přiřazení

V záložce vedoucí/administrátor/bezpečnost uvidí, že uživatel má nebo nemá přiřazenou roli „Proxio-Agendio:Uživatelská role – os.číslo“. Volitelně po rozkliknutí může vidět, co uživatel má aktuálně v EOS za profily a v Nadstavbě za pracovní náplně.

Dále zde bude tlačítko „Správa rolí v Proxio-Agendio“. Po kliknutí dojde k přesměrování na Nadstavbu s předvolbou vybraného uživatele.



1.4 Funkcionalita v pozadí

1.4.1 Vytváření žádosti pro SD

IdM bude „odchytávat“ změnu role „Proxio-Agendio:Uživatelský přístup XY“, na základě které vytvoří SD standardní ticket obsahující v popisu konkrétní obsah pracovních náplní.

SD ticket se bude vytvářet na základě změny personální role pro Proxio Agendio, nikoliv klasicky po přiřazení role.

1.4.2 Historie pracovních činností v rámci Proxio Agendio

IdM bude k uživateli zapisovat historii změn v rámci tohoto systému ve formátu: „Přidání/odebrání pracovní činnosti XY: Datum: zadavatel“. Historie bude k dispozici specialistům/managerům bezpečnosti a administrátorovi.

1.4.3 Po schválení nové role

Po schválení nové role dojde ke smazání původní role ze systému, nicméně uživateli bude obsah role zapsán do historie. Nová role pak nahradí roli původní.

1.5 Technologie

K předávání dat z IdM midPoint do Nadstavby bude využito protokolu http, kde dojde k předání parametru login pomocí url linku nebo post volby (JSON).

Ke komunikaci ve směru Nadstavba -> IdM bude využito technologie REST a rozhraní systému IdM midPoint.

1.5.2 Přesměrování do Nadstavby

Do Nadstavby je z IdM možno přesměrovat klasicky odkazem s tím, že jako parametr za „?“ by byl předán „login=xy“, nebo metodou post s přiloženou informací ve formátu XML nebo JSON.

1.5.3 Nadstavba - načtení

- Po přesměrování by pro GET vstupní stránky mělo dojít k dotazu Nadstavby prostřednictvím rest na vlastnictví role „Proxio-Agendio:Uživatelský přístup XY“. Pokud je role přiřazena, dojde k volání detailu přiřazení role a v tomto detailu budou uvedeny pracovní náplně, které má uživatel původně přiřazeny.
- Na základě získaného detailu Nadstavba vyplní zobrazovaný obsah.

1.5.4 Nadstavba - potvrzení

Poté co uživatel potvrdí nový rozsah oprávnění, dojde k následujícím akcím:

- Nadstavba připraví finální seznam pracovních náplní a profilů, které mají být přiděleny (za předpokladu, že je informace k dispozici již nyní).
- Pokud Nadstavba vyhodnotí změnu proti původně načtenému (popřípadě znova zavolá detail přiřazení role) i v rámci profilů, zavolá nové vytvoření role s parametry obsahujícími seznam pracovních náplní a profilů, pokud se aktuální stav neshoduje s navoleným.

Etapa 2: Aplikace selfservice pro městské části - aplikace pro správu hesel

2.1 Změn hesla pro uživatele MČ

MHMP má za cíl zpřístupnit systém i na úrovni hostovaného řešení – MČ a přidružených organizací (viz předaná Dokumentace skutečného provedení). Momentálně změna hesla u MČ probíhá skrze IdM, nicméně přidružené organizace do sítě mepnet nemají přístup, a tak je zde tendence použít tento univerzální nástroj, viditelný ze sítě vnější.

2.2 Reset zapomenutého/expirovaného hesla

V případě, že uživatel heslo zapomene, je nutné, aby v případě MČ přistoupil do IdM a tam využil možnosti zaslání možnosti resetu hesla na svojí e-mailovou adresu. V případě přidružených organizací je nutné kontaktovat správce za MHMP.

2.3 Požadované řešení

2.3.1 Aplikace Self-service

Řešení zakládá na architektuře a aplikaci vytvořené již v rámci CHR24, nicméně pro účely MČ a přidružených organizací bude zřízena nová instance aplikace Self-Service, s vlastním aplikačním serverem a databází. Databáze nové instance aplikace Self-Service bude integrována s IdM pro MČ a MO.

Důvody pro toto řešení jsou následující:

- **Architektura**
 - Identity MČ a MO jsou **primárně řízeny v IdM MČ a MO** (IdM Host), které propaguje změněná hesla do dalších systémů.
 - Je žádoucí, aby v IdM pro MČ a MO byly veškeré auditní záznamy o změnách v identitách MČ a MO.
 - Zadavatel počítá s oddělením Active Directory (AD) pro MČ a MO od AD pro Zadavatele. Do AD zapisuje hesla uživatelů MČ a MO IdM Host. Zvolené řešení umožní zpřístupnit nové AD pro MČ a MO jen pro IdM Host, nebude muset existovat propojení Centrálního IdM s AD pro MČ a MO.
 - IdM pro MČ a MO má informace o použitých heslech uživatelů MČ a MO.
- **Optimalizace zátěže**
 - Rozdělení synchronizačních úloh mezi aplikacemi Self-Service a IdM.
 - Rozdělení bezprostřední zátěže na aplikace Self-Service.
 - Případný problém na jedné instanci nebo její synchronizaci s IdM neovlivňuje instanci druhou.

2.3.2 Napojení IDM Host na novou aplikaci Self-Service

Pro aplikaci bude zřízeno za použití již vytvořeného konektoru napojení, které bude nakonfigurováno vůči nově zřízené aplikaci v rozsahu údajů využitých i pro řešení Zadavatele.

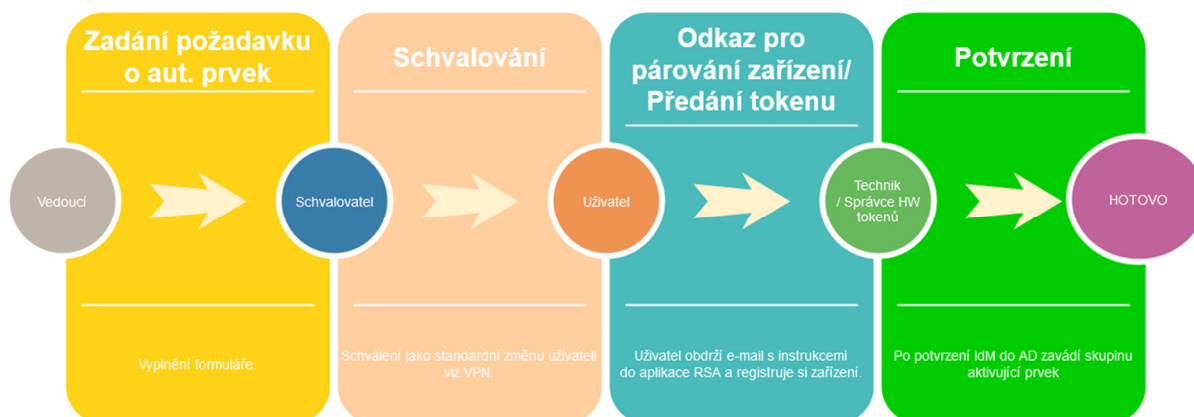
K napojení bude vytvořena synchronizační úloha a nastavena tvorba účtů v aplikaci pro všechny uživatele.

Etapa 3: Integrace více faktorové autentizace

3.1 Funkční požadavky řešení na IDM

- Zadání požadavku pro tvorbu autentizačního prvku pro uživatele v IDM.
- Schvalování požadavku pro tvorbu autentizačního prvku v SD/IDM.
- Zaslání instrukcí pro napárování/aktivaci mobilního zařízení jako autentizačního prvku.
- Předání informace o aktivní žádosti a potvrzení předání/aktivaci autentizačního prvku.

3.2 Zapojení IDM do workflow VFA



3.3 Formulář Pro žádost o aut. Prvek V IDM

Formulář uživatele bude obsahovat nové pole „autentizační prvek“.

V poli bude možno žádat až o dva autentizační prvky. Výběr bude proveden za pomoci našeptávače číselníku. Číselník bude obsahovat hodnoty „mobilní zařízení“ a „HW token“.

Hodnoty bude možno vyplnit v profilu uživatele v IDM. K dispozici bude také při tvorbě nového externisty.

Vedoucí pracovník bude toto pole moci změnit v profilu svých podřízených interních i externích zaměstnanců. Množina podřízených zaměstnanců se vždy standardně řídí organizační strukturou v IdM.

Zrušení autentizačního prvku bude moci vedoucí pracovník provést odebráním prvku z formuláře.

3.4 Schvalování

Po zadání žádosti o autorizační prvek vedoucím zaměstnancem je žádost odeslána pod hlavičkou „Změna uživatele“ ke schválení řediteli daného odboru/sekce dle původu žadatele (podle organizační struktury v IdM) standardní cestou prostřednictvím service-desk.

V ticketu samotném bude uvedeno, že se jedná o změnu atributu a jeho hodnota. Odebrání prvku nebude předmětem schvalování.

3.5 Zaslání podkladů pro fyzickou aktivaci tokenu

Schválený požadavek bude automaticky zpracován a na jeho základě IdM dle typu žádosti vygeneruje e-mailové notifikace.

- SW/HW Token:
 - Service-desk CORPUS žádost o tvorbu tokenu (na základě dodané šablony od MHMP/CORPUS).
 - Správce tokenů/Technika o vzniklé žádosti (na základě dodané šablony od MHMP).
- Mobilní zařízení:
 - Uživatel, pro kterého je žádáno, je zaslán odkaz na adresu pro aktivaci zařízení jako autentizačního prvku (na základě dodané šablony od MHMP/dodavatel RSA).
 - Správce tokenů/Technika obdrží informaci o vzniklé žádosti (na základě dodané šablony od MHMP).

Zároveň je uživateli v systému AD přiřazena skupina „MFA MT-install“ nebo dle specifikace „MHMP/CORPUS“.

V případě odebrání prvku je na Správce tokenů/Technika zaslána notifikace o zrušení (dle specifikace MHMP). Zároveň dojde k odebrání skupin v AD skupina „MFA MT-install“ a „MFA MT“.

Předpokladem je tvorba role Správce tokenů/Technika a dodání seznamu členů této role ze strany MHMP.

3.6 Potvrzení z RSA o aktivaci tokenu

Systemy help-desk Corpus a RSA po potvrzení/vystavení autentizačního prvku zašlou pomocí rozhraní REST do IDM informaci o dokončeném vytvoření tokenu.

Přesný tvar REST požadavku a dedikovaný technický uživatel v IDM pro tento krok/ zapsání změny bude součástí dodaného řešení ze strany IDM. Dodavatel RSA/Service-Desk by měl na své straně zároveň ověřit zapsání změny prostřednictvím dalšího dodaného dotazu. Potažmo v případě nedostupnosti do IdM zapsat znovu.

Pro potvrzení bude dedikován meta atribut nesoucí informaci o přiděleném prostředku.

Informace o potvrzení/aktivaci tokenu bude notifikovat uživatele dle členství v roli Správce tokenů/Technik dle dodané šablony ze strany MHMP.

Na základě potvrzení IDM přiřadí v AD uživateli skupinu „MFA MT“ a tím aktivuje token.

Etapa 4: Integrace aplikace Zahraniční služební cesty

4.1 Napojení Koncového systému

- Napojení systému bude realizováno prostřednictvím SQL připojení do databáze vystavené na straně dodavatele systému.
- Realizace bude prostřednictvím připravených procedur a pohledů na aktuální data.
- Napojení bude realizováno v entitním rozsahu – organizační jednotka, funkční místo, uživatel, zastupitel, zástup – delegace, zástup - částečná delegace a zástup – dočasné pověření řízení s vzájemnou vazbou.
- Rozsah přenášených atributů je dán ze strany Dodavatele a připraveného schváleného DB rozhraní.
- Jako zdroj identifikátorů bylo navrženo IDM.
- Součástí nabídky je dokumentace v rozsahu DSP předchozích systémů.

4.2 Nadstandardní položky

Přenos částečné delegace bude nutné „odchytávat“ a v IdM reprezentovat jako entitu přenositelnou do dalších systémů. Bude se jednat pouze o delegaci obsahující oprávnění směrem do systému ZSC.

Etapa 5: Úprava systému pro robustní kontrolu duplicit identit

Důvodem změny je získat přehledný přístup k informaci, zda-li v systému existuje osoba se shodným jménem a příjmením během zadání s uvedenou kontaktní osobou pro bližší informaci. Duplicitně zadaný zaměstnanec z autoritativního zdroje (FLUX), někdy zůstává aktivní delší dobu, o tomto je třeba automaticky okamžitě informovat a žádat nápravu.

Cílem je Rozšíření procesu kontroly duplicitních identit o kontrolu na základě shody jména a příjmení. Systém zobrazí existující identity, aby došlo k jasnému rozlišení, zda-li jde o stejnou osobu. Následně uživatel potvrdí, že jde o novou identitu. Systém pohlíká i zadání interních uživatelů na úrovni shody: jméno příjmení, email. Detailnější specifikace uvedené změny je následující:

5.1 Rozšíření kontrolního mechanismu při zadávání uživatele

V případě existující kombinace jméno+příjmení systém zobrazí upozornění a vypíše shodné uživatele s atributy existujícího uživatele/uživatelů. Kontrola bude probíhat proti všem existujícím identitám v IdM:

Text upozornění – informační hláška, jako příklad (finální formulace bude součástí návrhu realizace):

„V systému existují následující účty se shodným jménem a příjmením <Jméno Příjmení>:“ <Login>, <e-mail>, <Společnost> (v případě externisty), „Vedoucí:“ <Příjmení vedoucího>, <zkr. Oddělení/Odbor>, <tel. č.>.

Obrázek 1: Ilustrace zobrazení upozornění. Konkrétní text může být upraven.



Výpis bude v prostém textu s využitím běžných oddělovačů (čárky, pomlčky, závorky apod.), výpis není možné formátovat do podoby tabulky.

Pokud nejde o duplicitní účet, hláška obsahuje návodnou informaci:

„klikněte na tlačítko "Pokračovat v editaci" a ve formuláři vyberte u položky "Provedena kontrola duplicit" hodnotu "Ano"“.

Obrázek 2: Ilustrace zobrazení potvrzení o vykonání kontroly.



Po zobrazení chyby bude možné vrátit se do formuláře a potvrdit „Provedena kontrola duplicit, účet vytvořit“ (výběr ANO/NE). Po nastavení atributu na „ANO“ IdM umožní tvorbu osoby.

Potvrzení, že žadatel prohlašuje, že vytvářená identita není duplicitou bude uvedena v schvalovacím kroku založení externího účtu a bude tedy také předmětem schvalování.

Příklad textu:

„Žadatel potvrdil, že ač v systému existují účty se shodným jménem a příjmením, jde o jinou osobu.“

5.2 Kontrolní mechanismus interních zaměstnanců

Po zadání duplicitního, údaje v FLUX HR – definovaného jménem, příjmením, e-mailem – IdM účet nevytvoří a zašle notifikaci na věcného a technického garanta FLUX, potažmo ředitele HR s chybou. Účet bude vytvořen následně po korekci e-mailu na straně jedné, nebo duplicita na straně FLUX bude odstraněna a účet tedy nevznikne.

Příklad textu:

„Systém IdM zjistil shodu kombinace jméno,příjmení,email u účtu m000xxxxx, tento účet již existuje jako m0000xxxxx. Pokud jde o správně zadaný záznam, bude nutné znovu přidat unikátní e-mail. IdM následně identitu automaticky založí v rámci nočního přepočítání.“

5.3 Kontrola již existujících dat

Již existující záznamy se shodnou kombinací „jméno“ + „příjmení“, případně „email“ je možné získat pomocí reportu se seznamem uživatelů a provést ruční zásah. Duplicitní záznam je možné vyřešit opravou dat nebo deaktivací jednoho z účtů.

Příloha č.1, část (C): Systémová podpora

1 SPECIFIKACE PROVOZNÍ PODPORY

V případech, kdy Dodavatel v rámci poskytování Služeb (Service level Agreement, SLA), jejichž předmět je smluvně vymezen příslušným Katalogovým listem, nedosáhne stanovené (dohodnuté) úrovně plnění během vyhodnocovacího období, vzniká tímto Objednateli nárok na jednorázovou slevu z ceny za Služby pro dané vyhodnocovací období. Za nedosažení stanovené (dohodnuté) úrovně plnění se nepočítá doba plánované odstávky dané Služby. Výše jednorázové slevy bude stanovena dle příslušného SLA parametru, který byl porušen, a dle úrovně porušení (specifikovaná jednotlivě pro každý SLA parametr).

V případě, že dojde k nedodržení více dílčích SLA parametrů v rámci jedné Služby, platí, že sleva z ceny se uplatní ke všem nedodrženým dílčím SLA parametrům.

1. OBECNÉ PARAMETRY SLUŽEB

Ustanovení jsou platná pro všechny KL, pokud není v KL stanoveno jinak.

a) Vazby na platnou legislativu

Poskytování Služeb musí být ve shodě s legislativním prostředím, které jejich provoz, resp. dílčí provozy dotčené Službami, upravuje.

Poskytovatel zajistí, že v rámci správy a rozvoje svěřeného prostředí bude tyto předpisy respektovat a bude v rámci poskytování Služeb sledovat změny příslušných právních předpisů a bez zbytečného odkladu upozorňovat Objednatele na zjištěný nesoulad.

Poskytovatel bude tato zjištění prezentovat a v součinnosti s Objednatelem následně realizovat prostřednictvím Objednávkových služeb.

b) Úplnost poskytovaných služeb

Součástí Služeb poskytovaných dle každého KL je také poskytování činností, jež svým předmětem spadají pod Služby poskytované na základě tohoto KL a jejichž poskytování je současně nezbytné pro naplnění účelu takto poskytovaných Služeb, a to i v případech, kdy tyto činnosti nejsou v KL konkrétně vyjmenovány. Součástí Služeb poskytovaných dle každého z KL je dále poskytování Služeb dle KL s přihlédnutím ke změnám vyvolaným vývojem technologií. Za tímto účelem Poskytovatel zajistí Objednateli plnou funkčnost Služby dle příslušného KL, a to i v případech, kdy dojde ke změně jako např.:

- změna verzí operačních systémů nebo standardních softwarů,
- vydání nové verze technologických standardů, dle nichž je Služba poskytována,
- v případě ekvivalentní obměny zařízení z důvodu náhrady vadného prvku.

V rámci úplnosti poskytovaných Služeb Poskytovatel poskytuje i níže uvedené služby, které nemusí být jmenovitě uvedeny v jednotlivých KL. Činnosti jsou prováděny dle uvedených periodicit, pokud není v jednotlivých KL uvedeno jinak:

- udržování aktuálního stavu SW zejména z pohledu možných bezpečnostních a funkčních hrozeb, tj. aplikace aktualizací (hotfix, patch, servicepack), a to v souladu s Release management procesem a plánem patchování schváleným Objednatelem (roční báze),
- předložení návrhu opatření a postupu implementace opravného balíku ke schválení Objednavatelem (roční báze),
- komunikace s výrobcem nebo dodavatelem poskytujícím softwarovou nebo hardwarovou podporu v rozsahu maintenance smluvně zajištěné Objednatelem,
- poskytnutí součinnosti Objednavateli (nebo jím jmenovaných subjektů) při návrhu a realizaci monitoringu prostředí.

V rámci Služeb Poskytovatel nezajišťuje migraci hardware či instalace nových verzí software. Tyto činnosti budou řešeny v rámci Objednávkových služeb.

c) Vazby na ostatní procesy podpory IT

Mimo služby, které jsou definované v KL podle této Smlouvy, zahrnují procesy správy, podpory a rozvoje IT prostředí i další procesy, práce a služby poskytované jak interními pracovníky Objednatele, tak jinými Poskytovateli Objednatele podle ustanovení jiných smluv.

Poskytovatel bude v případě potřeby řešení úkolů s přesahem mimo definici podle KL poskytovat součinnost Objednateli, a to především v oblastech:

- koordinace procesů správy a řízení IT prostředí (ITSM, ISMS, ITIL, PRINCE2 apod.),
- poskytnutí informace nebo dokumentace,
- umožnění přístupu k technologii,
- součinnost při testech funkčnosti systému po plánovaných zásazích Objednatele nad infrastrukturou,

- součinnost a účast při provádění testů systému po provedení změn (např. po opravách chyb systému, během změny nebo před nasazením nových funkcionalit systému) před jeho nasazením do provozu, zejména v přípravě a vyhodnocování požadovaných simulovaných situací a dat pro účely testování,
- poskytování součinnosti při integraci jiných systémů,
- poskytování součinnosti s dodavatelem zajišťujícím rozvoj.

Poskytovatel může odmítnout poskytnutí součinnosti v případě, kdy by došlo k:

- kompromitaci informační bezpečnosti,
- porušení závazných právních předpisů a interních řídicích dokumentů Objednatele,
- narušení primární funkce dotčeného systému dle této Smlouvy,
- jinému ohrožení provozu systémů a služeb podle KL.

V případě pochybností nebo sporu určuje oprávněnost požadavku na součinnost Objednatel.

d) Centrální nástroje řízení IT služeb

Objednatel provozuje nástroje pro podporu provozu a řízení IT prostředí. Poskytovatel bude mít k těmto nástrojům přístup a je povinen je používat ve smyslu jejich účelu. Jedná se zejména o systémy:

- Provozní dohledové systémy,
- Bezpečnostní dohledové systémy*,
- ServiceDesk,
- Centrální konfigurační databáze (CMDB)*,
- a jiné stanovené Objednatelem.

Nástroje, které ke dni podpisu Smlouvy nejsou Poskytovateli k dispozici, jsou označeny * výše v textu.

Požadavky typu D budou v ServiceDesku Objednatele, kdy žadatel je Objednatel nebo v jiném systému stanoveném Objednatelem.

e) Periodické činnosti

Periodické činnosti se definují tak, že se jedná o činnosti, které je pro zajištění řádného provozu systému nutno vykonávat opakovaně, a to s definovanou periodou. Termín vykonání činností si může Poskytovatel určit podle svých provozních potřeb tak, aby časový odstup mezi činnostmi nepřekročil uvedenou periodu.

Pro vyloučení pochybností a upřesnění se uvádí:

- je-li činnost v KL definována jako „roční báze“, musí být vykonána minimálně jednou za rok, nejdříve však 3 měsíce od předchozí,
- „kvartální báze“ znamená činnost minimálně jednou za 3 měsíce, nejdříve však 1 měsíc od předchozí,
- „měsíční báze“ znamená činnost minimálně jednou měsíčně, nejdříve však po 14 dnech od předchozí,
- „týdenní báze“ znamená činnost minimálně jednou za týden, nejdříve však po 3 dnech od předchozí,
- „denní báze“ znamená činnost minimálně jednou za pracovní den.

Periodické činnosti mohou zahrnovat:

- kontrola logů,
- zálohování konfigurací,
- kontrola funkcionality,

- kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíčků výrobce a doporučení na nasazení patchů, hotfixů a service packů.

Seznam periodických činností je vždy určen dokumentací k dané službě.

f) Dokumentace

Poskytovatel udržuje a aktualizuje dokumentaci systémů a služeb podle definice ve smlouvě, pokud KL nestanoví jinak. Dokumentace zahrnuje zejména, nikoliv však výhradně, následující položky:

- hlavní komponenty IS na úrovni celků, na které lze aplikovat změnu ve smyslu metodiky ITIL,
- veškeré licence včetně volně šiřitelných a neplacených licencí,
- popisy vazeb mezi komponentami IS na úrovni datové, logické, fyzické,
- uživatelskou dokumentaci,
- bezpečnostní dokumentaci,
- administrátorskou dokumentaci,
- postupy pro provoz a správu IS,
- zálohovací plány a postupy,
- seznamy použitých softwarových komponent a standardního SW včetně určení jejich verzí,
- konfigurační databázi (CMDB),
- adresní plán,
- provozní deník,
- katalog periodických činností určených jednotlivými KL.

Elektronická dokumentace je ukládána do sdíleného datového úložiště určeného Objednatelem.

Písemná dokumentace

Po provedení změny na systémech publikuje Poskytovatel novou verzi dokumentace nejpozději 14 dní od ukončení prací, pokud KL nestanoví jinak.

Dokumentace je revidována a publikována v nové verzi po uplynutí maximálně 6 měsíců od poslední revize, nemá-li Poskytovatel důvod vydat novou verzi dříve z důvodu zásadní změny nebo pokud není stanoveno v KL jinak.

Toto ustanovení o vydávání dokumentace platí i v případě, kdy na systémech a/nebo službách nedošlo ke změnám. V takovém případě bude v seznamu změn uvedeno, že nedošlo ke změnám.

Dokumenty mají v úvodní sekci seznam změn, ve kterém jsou stručně shrnuty změny provedené od předchozího vydání dokumentace.

g) Datový popis infrastruktury - CMDB

Objednatel provozuje konfigurační databázi (CMDB) obsahující data o IT infrastruktuře.

Formát, rozsah a způsob předávání dat (databází) je předmětem dohody Poskytovatele s Objednatelem.

h) Provozní deník

Poskytovatel je povinen při poskytování Služeb dle této Smlouvy využívat Provozní deník Objednatele.

Zaznamenávané skutečnosti

Poskytovatel je povinen do Provozního deníku zaznamenat minimálně následující skutečnosti:

- záznam o provedení úkonů předepsaných v KL včetně identifikace příslušného KL a zdůvodnění, na základě jakého požadavku (např. ID záznamu v SD Objednatele),
- druh změny konfigurací a systémového nastavení,
- výkon pravidelných kontrol.

Obsah záznamu do Provozního deníku

Každý záznam v Provozním deníku obsahuje minimálně následující informace:

- datum a čas pořízení záznamu,
- identifikace osoby pořizující záznam,
- popis události.

Pro vyloučení pochybností se uvádí, že Provozní deník není systémovou dokumentací. Provozní deník je chronologicky uspořádán, při realizaci změny se do Provozního deníku zapisuje její provedení a její stručný popis. Popis změny, resp. nově vzniklý stav a konfigurace systému, je detailně uveden v systémové dokumentaci. Pro vyloučení pochybností se uvádí, že změnou se myslí jakákoliv změna ve smyslu „Change management“ podle metodiky ITIL.

Poskytovatel je povinen při vedení Provozního deníku využít elektronické nástroje Objednatele, do nichž zajistí Objednatel Poskytovateli přístup.

Objednatel připouští vedení jednotného Provozního deníku pro všechny KL.

i) Výkazy práce

Poskytovatel je povinen při poskytování Služeb dle této Smlouvy vést záznamy o provedených pracích, včetně těch, které byly provedeny v souvislosti se Smlouvou a nejsou předmětem záznamu v Provozním deníku. Příkladem může být účast na jednání, zpracování dokumentu na vyžádání Objednatele, úprava dokumentace apod.

Výkaz práce je předáván Objednateli v rámci reportingu Vyhodnocovacího období.

Obsah záznamu

Každý záznam Výkazu práce specifikuje činnosti vykazované Poskytovatelem a obsahuje minimálně následující informace:

- datum provedení činností,
- identifikaci osoby, která činnosti vykonala,
- stručný popis provedených činností.

j) Plány řešení závažných situací

Za závažné situace se považují úplná selhání a situace pokryté procesy Business Continuity a Disaster Recovery.

Poskytovatel vypracuje plány BCP (Business Continuity plan) a DRP (Disaster recovery plan) takto:

- plány zahrnují činnosti potřebné k obnově provozu Poskytovatele,
- plány zahrnují činnosti potřebné k obnově provozu svěřených systémů (IDM a integrační vazby IDM, nikoliv koncové systémy),
- plány jsou vypracovány v součinnosti s Objednatelem s cílem zajistit vzájemnou součinnost v případě závažné situace.

Rozsah plánů a testování účinnosti a úplnosti těchto plánů je stanoven na základě dohody mezi Poskytovatelem a Objednatelem v rámci Objednávkových služeb.

k) Odstávky

Standardní odstávky jsou odstávky plánované na základě návrhu, který předkládá Poskytovatel Objednateli anebo na základě požadavku Objednatele. Odstávky se týkají zejména nasazování nových verzí, profylaktických prohlídek a dalších služeb uvedeného v KL. Požadovaný termín a rozsah odstávky předkládá Poskytovatel Objednateli vždy nejméně 14 kalendářních dnů do SD Objednatele, pokud není stanoveno jinak.

Standardní odstávka je možná pouze se souhlasem Objednatele. Objednatel se zavazuje, že svůj souhlas nebude bezdůvodně odírat. Pokud nebude souhlas udělen ve vztahu ke konkrétnímu termínu, není Poskytovatel oprávněn takovou odstávku provést a Objednatel je povinen bezodkladně navrhnout nový termín pro provedení odstávky.

Objednatel má právo zrušit standardní odstávku nejpozději do 24 hodin před jejím plánovaným uskutečněním, a to v případě, že by tato odstávka mohla ohrozit provoz systémů Objednatele. O tomto bude Objednatel informovat Poskytovatele emailem s využitím k tomu určených kontaktních osob nebo jiným domluveným způsobem.

Kritické odstávky jsou zejména odstávky vzniklé v důsledku nezbytnosti řešit bezpečnostní incidenty a s tím spojené nasazení bezpečnostních záplat, řešení možných problémů s integritou dat, zajištěním důvěrnosti dat, jejich dostupností apod. Informace o provedení kritické odstávky předkládá Poskytovatel Objednateli s využitím SD Objednatele a emailem na kontaktní osobu Objednatele, a to neprodleně.

Odpovědnost za vložení návrhů na uskutečnění odstávek do SD Objednatele má Poskytovatel. V případě požadavku na odstávku ze strany Objednatele je odpovědnost za vložení návrhů na uskutečnění odstávky do SD Objednatele u Objednatele.

l) Bezpečnostní incident

V případě identifikace bezpečnostního incidentu je Poskytovatel povinen oznámit tuto skutečnost Objednateli. V případě řešení incidentu se Poskytovatel řídí pokyny Objednatele a jeho služby jsou následně vykazovány a objednány dle Objednávkových služeb.

m) Součinnost Objednatele nezbytná pro poskytování Služeb Poskytovatelem

Součinnost Objednatele je Poskytovatelem požadována pouze v míře nezbytné pro provoz Služeb. Součinnost Objednatele v rámci provozu Služeb bude spočívat především v následujících činnostech:

- Zajištění přístupu do objektů Objednatele, které mají spojitost s plněním Smlouvy, pro členy realizačního týmu Poskytovatele.
- Zajištění přístupu do všech provozovaných systémů, jež se vztahují k provozovaným Službám, pro členy realizačního týmu tak, aby Poskytovatel mohl vykonávat všechny činnosti popsané v této Smlouvě.
- Dle potřeby a řešeného tématu zajištění účasti a součinnosti odpovědných pracovníků Objednatele při schvalování, analýzách, testování, akceptaci, školeních apod.
- Jmenování kontaktních osob Objednatele.
- Poskytování informací o ostatních projektech v daném prostředí, pokud budou mít jakýkoli vliv na plnění závazků Poskytovatele z této Smlouvy.
- Zajištění součinnosti třetích stran, které jsou v přímém smluvním vztahu s Objednatelem, a to v rozsahu nezbytném pro plnění závazků Poskytovatele.
- Zajištění součinnosti třetích stran, které nejsou v přímém smluvním vztahu s Objednatelem, avšak jejichž činnost se přímo i nepřímo může dotýkat plnění dle této Smlouvy, pokud bude tato součinnost nezbytná pro plnění závazků Poskytovatele.
- Zajištění dostatečné kapacity a dostupnosti systémů/serverů/zařízení nebo částí informačních systémů ve vlastnictví Objednatele, které jsou nezbytné pro řádné a bezproblémové poskytování Služeb Poskytovatelem dle dohodnutých SLA, a to po předchozím odsouhlasení a na náklady Objednatele, pokud není v této Smlouvě stanoveno jinak. Poskytovatel bude pravidelně předkládat požadavky na tyto kapacity dle plánu rozvoje a plánovaných změn provozovaných systémů. Jestliže v důsledku nedodržení této součinnosti Objednatele dojde k nedodržení parametrů SLA příslušné Služby ze strany Poskytovatele, není Objednatel oprávněn uplatnit sankci ve vztahu ke Službám, jež byly tímto nedodržením součinnosti Objednatele ovlivněny.
- Poskytnutí licenčních podmínek stávajícího software Objednatele, jenž je Poskytovatel povinen při poskytování Služeb zohlednit.

2. KLASIFIKACE VAD A SLA, MĚŘENÍ SLA

1. Kvalita Služeb, jež jsou poskytovány na základě této Smlouvy, je sledována prostřednictvím parametrů SLA. Konkrétní parametry SLA, které mají Služby naplňovat, jsou vymezeny v katalogových listech.
2. K nežádoucímu narušení kvality poskytování jednotlivých služeb dochází událostmi, které se projevují jako nedostupnost (rozsáhlý výpadek) nebo jiné narušení (dílčí výpadek či závada) hardware, služeb IS a koncového zařízení pro uživatele. Tyto události jsou dále souhrnně nazývány výpadky provozu Služeb poskytovaných dle jednotlivých katalogových listů (dále jen „**Výpadky**“).
3. Výpadky jsou monitorovány a zaznamenávány systémy automatizovaného dohledu Objednatele a/nebo identifikovány uživateli, pracovníky Poskytovatele nebo jinými oprávněnými osobami. V obou případech jsou výpadky hlášeny pracovišti dispečinku, které je eviduje a spravuje ve formě incidentů s cílem obnovení plného provozu služby nacházející se ve stavu výpadku.
4. Pokud je zjištěno úmyslné podávání nepravdivých dat a výkazů Poskytovatelem, je celé Vyhodnocovací období, ve kterém bylo toto zjištěno, považováno za nesplněné ve všech parametrech, u kterých bylo toto pochybení zjištěno.
5. Prokázání, že k nedostupnosti IS, koncového zařízení a hardware a/nebo poskytování Služeb došlo vinou vnějšího vlivu (mimo působnost Poskytovatele) nebo nesoučinností Objednatele, je povinností Poskytovatele.
6. Pokud je měření a vyhodnocování Služeb a jejich parametrů závislé na datech, jejichž dodávku zajišťuje Poskytovatel, je absence dat považována za nedodání Služby.
7. Uplatnění požadavku na slevu nemá vliv na povinnost poskytování Služeb ve sjednaných úrovních. Oprávnění požadovat slevu z ceny Služeb se nedotýká závazku Poskytovatele splnit povinnost, se kterou je v prodlení, pokud je to vzhledem k povaze předmětné Služby objektivně možné.
8. Jednotlivé kategorie incidentů jsou uvedeny v příslušných katalogových listech a jsou označeny písmeny A, B, C.
9. Požadavky jsou uvedeny v příslušných katalogových listech a jsou označeny písmenem D. Objednatel může klást požadavky, které nejsou uvedeny v KL. V případě požadavku kategorie D je čas vyřešení určen v KL nebo dohodou Objednatele a Poskytovatele zachycenou formou zápisu do SD Objednatele.

10. Měření a vyhodnocování dostupnosti služeb:

Parametry dostupnosti systému	
Dostupnost (D)	<p>Dostupností je míněna dostupnost služby v průběhu provozní doby vyhodnocovaná v rámci Vyhodnocovacího období. Do výpočtu parametru dostupnosti služeb jsou zahrnuty pouze incidenty kategorie A, incidenty kategorie B a C se do vyhodnocení celkové dostupnosti nezahrnují.</p> <p>Sjednaná doba Standardní odstávky se do výpočtu Dostupnosti Služby dle příslušného Katalogového listu nezapočítává.</p>
	<p>Dostupnost (D) dosažená v rámci Vyhodnocovacího období bude vypočtena podle vzorce uvedeného níže a aritmeticky zaokrouhlena na 1 desetinné místo:</p> $D = \frac{TS - TV - TO}{TS - TO} \times 100$ <p><i>D</i> Dosažená dostupnost v % aritmeticky zaokrouhlena na 1 desetinné místo <i>TS</i> Souhrnný provozní čas v minutách v rámci Vyhodnocovaného období. Celkový čas, po který by Služba měla být poskytována dle KL. <i>TV</i> Souhrnný čas Výpadků v rámci Provozní doby Služby v minutách. Čas je vypočten jako součet doby trvání Výpadků. Zdrojem dat je SD a monitorovací nástroj Objednatele. <i>TO</i> Souhrnný čas všech plánovaných a schválených Odstávek v rámci Provozní doby v minutách.</p>
Reakční doba na zahájení	<p>Reakční doba na zahájení označuje maximální dobu, která uplyne od okamžiku nahlášení incidentu nebo požadavku dispečinkem v SD až do okamžiku zaznamenání přijetí incidentu nebo požadavku Poskytovatelem v SD.</p>
Doba odstranění incidentu kategorie A, B, C	<p>Doba odstranění incidentu označuje maximální dobu, která uplyne od okamžiku nahlášení incidentu nebo požadavku dispečinkem v SD až do okamžiku obnovy provozu Služby. Je-li provoz Služby nahrazen náhradním řešením, je doba pro obnovu provozu Služby původním technickým řešením či jiným technickým řešením určena dohodou mezi Poskytovatelem a Objednatelem.</p> <p>Hardware pro odstranění/vyřešení kvalifikovaného incidentu/požadavku zajistí včas Objednatel. Do zajištění potřebného hardware pro zajištění odstranění incidentu jsou Poskytovateli pozastaveny lhůty určené SLA.</p> <p>Čas potřebný k odstranění závady (hardwarové nebo softwarové), kterou má odstranit smluvní strana odlišná od Poskytovatele, se do doby vyřešení incidentu nezapočítává.</p> <p>Doba odstranění se vztahuje pouze na incidenty, které jsou v implementační a customizační části IDM nebo integračních vazbách IDM, nikoliv v produktu IDM, HW či SW třetích stran.</p>
Doba vyřešení požadavku kategorie D	<p>V případě požadavku kategorie D je čas vyřešení určen dohodou Objednatele a Poskytovatele formou zápisu do SD Objednatelem. Pokud nedojde k dohodě, tak je čas vyřešení požadavku určen na 30 dní.</p>

3. DEFINICE ROZSAHU A PARAMETRŮ SLUŽEB – KL A SLA

Souhrnná tabulka:

ID KL	Označení služby	Popis služby	Typ KL
KL01 - SD	SD	Service Desk	Paušální služby
KL02 - Maintenance	MAINT	Služba maintenance	Paušální služby
KL03 - Podpora a údržba	PODUDR	Poskytování služeb podpory	Paušální služby
KL04 - ROZ	ROZVOJ	Realizace požadavků Objednatele	Objednávkové služby
SUP01	SUP	Služby 2. a 3. úrovně podpory	Parametry služby

KL01 – Služby Service Desku

OZNAČENÍ SLUŽBY	KL01 - SD	TYP KL:	Paušál
Název služby	Zajištění služeb Service Desk		
Zkrácený popis služby	Zajištění služeb monitoringu, diagnostiky a Service Desku		
Rozsah požadovaných činností			
<p>Monitoring</p> <ol style="list-style-type: none"> 1. Monitoring stavu funkčnosti systému v prostředí monitoringu Objednatele. Dodavatel je povinen přistupovat přes zabezpečený protokol HTTPS. 2. Nastavení monitoringu pro identifikaci problémového stavu a nahlášení závady na Service Desk 3. Vyhodnocení nestandardního chování <p>Diagnostika – 2. a 3. úroveň podpory v rámci Service Desku</p> <ol style="list-style-type: none"> 4. Diagnostika a identifikace závady 5. Analýza vzniklých problémů, návrh řešení a přiřazení řešitele 6. Správa a aktualizace dokumentace <p>Service Desk</p> <ol style="list-style-type: none"> 7. Zadávání a nahlášení servisů, které byly zjištěny průběžnou kontrolou a preventivní činností 8. Měsíční/kvartální Reporting ze Service Desku a Monitoringu (dle Objednatelem nastavených reportů). 9. Kontrola plnění tiketů - SLA 10. Hlášení výluk a mimořádných opatření <p>Služba – Incident</p> <p>Zajištění a vypořádání nahlášených incidentů od uživatelů podle stanovených priorit</p> <p>Služba – Požadavek</p> <p>Zajištění a vypořádání nahlášených požadavků od uživatelů podle stanovených priorit</p>			
Služby podpory			
Poskytování služeb 2. a 3. úrovně podpory dle Katalogového listu ID: SLA Služby.			
Podmínky a omezení služby			
<ul style="list-style-type: none"> • Příjem tiketů skrze SD MHMP (konfiguraci, nastavení reportů, definice způsobu zaznamenávání a školení SD MHMP zajistí v rámci své součinnosti Objednatel pro Poskytovatele). • Monitoring spokojenosti uživatelů s danou službou <p>Monitoring MHMP poskytne systém centrálního monitoringu k nastavení konfigurace.</p> <p>Service Desk Pro komunikaci se systémem Service Desk bude využito předávání informací o servisních požadavcích pomocí e-mailu ve smluvené formě – notifikace ze SD. SD notifikuje Poskytovatele o zadaném ticketu.</p>			

KL02 – Maintenance

OZNAČENÍ SLUŽBY	KL02 - Maintenance	TYP KL:	Paušál
Název služby	Zajištění služeb Maintenance		
Zkrácený popis služby	Maintenance		
Rozsah požadovaných činností			
<p>Služba maintenance obsahuje poplatek, který zahrnuje zejména poskytování nových verzí IDM a opravných patchů: (i) poskytování aktualizací a nových verzí IDM (update, upgrade, legislativní podpora); (ii) poskytování opravných patchů nutných pro bezchybný chod IDM.</p> <p>Objednatel má nárok na veškerá zlepšení a dodatky k IDM (upgrade nebo update IDM) vydané během účinnosti Smlouvy. Součástí poskytnutí těchto upgrade a update je též jejich testování a implementace u Objednatele a rozdílové školení, pokud bude potřeba s ohledem na rozsah upgrade či update.</p> <p>Update se rozumí aktualizace IDM formou opravných patchů, zohledňující většinou chyby nebo bezpečnostní mezery, které u předcházející verze nebyly známy včetně veškerých dokumentací (tj. (i) dokumentace zahrnující popis změn včetně specifikace všech možných dopadů do stávajících řešení, (ii) uživatelské a školící dokumentace, pokud taková v rámci nové verze vznikla, (iii) administrátorské a technická dokumentace zahrnující i případné bezpečnostní pokyny související s opravným balíčkem k IDM).</p> <p>Upgrade se rozumí vylepšení dosavadního IDM na vyšší výkonnost a nové funkce včetně veškerých dokumentací (tj. (i) dokumentace zahrnující popis změn včetně specifikace všech možných dopadů do stávajících řešení, instalačního manuálu a doporučení pro implementaci, (ii) uživatelské a školící dokumentace, pokud taková v rámci nové verze vznikla, (iii) administrátorské a technická dokumentace zahrnující i případné bezpečnostní pokyny související s aktualizací komponent IDM).</p> <p>Poskytovatel do 5 pracovních dnů ode dne vydání update či upgrade oznámí oprávněné osobě Objednatele uvolnění každého update i upgrade a důvod, proč k update či upgrade dochází.</p> <p>Poskytovatel je povinen do 5 pracovních dnů ode dne vydání update či upgrade zajistit jejich neomezenou dostupnost tak, aby takový update <i>aj</i> nebo upgrade byl pro Objednatele kdykoliv přístupný.</p> <p>Legislativní podpora zahrnuje úpravy IDM Poskytovatelem tak, aby IDM byl v souladu s aktuálním stavem právního řádu České republiky. Služba dále zahrnuje odbornou pomoc oprávněným osobám Objednatele v oblasti konzultací souvisejících s důsledky legislativních změn na fungování IDM, a to v rozsahu 5 člověkohodin měsíčně. Jednou člověkohodinou se rozumí práce vykonaná jedním pracovníkem Poskytovatele za dobu jedné (1) hodiny (dále jen "člověkohodina"). Služba zahrnuje návrh dočasného fungování IDM v případě, že nebude objektivně možné legislativní změnu zapracovat ke dni účinnosti legislativní změny. Legislativní úpravou se rozumí úprava stávající funkčnosti stávajícího IDM, kterou je nutné provést, protože stávající funkcionality by nutila Objednatele postupovat v rozporu s novou legislativní úpravou. Legislativní úpravou v žádném případě není doplnění funkcionality (řešené oblasti), kterou stávající IDM zatím nedisponuje. Legislativní úpravy budou realizovány tak, aby bylo možné tyto úpravy předat Objednateli standardně v den, kdy vešla nová právní úprava v účinnost, nejpozději však do 60 dnů ode dne, kdy vešla nová právní úprava v účinnost. Nebude-li splnění této lhůty vzhledem k rozsahu nutných úprav možné, je Poskytovatel povinen na tuto skutečnost Objednatele upozornit neprodleně po zjištění této skutečnosti, sdělit lhůtu, ve které dojde k dodání příslušné legislativní úpravy a navrhnout opatření pro přechodné období. Legislativní úprava IDM bude zajišťována prostřednictvím poskytnutí upgrade nebo update. Součástí legislativní podpory je též aplikace (implementace) těchto upgrade a update.</p> <p>V případě, že Objednatel kontaktoval Poskytovatele za účelem konzultace prostřednictvím Service Desk, je Poskytovatel povinen řádně odeslat Objednateli svou odpověď nejpozději do 48 hodin po obdržení předmětného požadavku.</p>			
Služby podpory			
Poskytování služeb 2. a 3. úrovně podpory dle Katalogového listu ID: SLA Služby.			
Podmínky a omezení služby			
<ul style="list-style-type: none"> • Příjem ticketů skrze SD MHMP 			

KL03 – Podpora a údržba

OZNAČENÍ SLUŽBY	KL03 – Podpora a Údržba	TYP KL:	Paušál
Název služby	Podpora a Údržba		
Zkrácený popis služby	Podpora a Údržba		
Rozsah požadovaných činností			
<p>Služby údržby systému jako celku Poskytovatel zabezpečí nutné služby pro spolehlivý a bezpečný provoz systému v prostředí Objednatele. Tímto se rozumí takové nezbytné úpravy systému, které budou vyžadovány zejména externími vlivy, např:</p> <ol style="list-style-type: none"> 1. Podněty pro instalaci aktualizací operačního systému, databáze a všech potřebných podpurných komponent pro provoz IDM na infrastruktuře Objednatele. 2. Podněty pro instalaci aktualizací v případě dispozice nové minoritní opravné verze platformy IDM s bezpečnostními a opravnými funkcemi. 3. Podněty pro instalaci funkční aktualizace platformy IDM v případě dispozice nové majoritní verze platformy od výrobce (např. z důvodů ukončení podpory nasazené verze platformy MidPoint). 4. Návrhy / podněty pro úpravu integračního rozhraní vyvolané změnou na straně připojených systémů. Tímto se nerozumí jejich samotná realizace. 5. Návrhy / podněty pro úpravu nebo úprava nastavení systému vyvolané změnou legislativy s dopadem na oblast řízení identit. Tímto se nerozumí jejich samotná realizace. 6. Návrhy / podněty pro úpravu nebo úprava nastavení systému vyvolané změnou ICT standardů a ICT provozních postupů Objednatelem. Tímto se nerozumí jejich samotná realizace. 7. Návrhy / podněty pro úpravu nebo úprava nastavení systému vyvolané změnou interních procesů Objednatelem zahrnující identity (změna workflow). Tímto se nerozumí jejich samotná realizace. 8. Návrhy / podněty pro úpravu systému vyvolané změnou uživatelských oprávnění/rolí. Tímto se nerozumí jejich samotná realizace. <p>Služby rozvojové profylaxe Poskytovatel zabezpečí pravidelné profylaktické kontroly IDM a všech jeho aplikačních komponent alespoň 1x za 3 měsíce. Cílem bude optimalizovat technické možnosti hardwarových i softwarových komponent IDM v kontextu celkové koncepce rozvoje systému. Součástí služby budou i doporučení ohledně preventivního odstraňování úzkých míst nebo změn parametrů, eventuálně doporučení použití nových verzí nebo řešení s ohledem na vývoj produktů, která budou v případě schválení Objednatelem realizována formou rozvojového požadavku.</p> <p>Služby analýzy a řešení provozních problémů Poskytovatel zabezpečí služby podpory procesu odhalování chyb a nejasností a vyšetřování nahlášených incidentů, a to nad rámec standardních Služeb podpory. Zvláště se tím rozumí:</p> <ol style="list-style-type: none"> 1. Analytické práce pro odhalení identifikovaného problému (např. chybně předané parametry do připojeného systému, nezpracovaný pokyn od IDM atp.) s cílem odhalení příčiny. <p>Zajištění komunikace se zúčastněnými stranami (věcný a technický garant IDM, administrátor IDM, techničtí a věcní garanti okolních systémů případně vlastní provozovatelé systémů) v rámci odhalování problémů nebo při analýze rozvojových požadavků.</p>			
Služby podpory			
Poskytování služeb 2. a 3. úrovně podpory dle Katalogového listu ID: SLA Služby.			
Podmínky a omezení služby			
Příjem ticketů skrze SD MHMP Service Desk Pro komunikaci se systémem Service Desk bude využito předávání informací o servisních požadavcích pomocí e-mailu ve smluvené formě – notifikace ze SD.			

ID: SUP01

OZNAČENÍ SLUŽBY	SLA	TYP KL:	Parametry služby
Název služby	Služby 2. a 3. úrovně podpory		
Zkrácený popis služby	Poskytování služeb 2. úrovně podpory a zprostředkování služeb 3. úrovně podpory		
Detaily služby			
<p>Předmětem služby je obsluha požadavků v rámci 2. a 3. úrovně podpory dle interní dokumentace.</p> <p>2. úroveň podpory Pracovníci této úrovně mají hlubší znalosti a větší specializaci ve svěřené oblasti. Jsou schopni řešit složitější problémy a hledat řešení. Jsou schopni již pracovat, vyhledávat a identifikovat chyby v datech a systémech. Provádí diagnózu a vyšetření incidentu a posuzuje incident z hlediska dopadu na ostatní systémy. Provádí vyšetření a diagnózu incidentu na své úrovni, pokud není incident možné vyřešit na 2. úrovni, je předáván na 3. úroveň podpory dle kategorie incidentu.</p> <p>3. úroveň podpory Jedná se o podporu IDM a rozhraní z IDM. Po vzájemné dohodě mezi Poskytovatelem a Objednatelem dochází k předání zařízení třetí straně za účelem zhodnocení daného problému a jeho případné vyřešení. Náhradní díly pro odstranění/vyřešení kvalifikovaného incidentu/požadavku zajistí včas Objednatel.</p>			
Parametry SLA			
<p>Parametry SLA pro jednotlivé priority požadavků jsou uvedeny níže.</p> <p>Omezení dostupnosti služby Dostupnost služby z pohledu SLA je omezena pouze po dohodě s odběratelem služby (např. stěhování je určeno po dohodě, kdy mají obě strany čas a na něm se dohodnou). Doba odezvy pro všechny služby je 90 minut. (notifikační email ze strany poskytovatele služby SD) Zahájení řešení problému je 5 hodin od přijetí doby odezvy systému. Incident může být Blokuující, Majoritní nebo Minoritní. V případě priority 1 se skupinovým dopadem (mimořádná událost 50 záznamů v SD za hodinu) se upravuje SLA dle priority D zapsané v SD.</p>			
Naléhavost	Dopad MHMP		
	Skupinový	Individuální	
<p>Některé nebo všechny části systému selhaly a jsou zcela nedostupné, jsou zcela nefunkční:</p> <ul style="list-style-type: none"> • znemožňuje fungování IDM u koncových uživatelů jako celku nebo znemožňuje provádění stěžejních operací IDM pro jednotlivé uživatele nebo skupiny uživatelů, • případně Objednatel není schopen plnit své povinnosti vůči třetím stranám - jedná se o stav, kdy je ohrožena přímo funkce IDM jako programu, je ohrožena funkčnost informačních systémů, • nebo je nutné přikročit ke komplikovaným a nákladným řešením mimo IDM. Týká se to i stavu, kdy je IDM zatížen právy třetích osob a tento stav je zaviněn Poskytovatelem. 	Priorita 1	Priorita 1	
<p>Systém je funkční pouze částečně, systém je ovlivněn selháním nebo omezením některé ze systémových funkcí podporujících činnosti systému. Některá ze služeb vykazuje funkční vady. Pouze některé funkce nejsou plně funkční:</p> <ul style="list-style-type: none"> • vada, která znemožňuje řádné fungování určité podstatné funkce IDM u některého koncového uživatele či informačního systému tak, že ohrožuje splnění závazků Objednatele vůči těmto třetím stranám, nebo IDM vykazuje nepřiměřeně dlouhé odezvy, a tyto vadné funkce nelze nahradit jinou funkcionalitou či náhradním 	Priorita 2	Priorita 2	

postupem bez podstatně zvýšené pracnosti nebo nákladů Objednatele.					
Zařízení je funkční, ale vyžaduje preventivní zásah: <ul style="list-style-type: none"> vada, která komplikuje nebo znemožňuje řádné fungování určité funkce IPM u některého koncového uživatele nebo IPM nekomunikuje s některou částí informačního systému, avšak jeho činnost lze dle pokynů Poskytovatele nahradit jinou funkcionalitou, byť za cenu vyšší pracnosti na straně Objednatele. 		Priorita 3	Priorita 3		
Požadavkem je žádost o součinnost anebo podání informace (dotaz, vysvětlení).		Priorita 3	Priorita 3		
Služby na objednávku/mimořádná událost: Požadavek na zlepšení / rozšíření funkce. Požadavky vznesené uživateli dle definice v jednotlivých KL		D	D		
OZNAČENÍ SLUŽBY	SLA	TYP KL:	Parametry služby		
Název služby	Služby 2. a 3. úrovně podpory				
Zkrácený popis služby	Poskytování služeb 2. úrovně podpory a zprostředkování služeb 3. úrovně podpory				
Parametry SLA					
Úroveň služby	Provozní doba služby (PDS)	Priorita – doba k vyřešení (v hod, měřeno v PDS)			
		1	2	3	D**
KL01-SD	5 x 8 (9 – 17 h)	8	24	48	D
KL02-MAINT*	5 x 8 (9 – 17 h) x Next Business Day	160	240	480	D
KL03-PODP	5 x 8 (9 – 17 h)	12	24	48	D
<p>* Poskytování služeb 3. úrovně se řídí podmínkami a časy výrobce, jež jsou uvedeny v dokumentu níže a tvoří součást tohoto KL.</p> <p>** V případě požadavku priority D je čas vyřešení určen dohodou Objednatele a Poskytovatele formou zápisu do SD Objednatelem.</p> <p>V případě součinnosti mezi Poskytovatelem a Objednatelem se nepočítá SLA na straně Objednatele pro Poskytovatele. Odpověď začíná notifikačním emailem na žadatele a řešitelskou skupinu Poskytovatele, případně zahájení incidentu či požadavku jinou cestou než SD. Proces SD je v samostatné příloze smlouvy.</p>					
Vyhodnocování kvality poskytovaných služeb					
Objednatel bude provádět vyhodnocení kvality poskytovaných služeb podpory dle tohoto katalogového listu. Měřícím bodem je SD Objednatele a měřícím obdobím kalendářní měsíc.					
V případě nedodržení parametrů SLA obsluhy incidentu priority 1 je Objednatel oprávněn požadovat smluvní pokutu za každý jednotlivý případ takového nedodržení vypočtenou dle následujícího vzorce:					
$SPSUP = PHOD \times 500$					
<p><i>SPSUP</i> Smluvní pokuta za jeden případ nesplnění parametrů SLA obsluhy incidentů priority 1 zaokrouhlená na celé Kč směrem nahoru</p> <p><i>PHOD</i> Počet hodin prodlení s obsluhou jednoho případu incidentu priority 1, přičemž za prodlení s obsluhou se považuje nedodržení parametru reakční doby (reakční doba je 7 – 19 h)</p>					
Doplňující informace					
Způsob dokladování a vyhodnocování		Měsíční přehled incidentů z SD Objednatele s uvedením Úrovně podpory, Priority, data a času Odpovědi a data a času Vyřešení v rozsahu Objednavatelem nastaveného SD MHMP.			

Podmínky poskytování služeb 3. úrovně

Evolveum s.r.o.
Vendelínska 109
900 55 Lozorno
Slovakia, EU



Product Support General Principles and Conditions

Evolveum typically provides third-level product support. We expect first and second-level product support to be provided by the partner or the customer. The focus of third-level product support is to resolve midPoint product bugs. It includes reactions to product issues reproducible in the usual midPoint environment, product issues presented in an accessible system by an Evolveum developer, supportable product issues by detailed log traces, and similar cases. We assume the partner or the customer will take over configuration-related cases as a part of second product level support.

Third-level Product Support

1. The support solves product bugs. It does not solve configuration bugs or bugs of inappropriate analysis, design, architecture, and so on.
2. The demonstration of bugs in a standard product environment (without customizations which are not part of midPoint) is expected. Alternatively, full remote access to the system with the bug is expected. In rare cases, bug analysis based on the log files is a possibility as well. This approach is solely available for bugs that are technically non-reproducible. It is not applicable for non-technical barriers (e.g., access to the system is denied for security reasons).
3. A documentation bug fixing is included (e.g., a mistake in the midPoint documentation). The bug must be entered into Evolveum's bug tracking system.
4. MidPoint is an open-source product based on an open community principle. Therefore, all bug reports are considered as public. All information entered into a ticket is displayed and publicly visible, meaning it is available to the other community members and to the general public. All sensitive information should be removed or anonymized by the partner/customer.
5. Public bug reporting, as well as any other communication, is performed in English.
6. Bug reporting must be entered into Evolveum's bug tracking system.
7. 8 x 5 x Next Business Day response time support is provided. The support is available during Evolveum's normal business hours. Response time support is the time beginning when the partner/customer creates a service request until Evolveum first responds to it. Within the response time, the ticket is accepted by setting a fix version, or denied if the ticket covers out of scope service.
8. The bundled connectors are covered by third-level product support, but the support has its limitations [REDACTED]

Evolveum expects a serious approach from the partner or the customer who should be supporting the lower levels (1st and 2nd level product support) by themselves. This is especially true with the initial diagnosis of a particular issue. Evolveum reserves the right to refuse the bug report acceptance that was not diagnosed in detail or not adequately described. Evolveum also reserves the right to automatically change the priorities, and in extreme cases, even terminate the cooperation with the partner or the customer who repeatedly neglects diagnosing and describing the problem or misuses the service.

Evolveum provides 2 main product release types, Feature Releases and Long-Term Support (LTS) Releases. Feature Releases are supported 1 year from their release date. LTS Releases are supported 3 years from their release date. There is a possibility to extend the length of support for a fee. Both LTS and Feature Releases may have related maintenance releases. They are supported as long as the particular LTS/Feature Release is supported.

© 2020-2022 Evolveum s.r.o.
Registration number: 46296859, VAT number: SK2023324358,
Tatra banka, a.s. IBAN SK381100000002941460606, SWIFT: TATRSKBX
Registered in the commercial register of District Court Bratislava I., Section: Sro,
File number 7499/B

Evolveum s.r.o.
Vendelínska 109
900 55 Lozorno
Slovakia, EU



All provided bug fixes are released as open source under the Apache 2.0 license as well as the EUPL license. Other open source licenses might be considered in the future.

Reservations

1. Fourth-level product support (development of new features, improvements, and enhancements into midPoint product) is not provided.
2. Backporting of the improvements and new features is not provided.
3. Third-level product support for features marked as experimental is not provided.
4. Second-level product support (configuration bug fixing) is not provided.
5. Consulting services (consultancies, configuration, analysis, design, project activities, etc.) are not provided.
6. Training & Certification are not provided.
7. Transfer of information and/or knowledge transfer is not provided.
8. Adding missing documentation is not included.

Subscription Cancellation

The subscription is activated based on the customer's decision for a specific period. The activation is considered as a commitment for the period. If the customer decides to cancel an activated subscription for any reason, they must provide a written notice at least 60 days prior to the end date of the active period. The active period expires, and the end date is the last day of cooperation with Evolveum. The subscription renewal is not realized.

The immediate cancellation of an active subscription is only possible if Evolveum neglects its obligations and does not deliver on its agreements.

If the customer leverages Evolveum's services through a partner, failure on Evolveum's part should not lead to the termination of the contract between the partner and the customer, and vice versa.

© 2020-2022 Evolveum s.r.o.
Registration number: 48298859, VAT number: SK2023324358,
Tatra banka, a.s. IBAN SK381100000002941460606, SWIFT: TATRSKBX
Registered in the commercial register of District Court Bratislava I., Section: Sro,
File number 74908/B

Příloha č. 1, část (D): Popis cílového stavu

Popis cílového stavu										
Oblast	ID	Požadavek	Funkční/ Nefunkční	Stav	Uživatelsky / garantem spravované	Administr. spravované	Portál uživatele	API/web service	Poznámky	
A Obecné požadavky										
	A.1	Identita musí být pro všechny spravované entity (osoby) unikátní, každá entita spravovaná v IDM bude mít právě jednu identitu, tj. každá fyzická osoba spravovaná IDM bude mít právě jeden identifikátor nezávislý n ačase, na pracovně-právních vztazích a dalších údajích.	Nefunkční	Požadované						
	A.2	IDM musí v návaznosti na zdrojové systémy dat o identitách udržovat a spravovat kompletní životní cyklus identity. Jedná se zejména o příchod zaměstnance, přidělení business rolí dle jeho organizačního zařazení (systematizovaného místa), doplňování business rolí i mimo systemizované místo, změna rolí v případě jeho změny jeho zařazení, odchod zaměstnance spočívající v deaktivaci, archivaci jeho identity apod. Seznam požadavků na podporu procesů řízení životního cyklu identity je uveden v oblasti B.	Nefunkční	Požadované						
	A.3	IDM musí v závislosti na zdrojových systémech zajistit správu více organizačních struktur (například standardní organizační strukturu systemizovaných míst, virtuální strukturu míst pro externisty, DPČ/DPP atd.)	Funkční	Požadované				Ano		
	A.4	IDM musí zajistit přiřazení aplikačních rolí a souvisejících uživatelských účtů pro cílové systémy na základě business rolí a dalších vlastností nebo atributů identity. Současně musí zajistit aktualizaci aplikačních rolí a souvisejících uživatelských účtů při změně business rolí nebo dalších vlastností nebo atributů identity.	Funkční	Požadované	Ano	Ano		Ano		
	A.5	IDM musí obsahovat registr aplikací a informačních systémů (souhrnné IS) a informace o správě jejich uživatelských účtů a rolí, včetně možnosti importu rolí přes definované rozhraní (webová služba, API apod.)	Funkční	Požadované	Ano	Ano		Ano		
	A.6	IDM musí umožnit identitě přiřazení více uživatelských účtů ("loginů") v závislosti na cílových systémech, například na základě role nebo atributu apod. Uživatelský účet dané aplikace nebo IS může být přiřazen i více identitám, ale v tom případě sdílený účet není řízen systémem IDM.	Funkční	Požadované		Ano				
	A.7	IDM musí obsahovat samoobslužné uživatelské rozhraní (portál uživatelské samoobsluhy) pro zadávání žádostí vztahujících se k řízení uživatelských rolí a přístupů (přidělování a změny business nebo aplikačních rolí, změny členství ze skupinách atd.). Požadavky na změny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může mít nastaveno vyřízení změny automaticky bez schválení.	Funkční	Požadované	Ano	Ano	Ano	Ano		
	A.8	IDM musí pro deaktivované a archivované identity zajistit anonymizaci jejich údajů.	Funkční	Požadované		Ano				
	A.9	Správa uživatelů (identit) musí obsahovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím definovaného rozhraní (např. webová služba)	Funkční	Požadované	Ano	Ano		Ano		
B Podpora procesů										
	B.1	IDM musí (v návaznosti na zdrojové systémy dat) podporovat procesy správy životního cyklu identity a sovisající obslužbě procesy, zejména:	Nefunkční	Požadované						
	B.2	vznik nové identity	Funkční	Požadované		Ano				
	B.3	nový pracovněprávní vztah	Funkční	Požadované		Ano				
	B.4	změna pracovněprávního vztahu a následná změna údajů identity	Funkční	Požadované	Ano	Ano				
	B.5	změny popisných atributů, např. jméno	Funkční	Požadované	Ano	Ano				
	B.6	změny organizačního zařazení	Funkční	Požadované	Ano	Ano				
	B.7	změny platnosti vlastností identity (rolí, atributů atd.)	Funkční	Požadované	Ano	Ano				
	B.8	automatická změna rolí na základě změny stavu / typu identity, případně jiného příznaku identity	Funkční	Požadované		Ano				
	B.9	změna evidenčního stavu identity (zejména v oblasti pracovně-právních vztahů, např. změna HPP, DPČ, mateřská, překážky na straně zaměstnavatele apod.), tj. například podporovat jen změnu evidenčních údajů, kdy se nemění pracovně-právní vztah apod.	Funkční	Požadované	Ano	Ano				
	B.10	ukončení pracovněprávního vztahu	Funkční	Požadované	Ano	Ano				
	B.11	aktivace/deaktivace (ruční, automatická) identity, rolí, atributů apod.	Funkční	Požadované	Ano	Ano				
	B.12	Anonymizace definovaných údajů identity na základě pravidla nebo na vyžádání	Funkční	Požadované	Ano	Ano			viz. A.8	
C Řízení identit, rolí, systemizace, atributů										
	C.1	IDM umožní přesun identity v rámci organizační struktury i mezi jednotlivými organizačními strukturami (např. mezi standardní strukturou systemizovaných míst a strukturou virtuálních systemizovaných míst pro externisty apod.)	Funkční	Požadované	Ano	Ano				
	C.2	IDM umožní kopírování rolí, pracovních pozic mezi jednotlivými systematizovanými/virtuálními místy organizačních strfuktur	Funkční	Požadované		Ano				
	C.3	IDM umožní přiřazení rolí konkrétní identitě, systemizovanému místu, skupině a organizační jednotce včetně možnosti nastavení data a času vypršení platnosti přiřazení. Po vypršení platnosti přiřazení IDM rolí přiřazenému objektu automaticky odebere.	Funkční	Požadované		Ano		Ano		

C.4	IDM umožní přidělení role nebo oprávnění konkrétní identitě, systemizovanému/virtuálnímu místu, skupině nebo organizační jednotce.	Funkční	Požadované	Ano	Ano				
C.5	IDM umožní správu business/aplikačních rolí, včetně zařazení uživatele do odpovídající role.	Funkční	Požadované	Ano	Ano				
C.6	IDM umožní dočasné nastavování rolí, po uplynutí nastaveného intervalu se role automaticky odebere.	Funkční	Požadované	Ano	Ano	Ano			
C.7	IDM umožní automatizované nastavování rolí nebo atributů na základě pravidel (událostí).	Funkční	Požadované	Ano	Ano	Ano			
C.8	IDM umožní kopírovat role mezi jednotlivými systemizovanými/virtuálními místy organizačních struktur.	Funkční	Požadované		Ano				
C.9	IDM musí obsahovat funkcionalitu kopírování veškerého nastavení oprávnění jednoho uživatele na druhého.	Funkční	Požadované		Ano				
C.10	IDM umožní definovat vztahy zastupitelnosti (delegování) mezi objekty (systemizovaná místa, business role atd.) – musí umožnit uživatelům, aby v souladu se strukturou organizace mohli delegovat v případě potřeby (nemoc, dovolená atd.) svoje role, nebo jejich část na jiné pověřené osoby, a to i tak, že jedna identita nebo objekt (systemizované místo, role..) může mít pro nastavené delegování na jiný objekt. Delegování bude defonavetné jako časově omezené, kdy se po nastaveném intervalu nebo podmínce (pravodlu) nastavená delegování automaticky v IDM zruší.	Funkční	Požadované	Ano	Ano		Ano		
C.11	Správa organizační struktury (systemizace) bude možná pro interní i externí identity, a to jako samostatné „větve“ struktury (např. organizační struktura virtuálních míst)	Funkční	Požadované	Ano			Ano		
C.12	IDM zajistí přidávání a správu dalších typů referenčních objektů (min. min. systemizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát) a to i v průběhu zakládání či úpravy konkrétní identity s možností okamžitého použití referenčního objektu u spravované identity	Funkční	Požadované	Ano	Ano		Ano		
C.13	IDM zajistí dodatečné rozšiřování identit a referenčních objektů o další atributy a zajistí publikaci i těchto nových atributů externím aplikacím prostřednictvím rozhraní webových služeb IDM	Funkční	Požadované		Ano		Ano		
C.14	Správa identity bude umožňovat i správu údajů o uživatelských digitálních certifikátech. Data o certifikátech bude možné nahrávat do systému prostřednictvím rozhraní webových služeb. Současně zajistí IDM notifikace uživatelů na základě definovaných pravidel správy certifikátů (vypšení platnosti apod.).	Funkční	Požadované	Ano	Ano	Ano	Ano		
C.15	IDM umožní k identitám přikládat obrazové soubory (fotografie)	Funkční	Požadované	Ano	Ano	Ano	Ano		
C.16	IDM musí obsahovat registr aplikací a informačních systémů (souhrnně IS) a jejich aplikačních rolí včetně možnosti importu rolí přes webové služby	Funkční	Požadované		Ano		Ano		
C.17	IDM musí obsahovat integrovanou správu aplikačních rolí, včetně zařazení uživatele do odpovídající role v napojených IS.	Funkční	Požadované		Ano		Ano		
C.18	IDM musí obsahovat integrovanou správu samostatných identifikovatelných objektů – referenčních objektů, na které se identity mohou odkazovat: min. systemizované místo, organizační jednotka, skupina, pracovní pozice, funkce, aplikace, skupina aplikací, aplikační role, certifikát, business role	Funkční	Požadované		Ano		Ano		
C.19	IDM umožní správu evidence osobních údajů, která bude obsahovat správu evidence subjektů údajů a evidenci jejich osobních údajů včetně jejich kategorií a klasifikací.	Funkční	Požadované		Ano			Je nutné počítat s tvorbou modelu zaměřeného na prostředí MHMP (dáno rozdílným přístupem každé organizace k uvedené problematice)	
C.20	IDM bude obsahovat evidenci účelů pro nakládání s osobními údaji subjektů údajů. V rámci daného účelu budou definována oprávnění, aplikační role pro přístup k osobním údajům.	Funkční	Požadované		Ano			viz C.20	
C.21	IDM bude obsahovat správu skupin s možností začleňovat více skupin do sebe, přiřazovat do skupin jednotlivé identity i systemizovaná místa.	Funkční	Požadované		Ano				
C.22	IDM musí umožňovat správu organizačních a procesních rolí, jejich vytváření a synchronizace do spravovaných systémů (provisioning) na principu RBAC, popř. ABAC	Funkční	Požadované		Ano			ABAC jako přesně definované rozšíření RBAC	
C.23	IDM podporuje jak statickou organizační strukturu danou systemizovanými místy, tak dynamickou strukturu (dynamické reporting lines) dané přiřazením vybraného typu business roli	Funkční	Požadované	Ano	Ano	Ano			
C.24	IDM umožní aktivovat nebo deaktivovat přiřazené role na základě splnění definovaných podmínek (vyhodnocení pravidla), např. aktivovat roli na základě absolvovaného školení uživatele.	Funkční	Požadované	Ano	Ano	Ano	Ano		
C.25	IDM umožní zjišťování/výpis aktuálního stavu pravidel řídicích přiřazování a aktivaci rolí (enablerů), včetně stavu jejich vyhodnocovaných parametrů (např. zjistit, které podmínky nejsou splněny pro automatické přiřazení nebo aktivaci role konkrétní identity).	Funkční	Volitelné		Ano				
D Automatizace řízení živ. cyklu identity, automatizace procesů									
D.1	IDM musí disponovat integrovanou podporou automatizace – na úrovni intuitivní tvorby pravidel v grafickém prostředí (např. pro automatické vytváření uživatelských účtů, začleňování identit nebo účtů do skupin, přiřazování business/aplikačních rolí na základě libovolných atributů identity a přidružených referenčních objektů – business role, aplikační role, systemizované místo atd.). Integrovaná automatizace pro řízení životního cyklu změn identit a schvalování změn musí umožnit minimálně následující:	Funkční	Požadované		Ano				
D.1.1	- zadávání požadavků uživatelů na změny v přiřazení rolí a skupin ke schválení nadřízeným	Funkční	Požadované		Ano				
D.1.2	- možnost sledování stavu svých požadavků uživateli	Funkční	Požadované		Ano				
D.1.3	- emailové upozornění schvalovatele na požadavek ke schválení	Funkční	Požadované		Ano				
D.1.4	- vytvoření a zobrazení přehledu úloh ke schválení pro každého schvalovatele	Funkční	Požadované		Ano				
D.1.5	- schvalování či zamítnutí požadavků včetně uvedení zdůvodnění	Funkční	Požadované		Ano				
D.1.6	- víceetapové schvalování	Funkční	Požadované		Ano				

D.1.7	- schvalování jedním nebo více schvalovateli (skupinou)	Funkční	Požadované		Ano			
D.1.8	- větvení pro ošetření výjimek vzniklých při schvalování	Funkční	Volitelné		Ano			Nutno prodiskutovat a definovat v rámci předimplementační analýzy rozsah výjimek implementovaných v rámci podpory procesů IDM
D.1.9	- řešení zastupitelnosti (delegování)	Funkční	Požadované		Ano			
D.1.10	- eskalace – upozornění při překročení termínu splnění	Funkční	Požadované		Ano			
D.1.11	- vkládání systémových kroků s voláním webových služeb a spuštěním skriptů	Funkční	Požadované		Ano			
D.1.12	- pro správce IDM pracovat se všemi úlohami	Funkční	Požadované		Ano			
D.2	IDM bude obsahovat administrátorský nastavitelnou automatizaci procesů správy životního cyklu osobních údajů subjektu údajů.	Funkční	Požadované		Ano			
D.3	IDM automatizovaně provede (vyžádá u příslušné CA) zneplatnění certifikátů, o kterým má uložené informace na základě definovaných podmínek (změn pracovní právního vztahem, vypršení platnosti certifikátu atd.)	Funkční	Požadované		Ano		Ano	
D.4	IDM umožní autonomní správu hesel (samoobsluha), tj. bude obsahovat uživatelské rozhraní pro reset hesla jednotlivých účtů daného uživatele. Zaslání kódů pro reset hesla danému uživateli musí být možno provádět pomocí SMS (tj. IDM musí být možné na SMS bránu či službu napojit). Rozhraní musí umožnit i běžnou změnu hesla (bez resetu).	Funkční	Požadované	Ano	Ano	Ano	Ano	
D.5	IDM bude obsahovat samoobslužné uživatelské rozhraní pro zadávání žádostí o přidělení jednotlivých business nebo aplikačních rolí a členství ve skupinách. Role a skupiny budou kategorizovány a kategoriím bude možné přidělit schvalovací workflow nebo může žádost vyřízena automaticky bez schválení.	Funkční	Požadované	Ano	Ano	Ano	Ano	
D.6	IDM musí podporovat vytváření workflow s více stupni schvalování a eskalací napříč organizační strukturou. Umožní přidělení oprávnění nebo role konkrétní identitě, systemizovanému místu, skupině nebo organizační jednotce.	Funkční	Požadované					
D.7	Samoobslužné rozhraní umožní na úrovni organizace a organizační jednotky definovat seznam rolí a skupin, o které mohou žadatelé požádat.	Funkční	Požadované					
E	Propojení na koncové (cílové) systémy, synchronizace							
E.1	Při napojování IDM na cílové (koncové) systémy pro automatizovanou synchronizaci rolí, účtů a přístupů se bude IDM přizpůsobovat koncovým systémům a nikoli naopak (tedy při vytváření rozhraní pro připojení cílového systému bude většinou probíhat tvorba rozhraní na straně IDM).	Funkční	Požadované		Ano		Ano	
E.2	IDM musí podporovat propojení na systémy typu PAM	Funkční	Požadované		Ano		Ano	
E.3	IDM musí procesně podporovat napojení systémů bez API (vytvářenín workorderů k práci s účty).	Funkční	Požadované		Ano		Ano	
E.4	IDM musí podporovat napojení na systém distribuce, ukládání, bezpečnou archivaci, změny, ničení, kontrolu a audit klíčů s využitím PAM.	Funkční	Požadované		Ano		Ano	
E.5	IDM musí podporovat napojení na RADIUS Server.	Funkční	Požadované		Ano		Ano	
E.6	IDM musí obsahovat API pro připojení dalších systémů MHMP	Funkční	Požadované		Ano		Ano	
E.7	IDM musí umožnit migraci z a do jiného Identity Manažeru.	Funkční	Volitelné		Ano		Ano	
E.8	IDM musí obsahovat Centrální GUI pro administraci administrátorem.	Funkční	Požadované		Ano		Ano	
E.9	IDM musí podporovat komunikaci SAML a napojení na AD.	Funkční	Požadované		Ano		Ano	
E.10	IDM musí podporovat napojení na Flux a případně další personální systémy	Funkční	Požadované		Ano		Ano	
E.11	IDM musí umožnit synchronizaci identit a jejich atributů v jednotlivých spravovaných systémech s centrálním stavem identit v IdM (reconciliation)	Funkční	Požadované		Ano		Ano	
E.12	IDM musí podporovat SCIM 2.0 (System for Cross-domain Identity Management)	Funkční	Požadované		Ano		Ano	
E.13	IDM musí podporovat definici SCIM							
F	Logování, auditní stopy, ostatní požadavky							
F.1	IDM musí umožňovat záznam definovaných důležitých událostí v IdentityManageru a následný audit a reporting.	Nefunkční	Požadované					
F.2	IDM musí podporovat auditní procesy, zejména evidenci nastavení vlastností objektu (identity, role, aplikační role, atributů apod.) v zadaném čase. IDM musí zajistit možnost zjistit nastavení daného objektu v požadovaném čase (příklad: možnost zjistit nastavení vlastností identity k určitému časovému okamžiku, tj. přiřazené business role, účty, aplikační role, atributy atd. + log záznam o přenesených změnách cílového systému platných ke zvolenému časovému okamžiku). Retence zachování těchto auditních informací je požadována jako parametrizovaná.	Nefunkční	Požadované		Ano		Ano	
F.3	IDM musí podporovat napojení na Logmanagement systém. Zaznamenávají se všechny aktivity v IDM a použít bude standardní logovací protokol (např. syslog).	Funkční	Požadované		Ano		Ano	
F.4	IDM musí podporovat napojení na systémy typu SIEM.	Funkční	Požadované		Ano		Ano	
F.5	IDM musí být integrováno na nástroj typu ServiceDesk	Funkční	Požadované		Ano		Ano	
F.6	IDM musí umožňovat testování všech typů rolí včetně jejich atributů a ověřování jejich správnosti a konzistence.	Nefunkční	Požadované		Ano			
F.7	IDM musí podporovat vysokou dostupnost a být implementován jako vysoce dostupný systém včetně geografické dostupnosti respektující geografické rozmístění systémů SŽ a topologii sítě (cluster s geografickou redundancí apod.).	Nefunkční	Požadované					

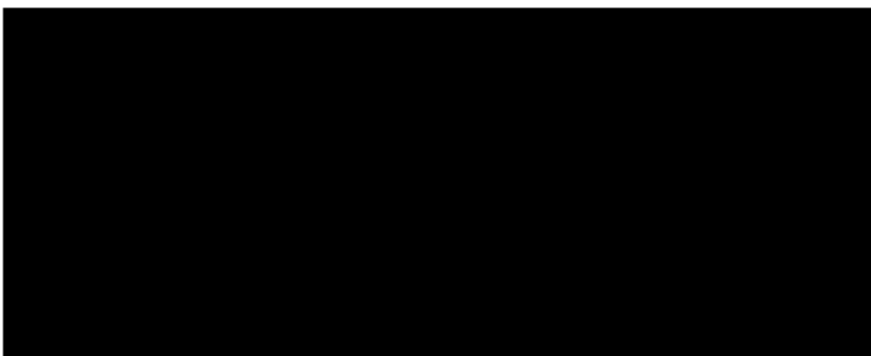
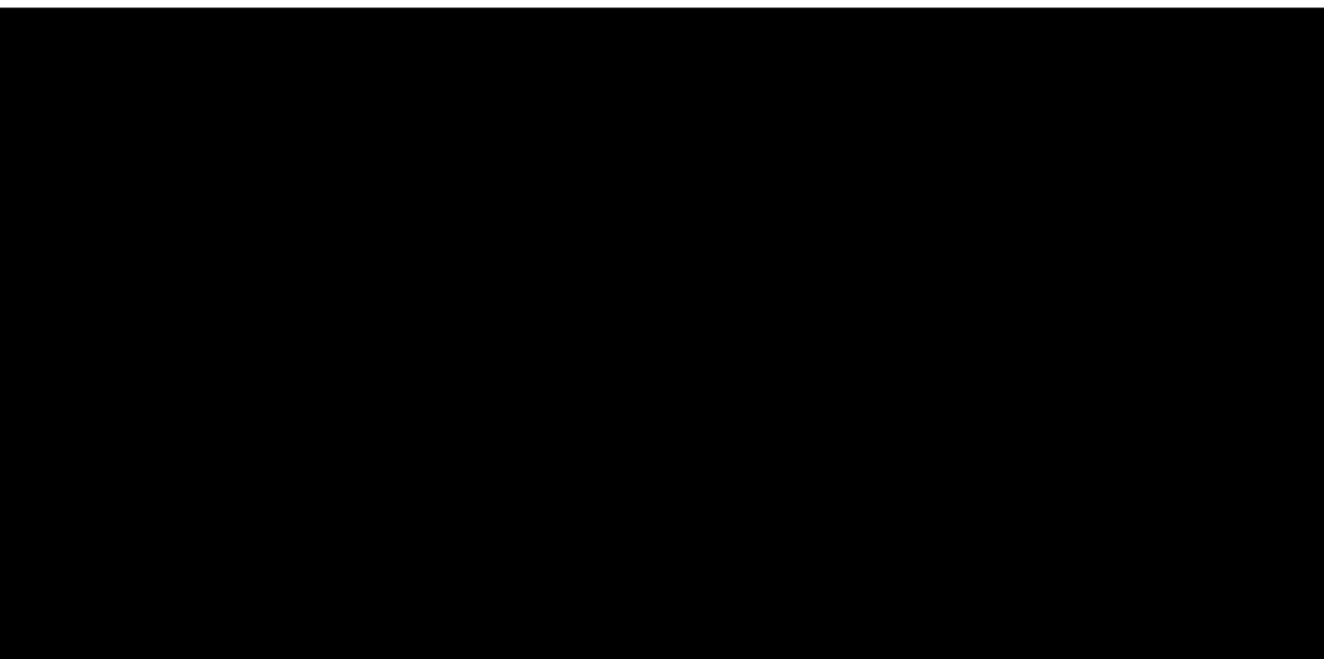
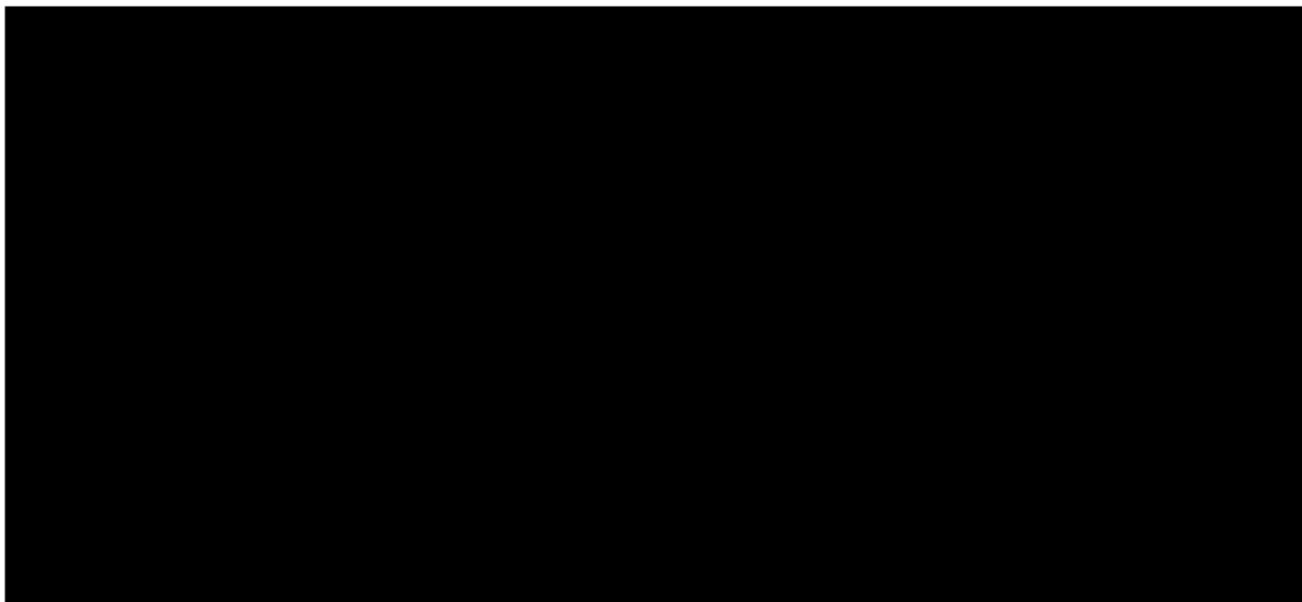
FNC	
Funkční	1
Nefunkční	0

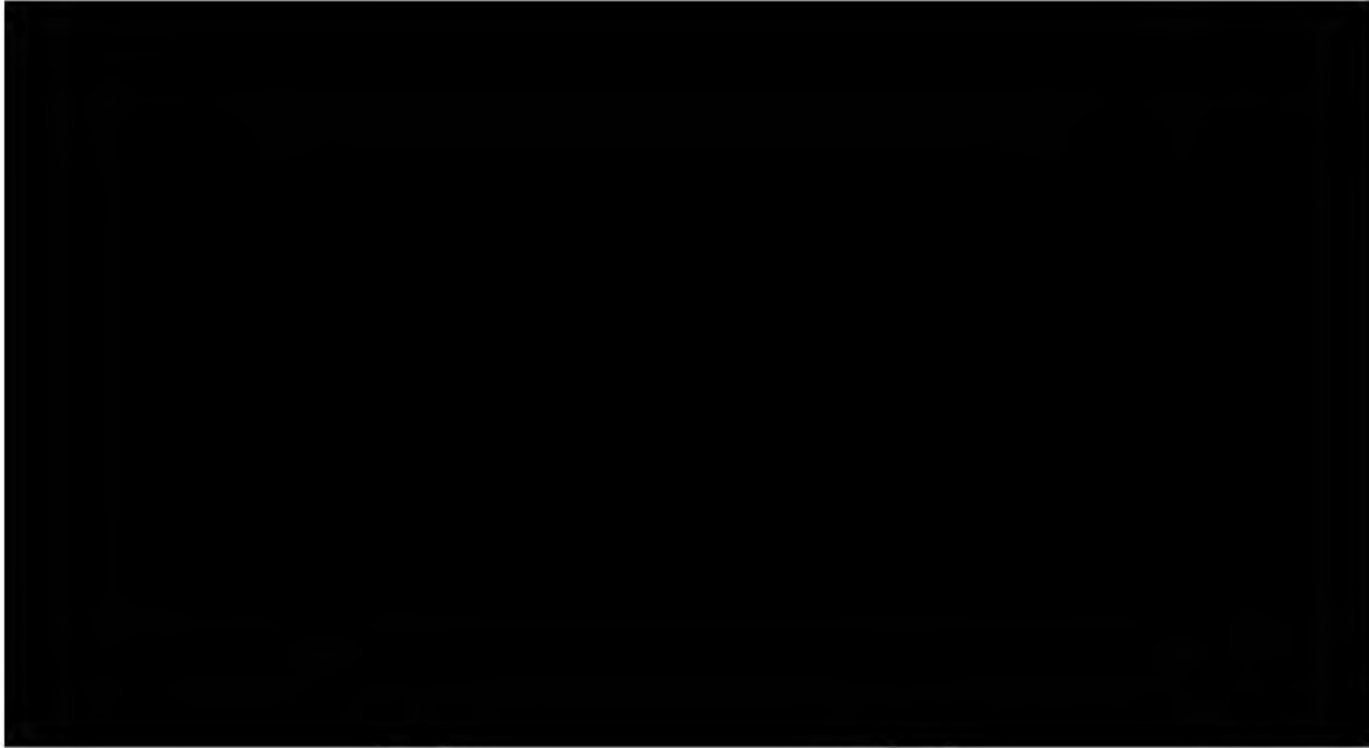
STATUS	
Požadované	1
Volitelné	0

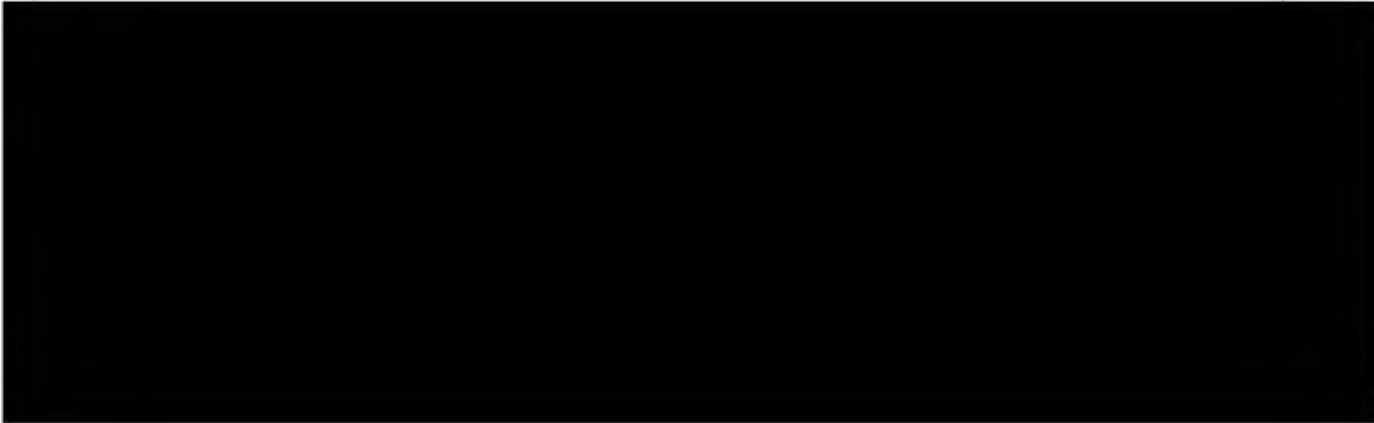
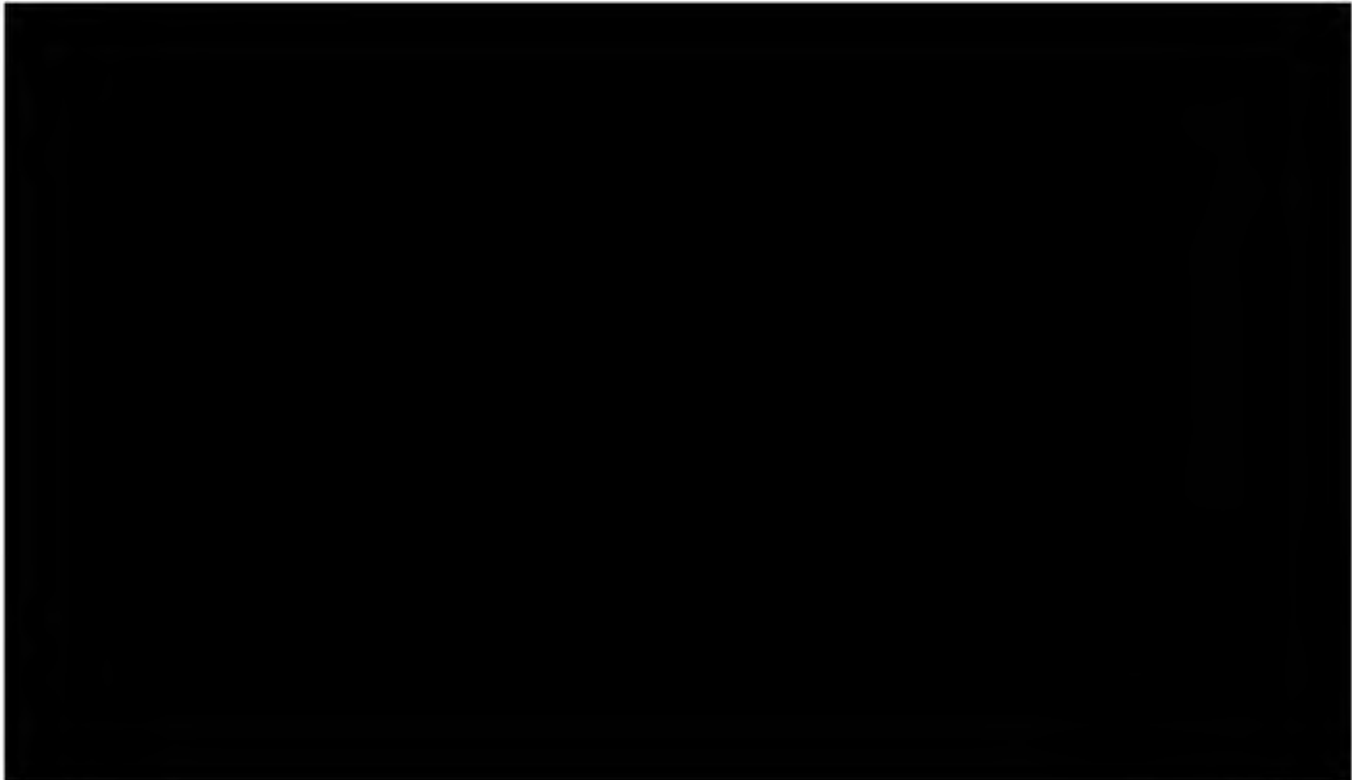
YN	
Ano	1
Ne	0

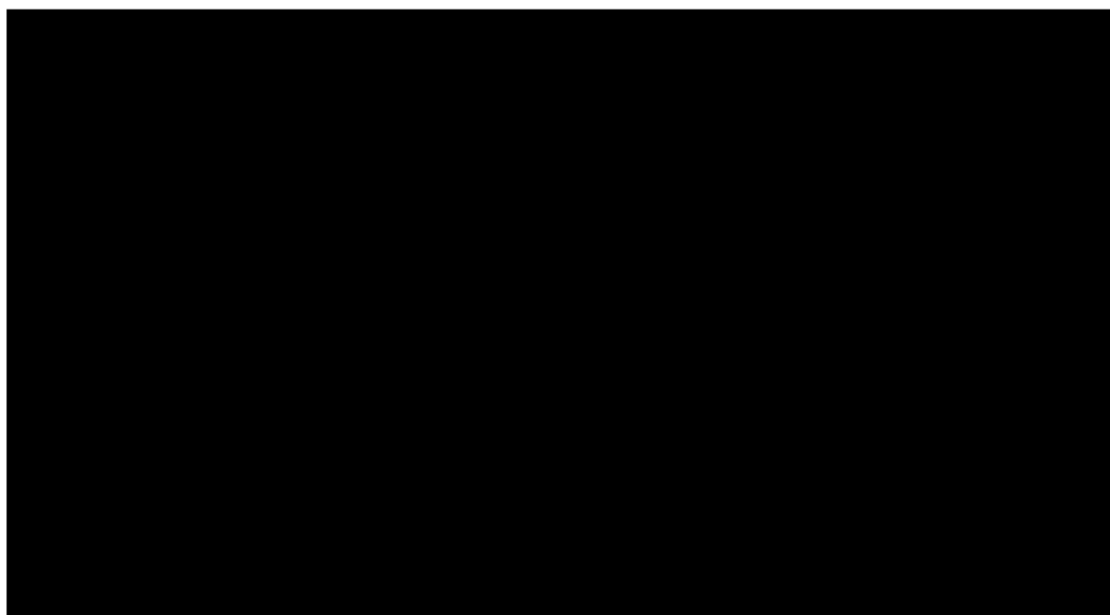
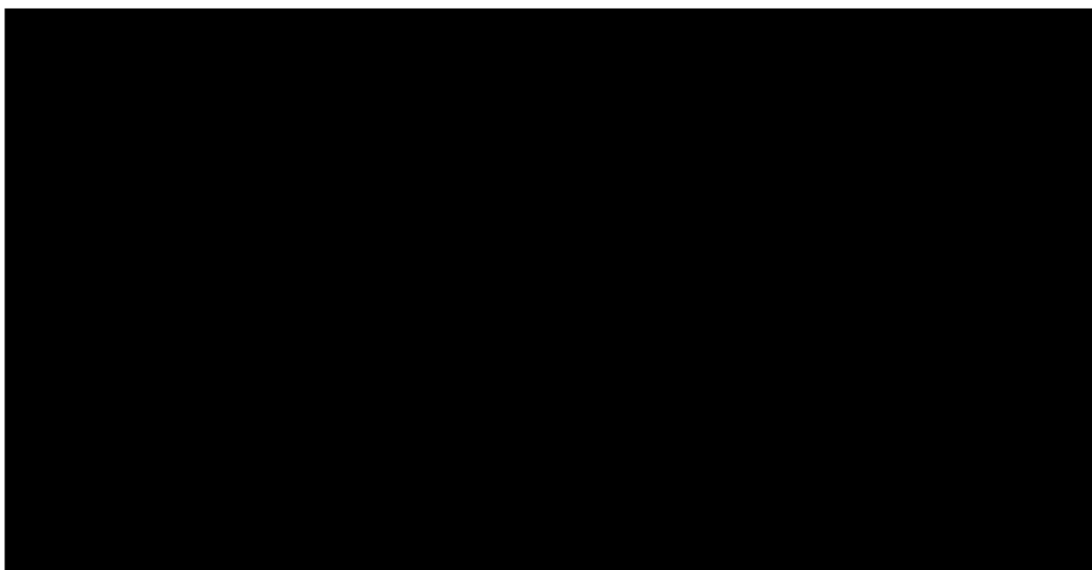
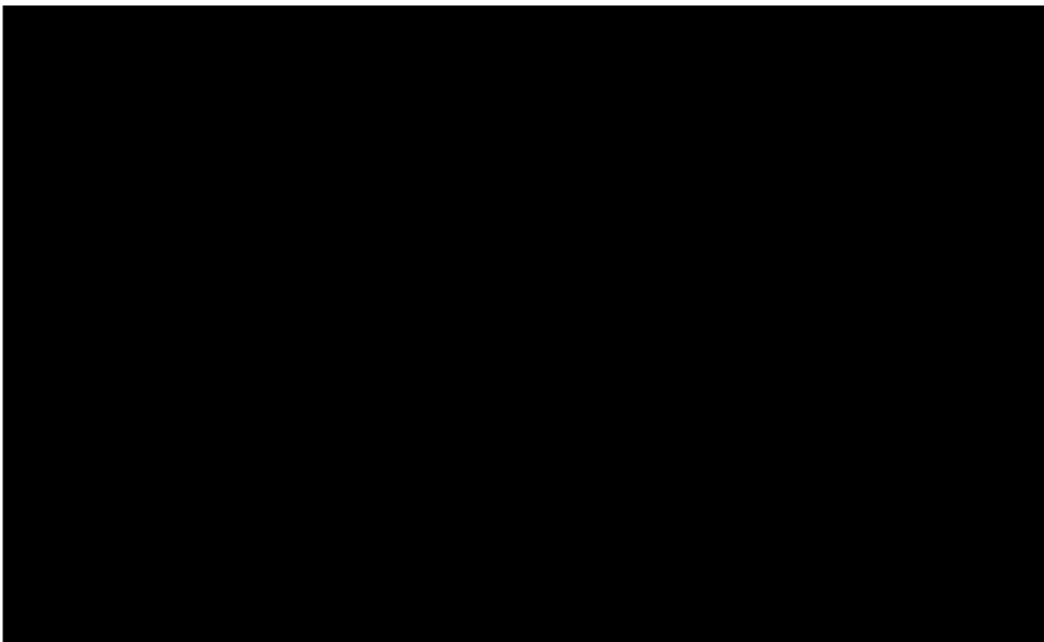
REV	
DRAFT	0
AFIN	1
FINAL	2

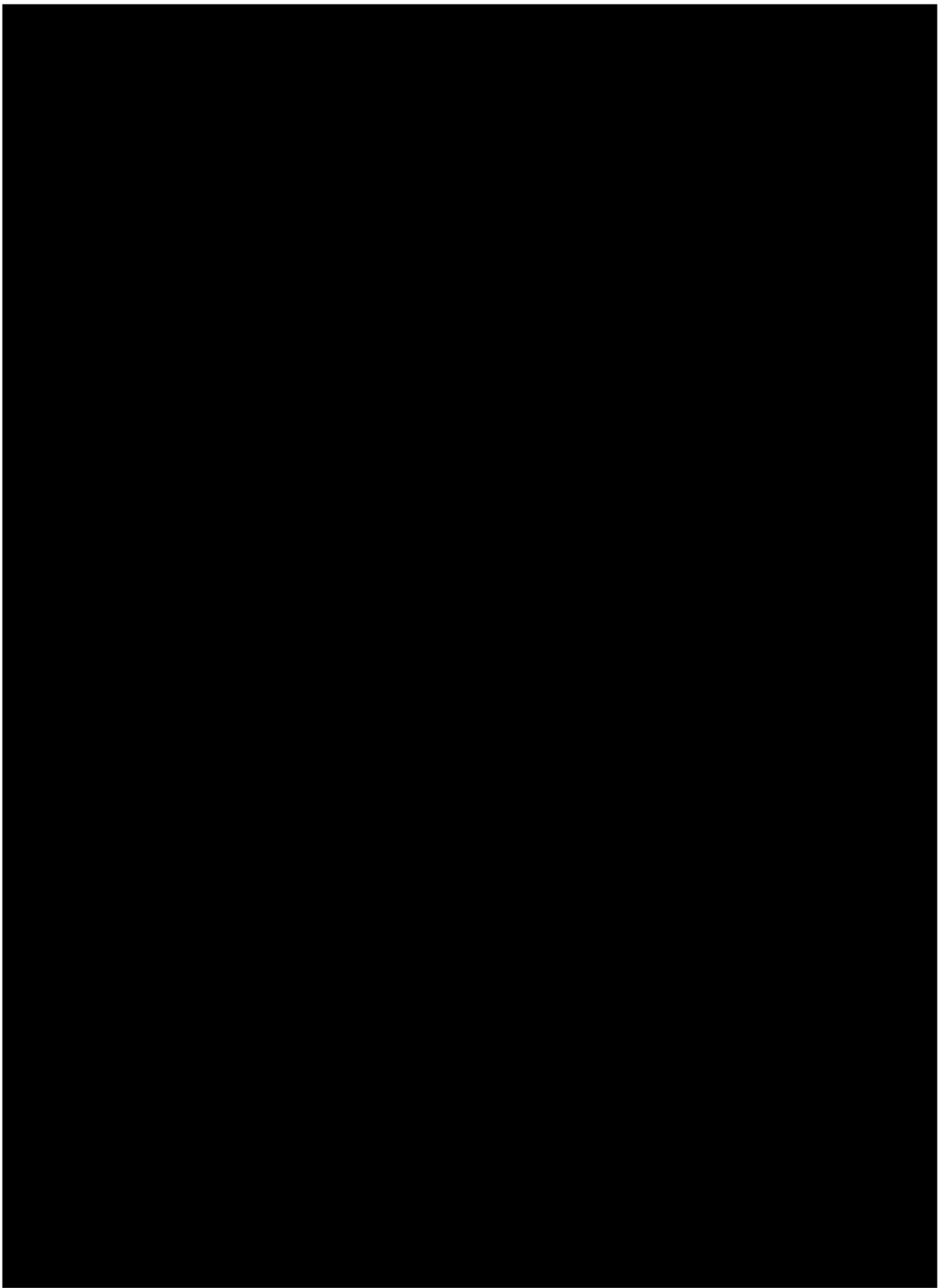
Příloha č.1, část (E): Popis současného stavu MHMP

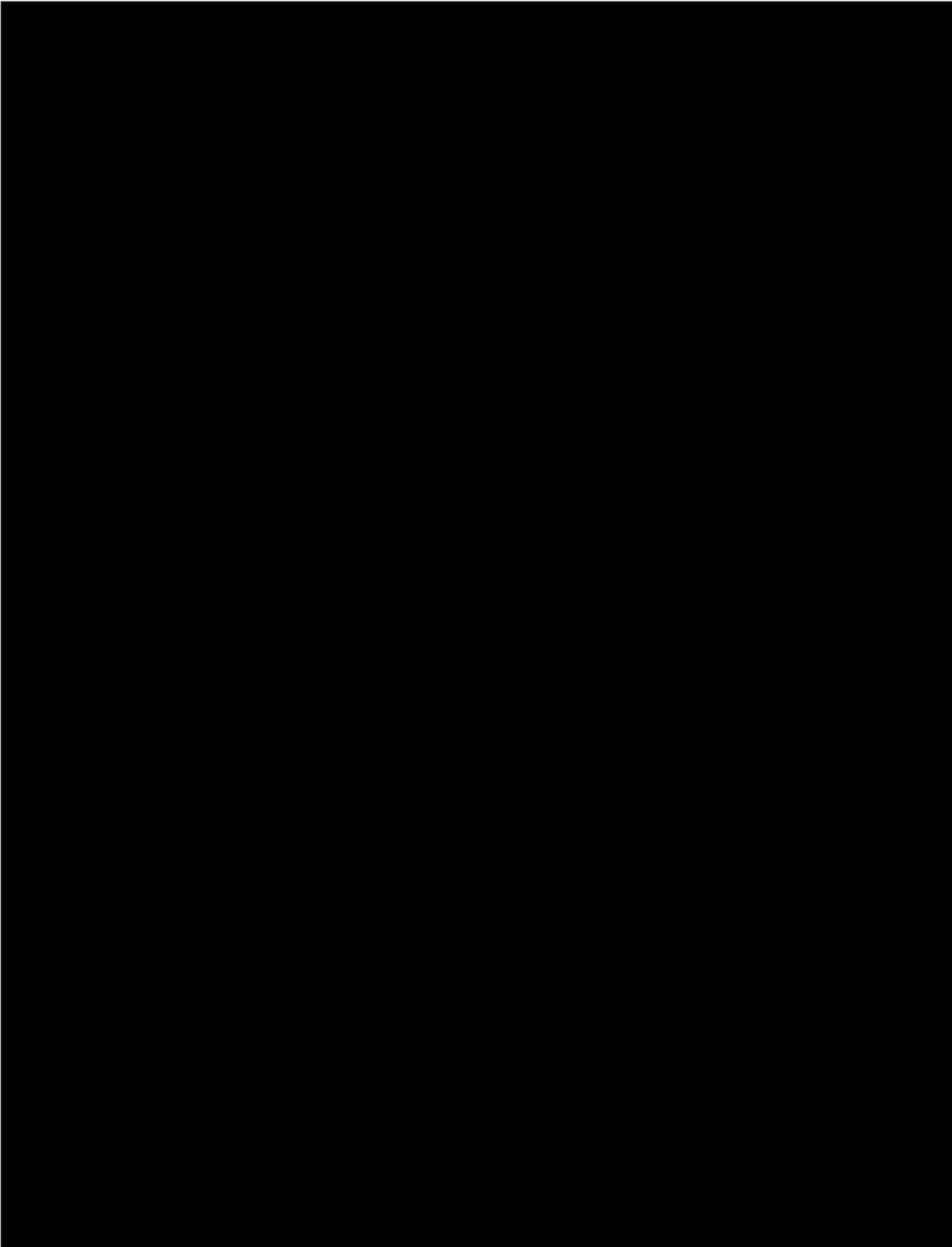


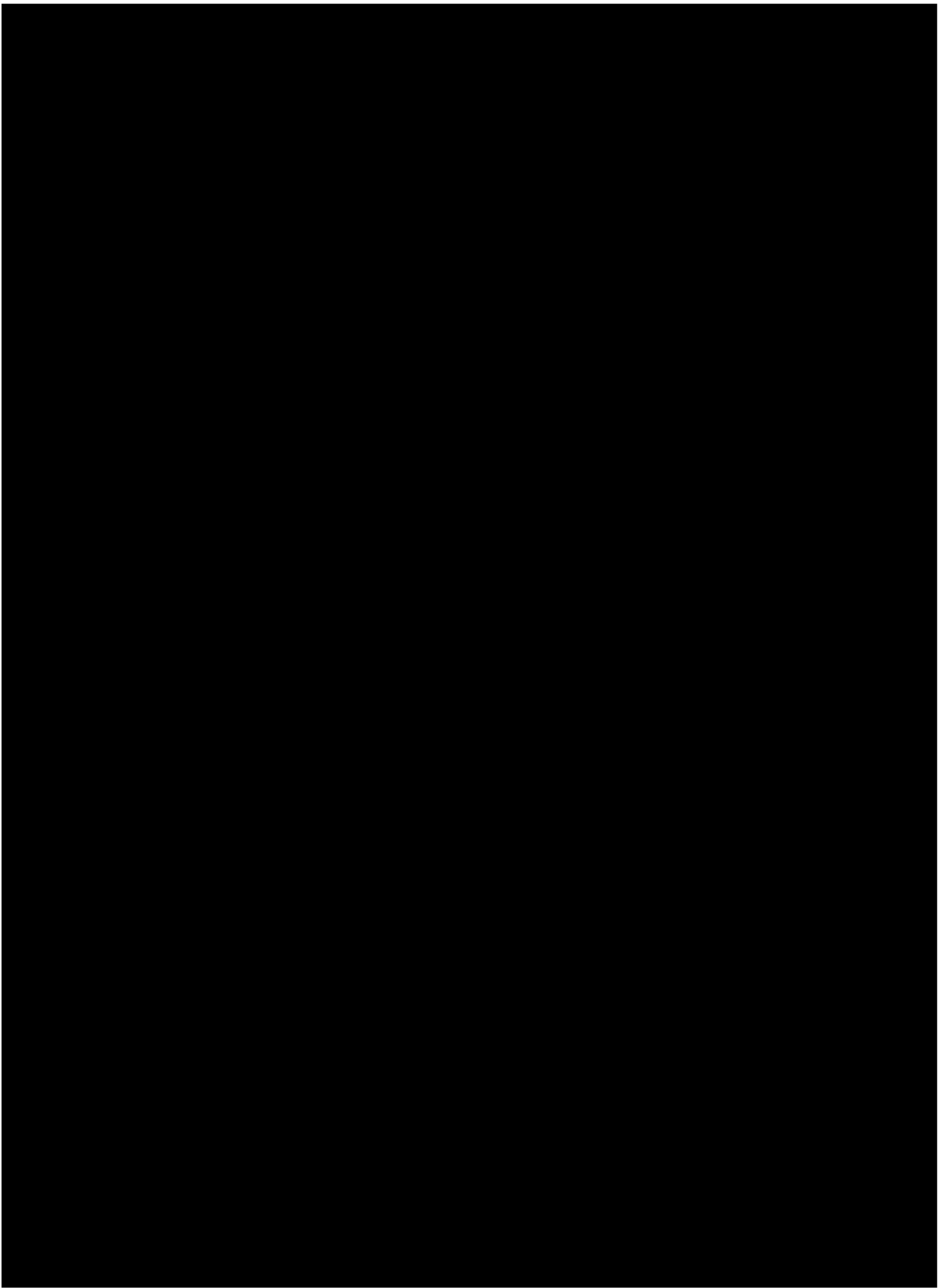


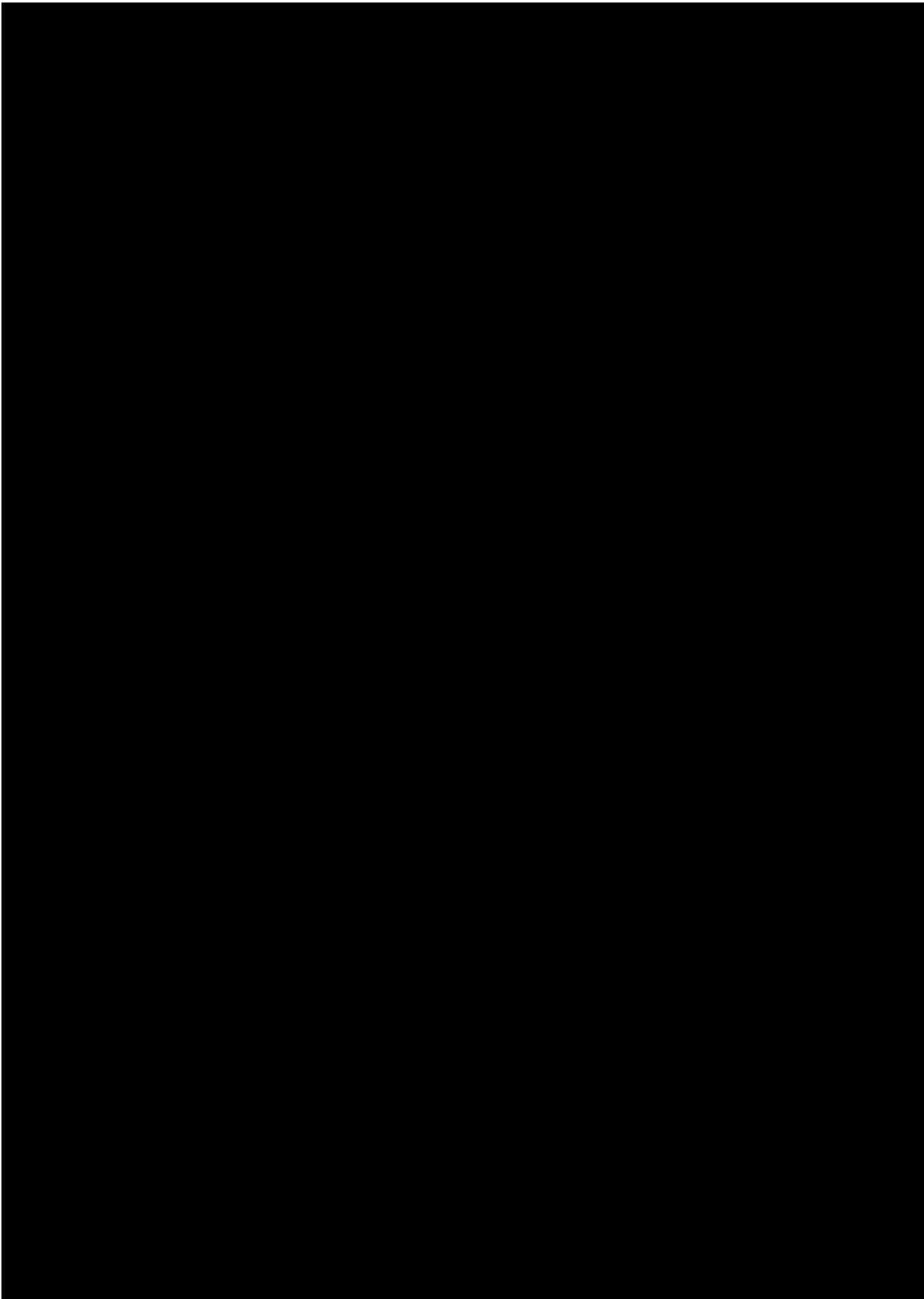


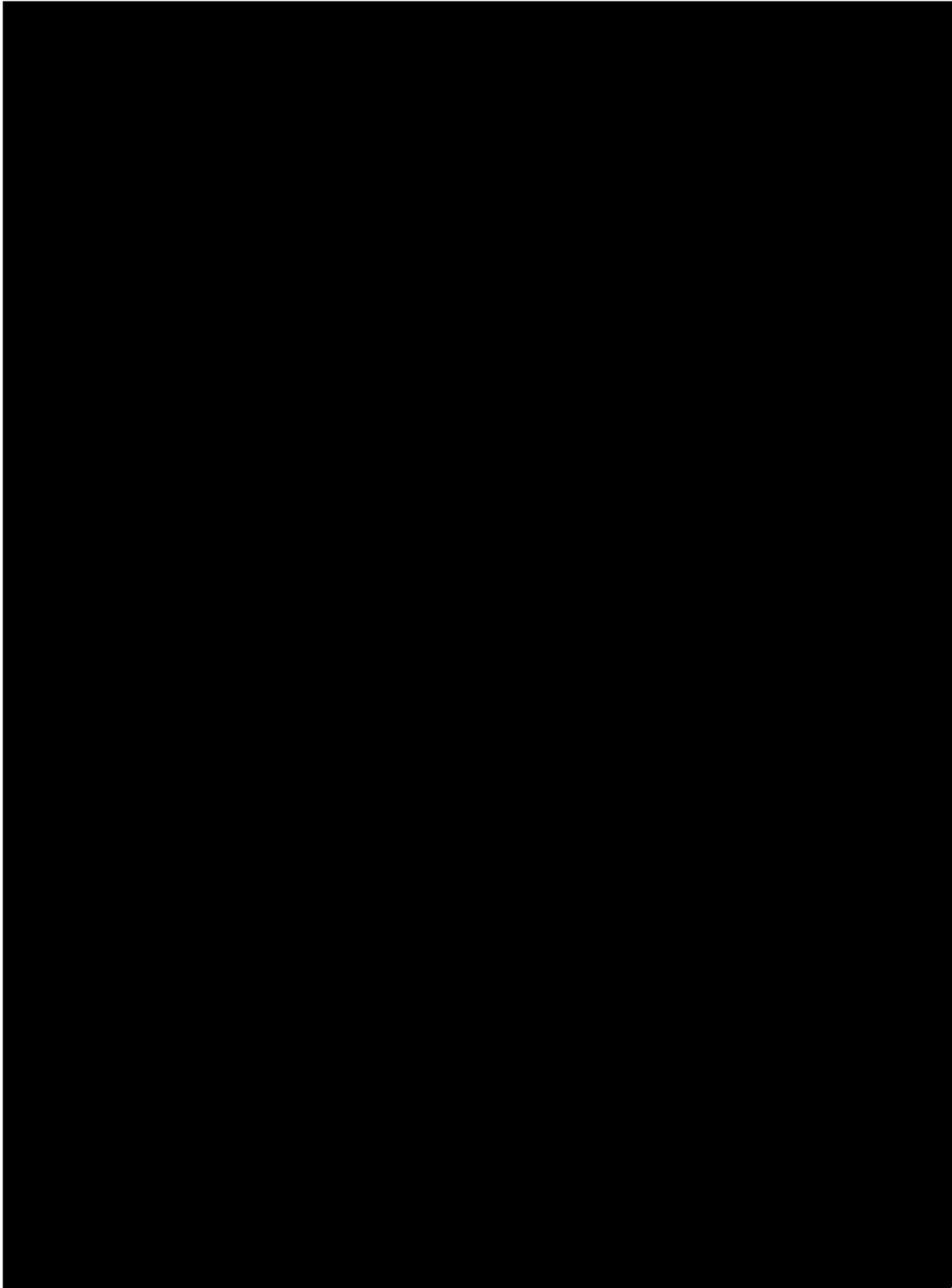


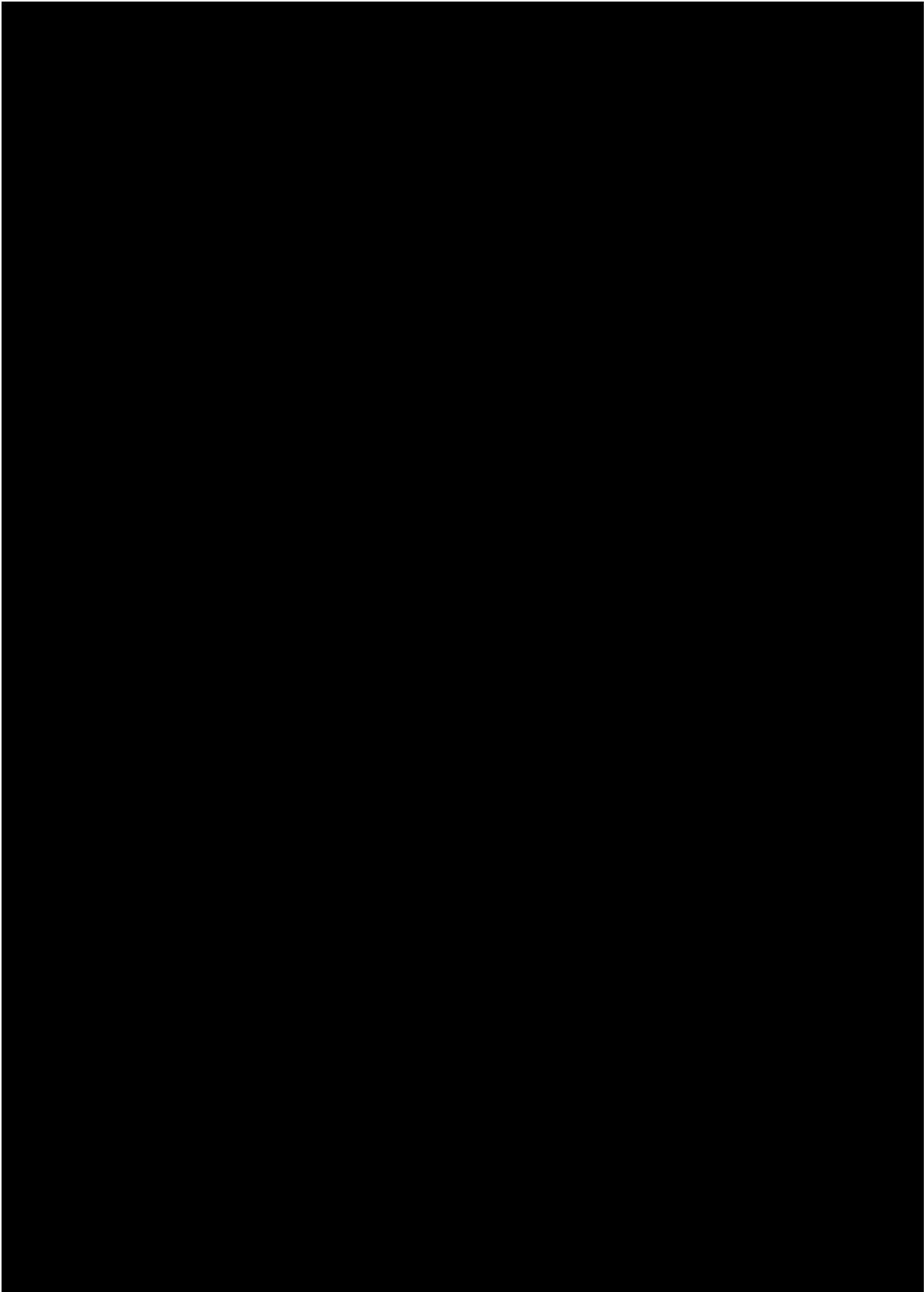


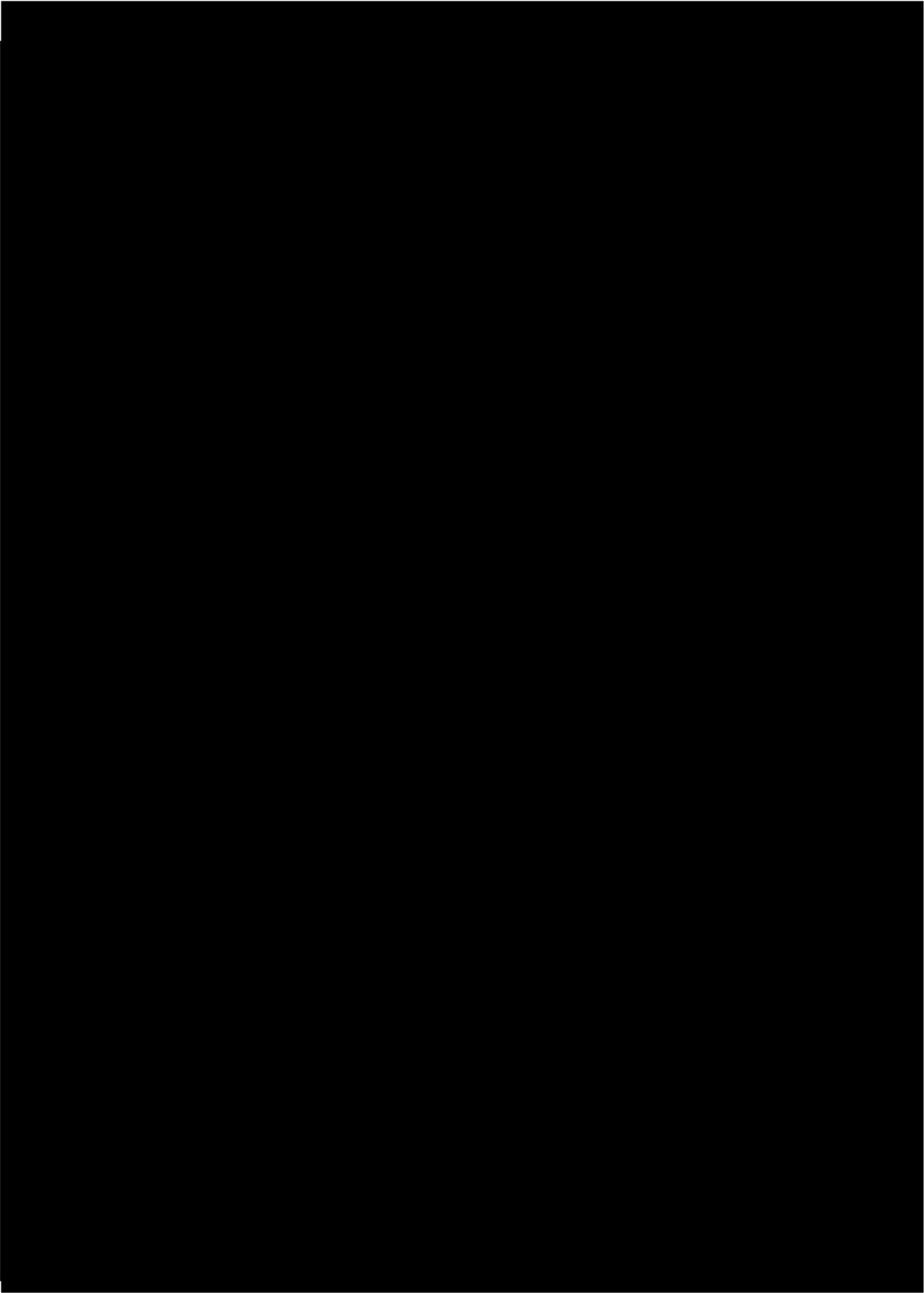


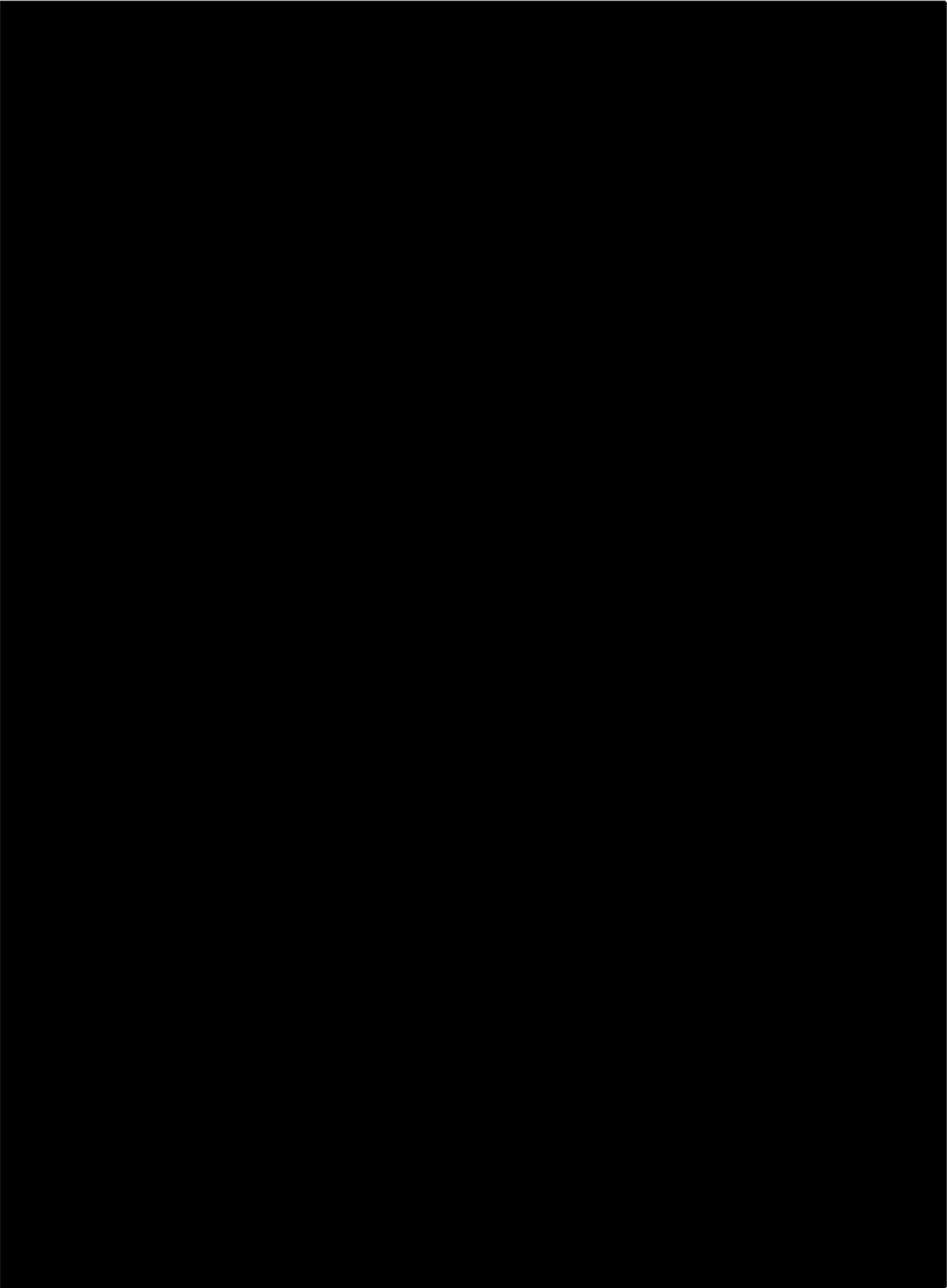


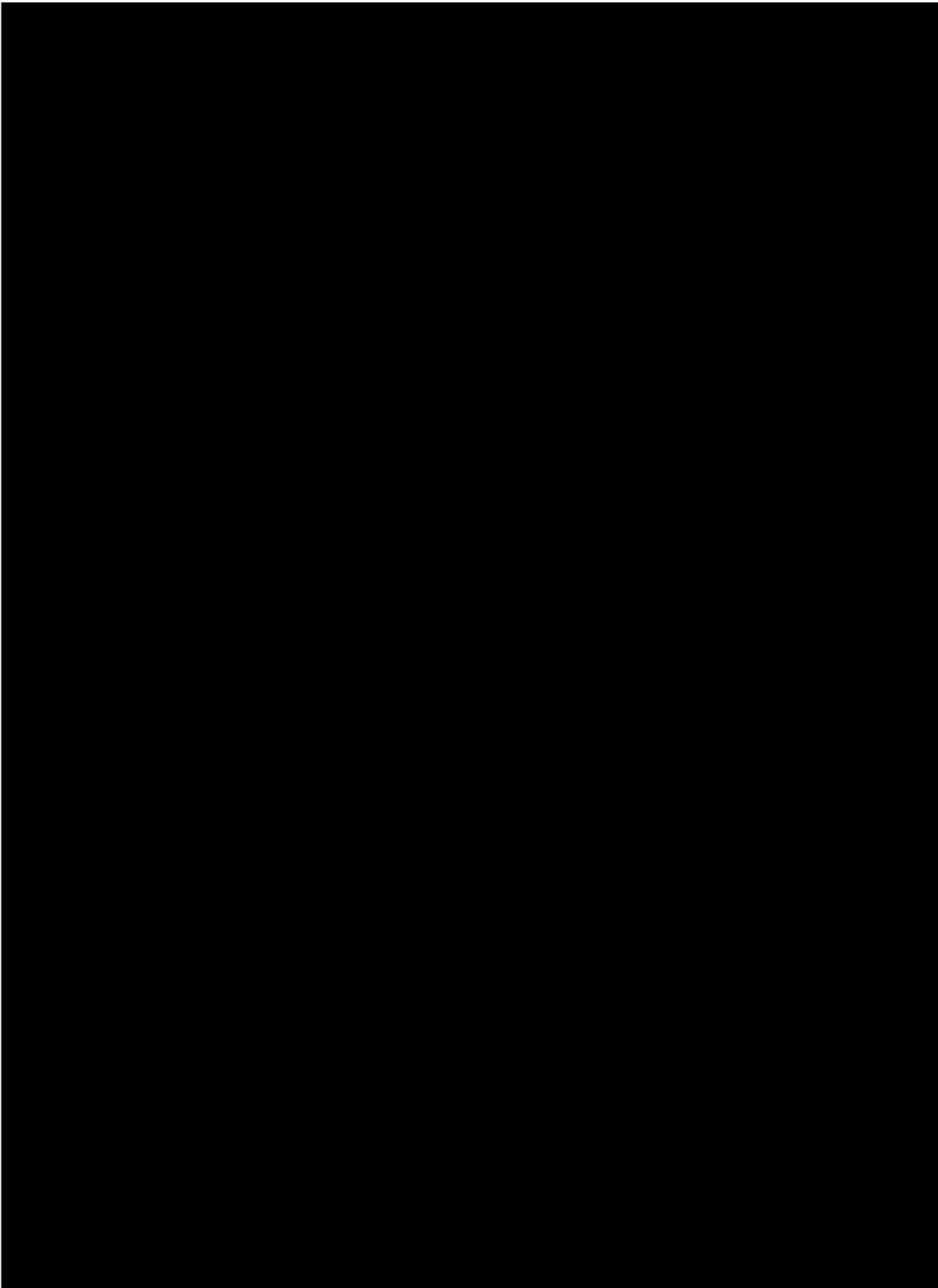


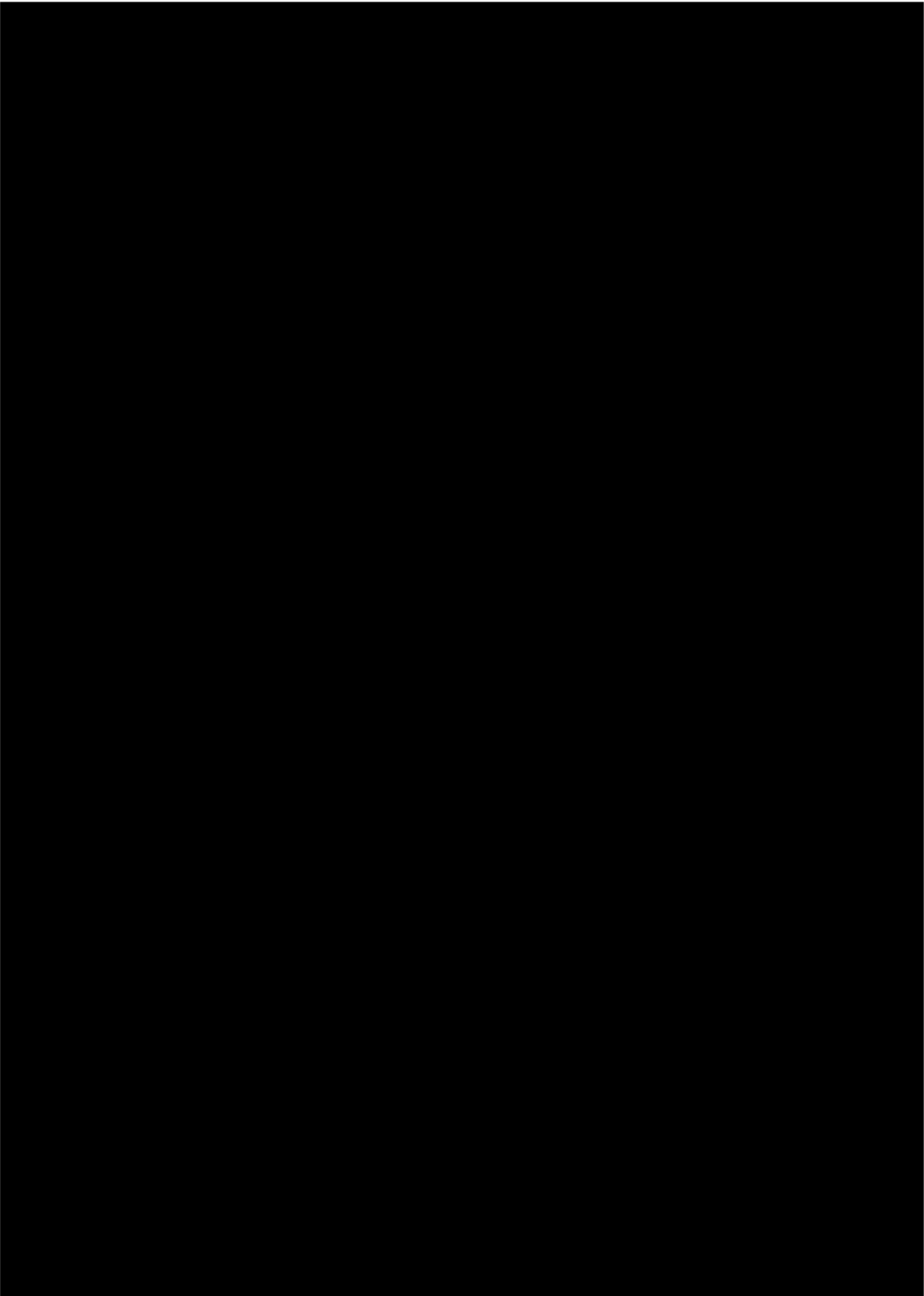


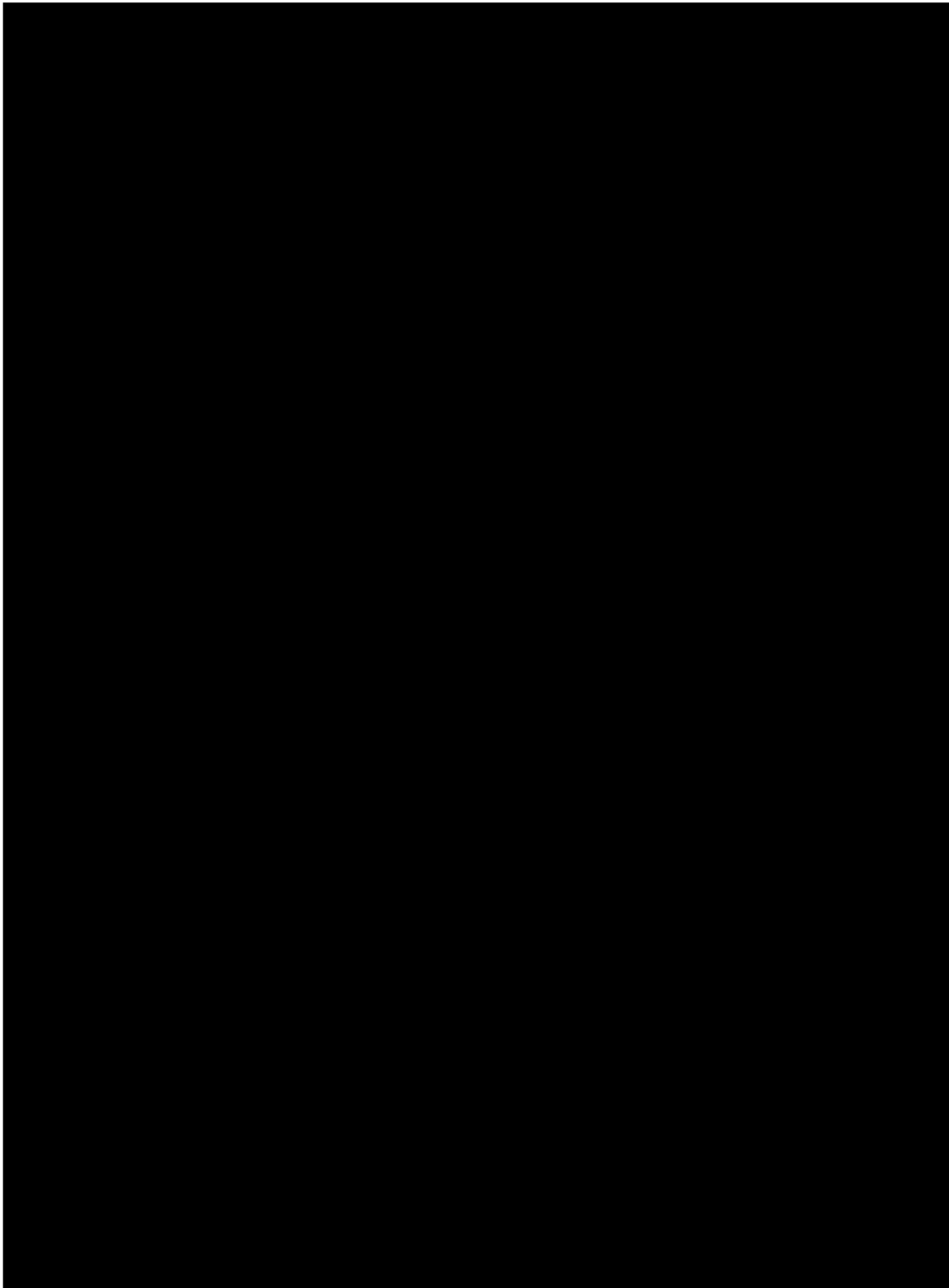


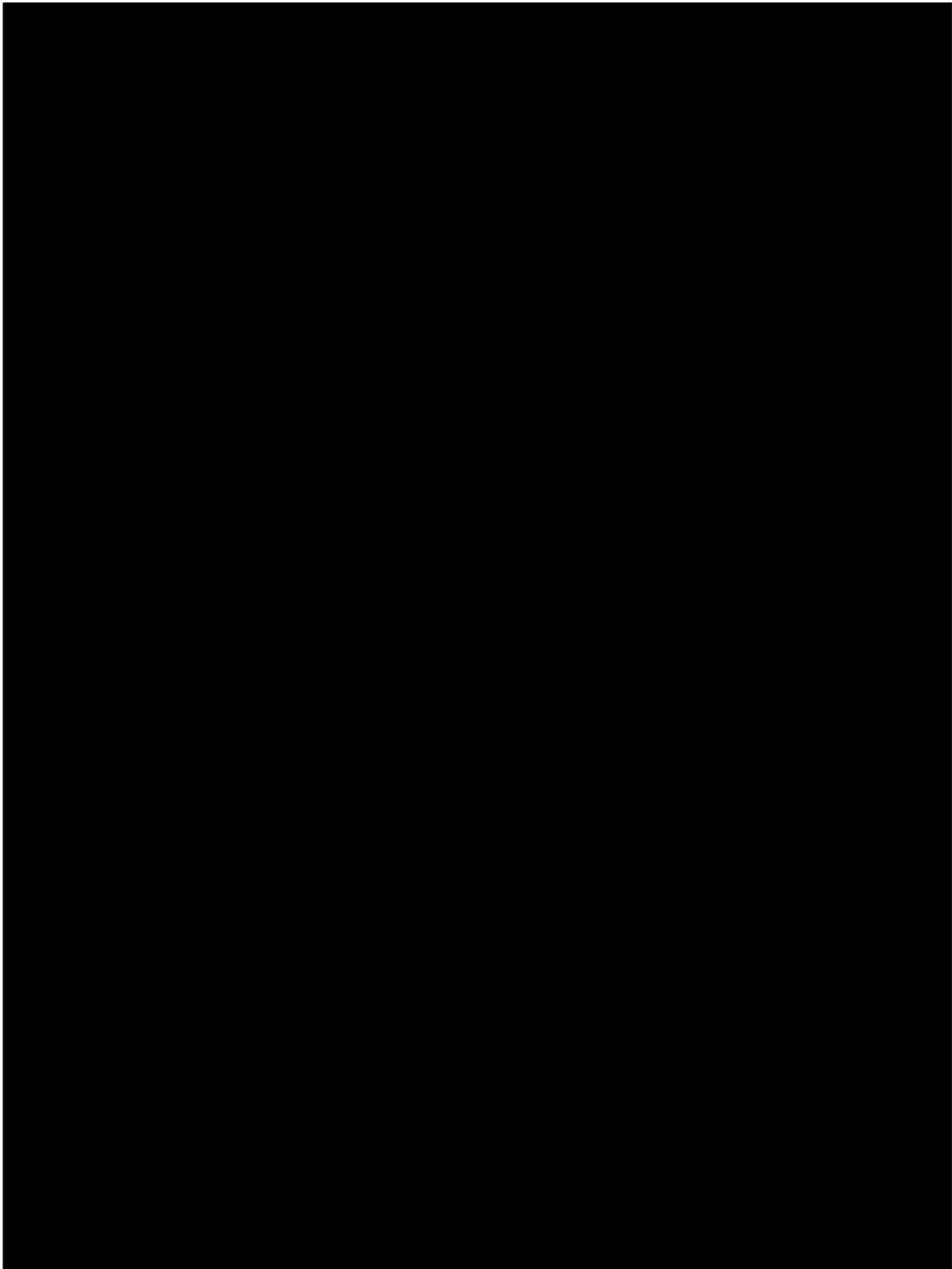


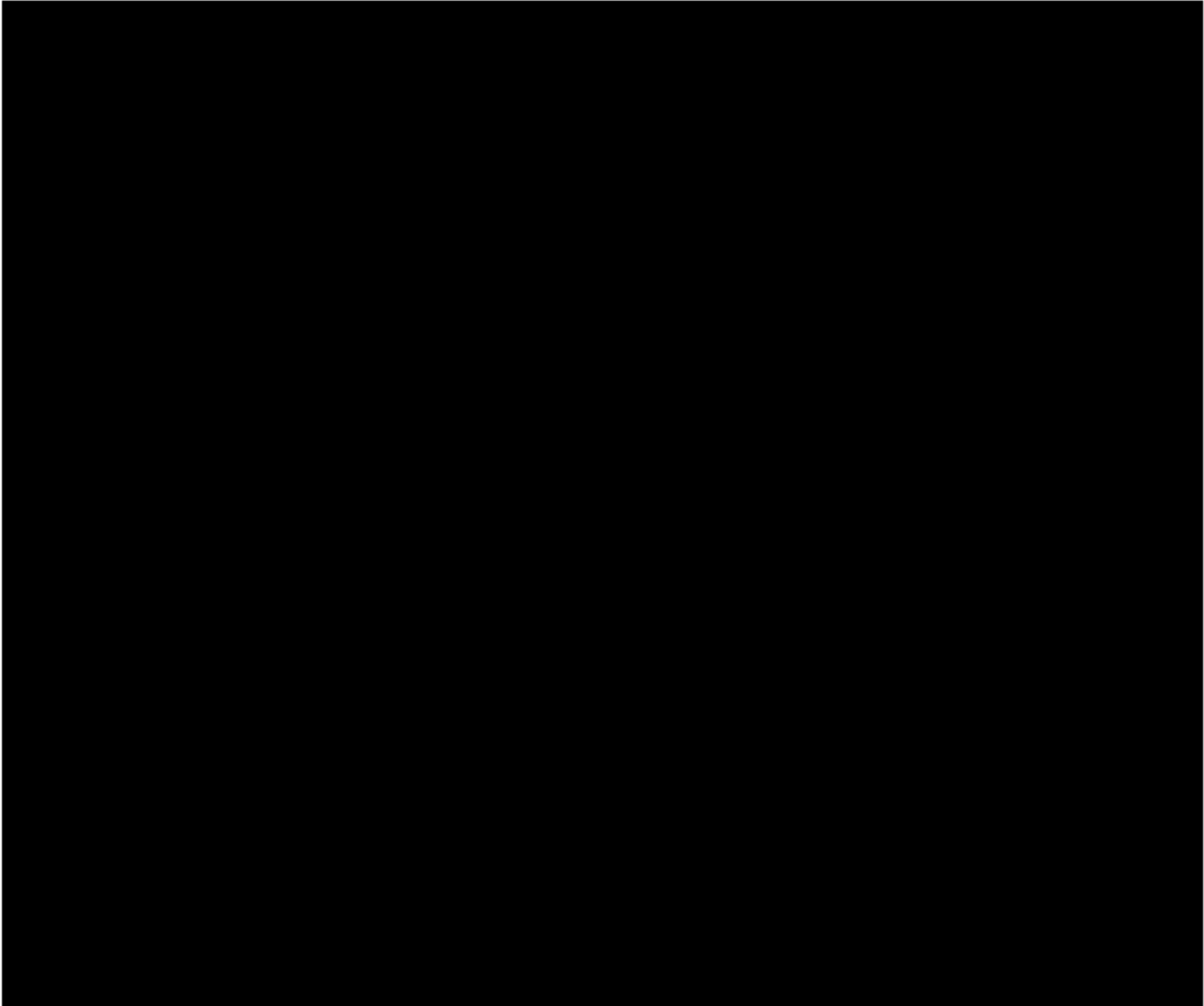






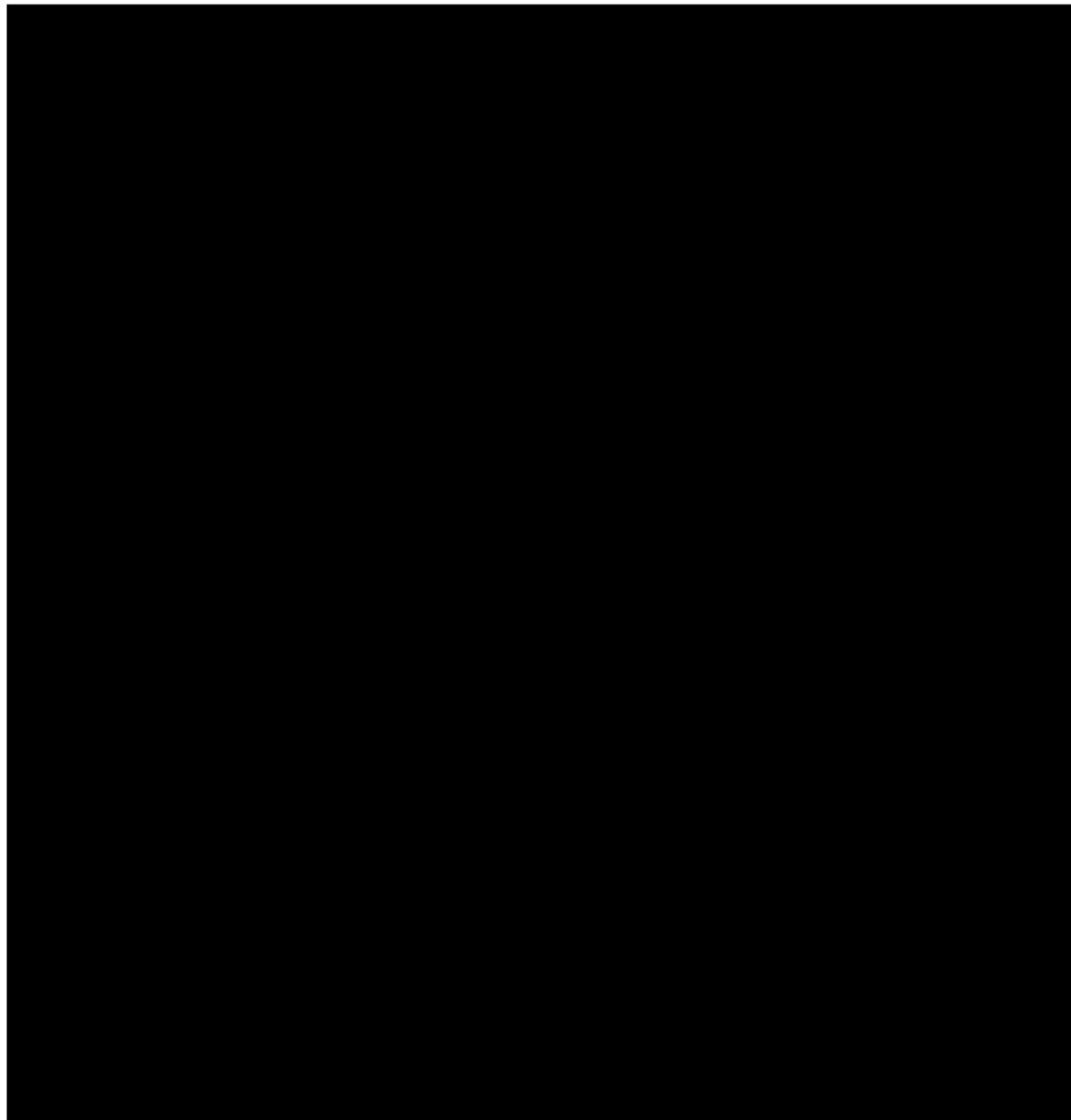




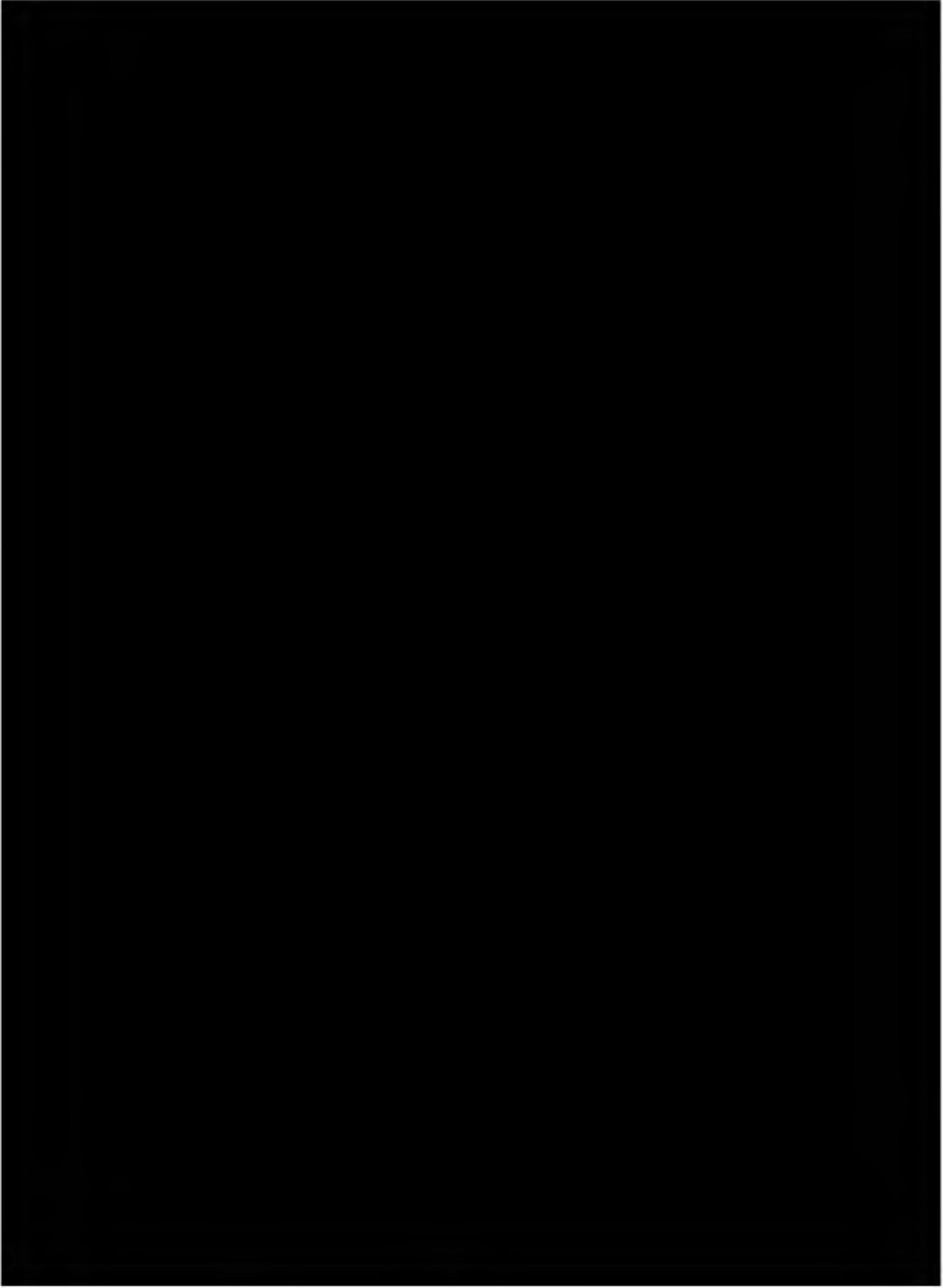


Veřejná zakázka: „Rozvoj a provoz systému pro správu, řízení a monitoring identit v prostředí hl. m. Prahy“

Příloha č.1, část (E): Popis současného stavu MPP







5

6

