Bijlage 2. Begrippen- en afkortingenlijst

Begrip	Gangbare IAM-term	Omschrijving
1. Algemeen		
IAM-systeem		Het Identity & Access Management (IAM)-systeem is de centrale oplossing waarmee de gemeente Zaanstad en haar partnerorganisaties de volledige lifecycle van Identiteiten en Autorisaties ondersteunt en grotendeels automatiseert. Het systeem beheert centraal de registratie van Identiteiten, verwerkt instroom-, doorstroom- en uitstroommutaties en kent op basis daarvan automatisch de juiste Autorisaties toe of trekt deze tijdig in. Daarnaast faciliteert het systeem een gestandaardiseerd aanvraag- en goedkeurproces voor Procesrollen en los aan te vragen Autorisaties. De effectuering van Autorisaties (provisioning) vindt plaats richting aangesloten Doelsystemen.
Opdrachtgever		De aanbestedende dienst die de opdracht tot levering, implementatie en het onderhoud de Oplossing heeft aanbesteed en de daaruit voortvloeiende prestaties gedurende de looptijd afneemt.
Opdrachtnemer		De partij aan wie de opdracht wordt gegund en die de Oplossing, inclusief bijbehorende functionaliteiten, componenten en diensten, levert, implementeert en onderhoudt gedurende de looptijd.

Begrip	Gangbare IAM-term	Omschrijving
Oplossing	IAM Solution / Platform	In deze aanbesteding wordt onder de term Oplossing verstaan: het in het kader van deze aanbesteding aangeboden en te leveren IAM-systeem, inclusief bijbehorende functionaliteiten, componenten en diensten.
Organisatie	Organization / Identity Domain	De Organisatie is de gemeente Zaanstad of een van haar Partnerorganisaties die gebruikmaakt van de Oplossing. Hiermee wordt de juridische entiteit bedoeld waarvoor Autorisaties worden beheerd. Binnen het IAM-systeem vormt de organisatie de context waarbinnen een Identiteit (zoals medewerker, externe, vrijwilliger of stagiair) bestaat. Deze organisatorische context wordt vastgelegd in een Identiteitscontainer, waarin wordt aangegeven tot welke Identiteitssoorten een Identiteit kan behoren.
Partnerorganisatie		De Partnerorganisaties van de gemeente Zaanstad zijn op dit moment: Omgevingsdienst, Gemeente Oostzaan Wormeland, Stichting Jeugdteam, Sociaal Wijkteam en Pact Zaandam Oost.
Gebruiker		Een Gebruiker is iedere natuurlijke persoon die gebruikmaakt van de Oplossing, waaronder Medewerkers, Rolhouders en functioneel- of technisch-beheerders.
2. Identiteitsmodel		
Identiteit	Identity / User	Een Identiteit is een persoon (bijvoorbeeld een medewerker) die aan een organisatie is verbonden en Gebruiker van de Oplossing.
Identiteitssoort	Identity Type / User Type	De Identiteitssoort is het type relatie of dienstverband tussen de Identiteit en de organisatie, zoals: vast dienstverband, externe inhuur, stagiair of BABS (trouwambtenaar).
Identiteitskenmerken		Identiteitskenmerken zijn gegevens uit het HR-systeem of uit handmatige invoer, zoals organisatorische eenheid, arbeidsrelatie, roltoewijzing en dienstverband.
Identiteitscontainer	Identity Store / Identity Domain	De Identiteitscontainer is de organisatorische context binnen de Oplossing waarin een Identiteit wordt geregistreerd en beheerd. De Identiteitscontainer correspondeert met een Organisatie. Elke Identiteitscontainer bevat een verzameling Identiteitssoorten waartoe een Identiteit kan behoren.
IAM-persoonskaart	Identity Profile / User Record	De IAM-Persoonskaart betreft een digitaal overzicht binnen het IAM-systeem met alle relevante gegevens van een Identiteit, waaronder het IAM-account, de Identiteitscontainer en het bijbehorende Contract(en). Dit vormt de centrale bron voor autorisatiebeheer. Deze kaart wordt gesynchroniseerd met het HR-systeem, ISTM en AD.
Contract		Een Contract krijgt een medewerker bij een dienstverband en is onderdeel van de IAM-Persoonskaart. Als een medewerker uitstroomt wordt het contract afgesloten en de IAM-

Begrip	Gangbare IAM-term	Omschrijving
		Persoonskaart op inactief gezet. Als de medewerker weer terug in dienst komt krijgt deze een nieuw contract en wordt de IAM-Persoonskaart weer gereactiveerd.
Topdesk-persoonskaart	Identity Profile / User Record	De Topdesk-persoonskaart betreft een digitaal overzicht binnen Topdesk met alle relevante gegevens van een medewerker, bedoeld voor IT- en facilitaire processen. Deze kaart wordt vanuit het IAM-systeem aangemaakt, gevuld en gemuteerd. Een persoonskaart kan geïnactiveerd worden en bij herinstroom weer geheractiveerd worden.
3. Autorisatiebeheer		
Autorisatie	Role / Entitlement	Een Autorisatie is een logische eenheid (minicontainer) binnen het IAM-systeem en bestaat uit één of meerdere Resources. De naam van een autorisatie is voor de organisatie herkenbaar en leesbaar en wordt gebruikt om gekoppeld te worden aan een Procesrol, HR-attribuut of kan als een zelfstandige entiteit aangevraagd worden.
ICT-rol	Role / Entitlement	In sommige IAM-systemen wordt de term *ICT-rol* gebruikt voor toegangsrechten. Deze term is verwarrend, omdat een rol ook kan leiden tot niet-ICT-voorzieningen (zoals een toegangspas). Daarom hanteren wij in dit document de term Autorisatie als overkoepelend begrip. In de context van Zaanstad is een ICT-rol synoniem aan een Autorisatie en verwijst deze naar een logisch samenhangend pakket aan resources.
Resource	Permission / Access Right / Asset	Een Resource is een concreet toegangselement of middel dat aan een medewerker kan worden toegekend of ingetrokken, zoals: • Lidmaatschap van een AD-groep in Active Directory • Aanmaken van een domeinaccount en e-mail adres in Active Directory • Een Basis-account in een logisch doelsysteem • Een specifiek gebruikersrecht een logisch doelsysteem • Een fysiek middel, zoals een toegangspas of laptop Een Autorisatie kan uit meerdere resources bestaan.
HR-attribuut	*HR-Driven Role / Entitlement Template → ABAC / automatische toekenning*	Een HR-attribuut wordt aan een Identiteit gekoppeld op basis van één of meerdere Identiteitskenmerken, zoals het type arbeidsrelatie of de rol van leidinggevende. Aan een HR-attribuut zijn één of meerdere Autorisaties gekoppeld. Identiteiten waaraan het betreffende HR-attribuut is toegekend, ontvangen de bijbehorende Autorisaties automatisch.

Begrip	Gangbare IAM-term	Omschrijving
Procesrol	*Business Role / Job Role / Process Role → RBAC*	Een Procesrol is een logische rol binnen een proces waarin de taken, verantwoordelijkheden en benodigde bevoegdheden van een medewerker zijn vastgelegd. Aan een Procesrol zijn één of meerdere Autorisaties gekoppeld die noodzakelijk zijn voor de uitvoering van de betreffende werkzaamheden. Wanneer een medewerker na aanvraag en goedkeuring aan een Procesrol wordt gekoppeld, worden de bijbehorende Autorisaties automatisch toegekend.
4. Governance en rolhouders		
Proceseigenaar	Process Owner	De Proceseigenaar is verantwoordelijk voor een proces en ziet erop toe dat medewerkers binnen dat proces de juiste toegangen hebben om hun taken uit te voeren. Hij of zij moet goedkeuring geven bij nieuwe aanvragen van Procesrollen.
Autorisatie-eigenaar	Asset Owner	Indien een autorisatie als zelfstandige entiteit kan worden aangevraagd, wordt hiervoor een autorisatie-eigenaar aangewezen die verantwoordelijk is voor de goedkeuring van nieuwe aanvragen. Wanneer de autorisatie onderdeel is van een procesrol, vindt goedkeuring plaats door de proceseigenaar. Indien de autorisatie gekoppeld is aan een HR-attribuut, wordt deze automatisch toegekend of ingetrokken op basis van HR-mutaties.
Leidinggevende		De Leidinggevende is de hiërarchisch verantwoordelijke (HR-manager) voor één of meerdere medewerkers en ziet erop toe dat deze medewerkers de juiste procesrollen en los aan te vragen autorisaties hebben om hun werkzaamheden uit te voeren.
Medewerker		De Medewerker is een persoon, bekend als Identiteit binnen de Oplossing, en werkzaamheden verricht binnen de organisatie en/of partnerorganisatie, en waarvoor Autorisaties worden beheerd binnen de Oplossing.
Rolhouders		Rolhouders zijn functionele rollen binnen het IAM-proces, waaronder leidinggevenden, proceseigenaren en autorisatie-eigenaren, die betrokken zijn bij het aanvragen, beoordelen, goedkeuren en beheren van procesrollen en los aan te vragen autorisaties binnen de Oplossing.
5. Provisioning		
Doelsysteem	Target System / Managed System	Een Doelsysteem is een uitvoeringskanaal waarin opdrachten voor het toekennen of intrekken van resources worden verwerkt. Binnen deze aanbesteding worden twee typen doelsystemen onderscheiden:

Begrip	Gangbare IAM-term	Omschrijving
		1. Geautomatiseerde uitvoeringskanalen Active Directory (AD) en Microsoft Entra ID, waarin toekenning en intrekking van resources automatisch plaatsvinden op basis van directe koppeling met het IAM-systeem. 2. Ticket-based uitvoeringskanalen TOPdesk en e-mail, waarin toekenning en intrekking handmatig worden uitgevoerd op basis van een door het IAM-systeem gegenereerde Bundelticket. De verwerking vindt plaats door een functioneelbeheergroep in TOPdesk of door de ontvanger van de e-mail.
Logisch Doelsysteem	Downsteam System	Een Logisch Doelsysteem is een applicatie zonder directe technische koppeling met het IAM-systeem. De verwerking van opdrachten vindt plaats via handmatige uitvoering door een functioneelbeheergroep, op basis van door het IAM-systeem gegenereerde Bundeltickets. Er is voor applicaties dus geen directe koppeling met IAM voor geautomatiseerde provisioning.
Wijzigingssjabloon	Ticket Template / Workflow Template	Een Wijzigingssjabloon is een template binnen het IAM-systeem of Topdesk dat wordt gebruikt voor het genereren van een Bundelticket voor een ticket-based doelsysteem. Elk Logisch doelsysteem beschikt over een eigen wijzigingssjabloon. Die is gekoppeld aan een functioneelbeheergroep (routing in Topdesk) of aan een e-mailadres. Het wijzigingssjabloon bepaalt de opmaak en structuur van de opdracht. Het IAM-systeem vult hierin de relevante inhoud in. De gekoppelde functioneelbeheergroep of het e-mailadres bepaalt vervolgens de routing naar Topdesk of e-mail.
Bundelticket	Provisioning Ticket / Workflow Request	Een Bundelticket is een door het IAM-systeem automatisch gegenereerde uitvoeringsopdracht voor een Ticket-based Doelsysteem voor het toekennen of intrekken van Autorisaties. Het bundelticket is gebaseerd op een wijzigingssjabloon en bevat uitsluitend de relevante wijzigingen (delta) ten opzichte van de actuele situatie.
Functioneelbeheergroep	Application Owner Team / Functional Support Group	Een Functioneelbeheergroep is een groep medewerkers die verantwoordelijk is voor het functioneel beheer van één of meerdere applicaties of het uitreiken van fysieke middelen. Zij ontvangen in Bundeltickets in Topdesk voor het intrekken, wijzigen of verstrekken van Autorisaties en verwerken deze opdrachten handmatig.

Begrip	Gangbare IAM-term	Omschrijving
6. Bronsystemen en doelsystemen (integraties)		
HR-systeem	HR System / Source of Truth	Een HR-systeem is de applicatie waar personeelsgegevens vandaan komen. Voor deze aanbesteding is dat YouForce, daarnaast is het ook handmatige invoer voor partnerorganisaties direct in het IAM-systeem.
AD	Directory Service	Active Directory (AD) is het centrale systeem voor het beheren van domeinaccounts, e-mailadressen en AD-groepslidmaatschappen (verspreid) van Identiteiten. Toevoegen, wijzigen en verwijderen gebeurt op basis van opdrachten vanuit het IAM-systeem. AD synchroniseert periodiek met Microsoft Entra Id.
ITSM	IT Service Management System	IT Service Management (ITSM) is het systeem voor het ondersteunen van IT- en facilitaire processen. Voor deze aanbesteding verwijst ITSM naar de applicatie Topdesk, die wordt gebruikt om via bundeltickets (opdrachten) aan functioneel beheer te verstrekken voor het toekennen of intrekken van Basis-accounts en gebruikersrechten in applicaties.
Topdesk-persoonskaart	Identity Profile / User Record	De Topdesk-persoonskaart betreft een digitaal overzicht binnen Topdesk met alle relevante gegevens van een medewerker, bedoeld voor IT- en facilitaire processen. Deze kaart wordt vanuit het IAM-systeem aangemaakt, gevuld en gemuteerd. Een persoonskaart kan geinactiveerd worden en bij herinstroom weer geheractiveerd worden.
7. Detail resources		
AD-account		Een AD-account is een soort van persoonskaart in AD met informatie zoals het Domeinaccount, emailadres en telefoonnummers.
Domeinaccount	Domain Account / Windows Account	Een Domeinaccount is het Gebruikersaccount waarmee een medewerker inlogt op de Zaanstad-werkomgeving (PC of laptop) en toegang krijgt tot applicaties binnen die omgeving.
Basis-account	Application Account	Een Basis-account is het account dat een gebruiker toegang geeft tot een specifieke applicatie. Samen met de bijbehorende gebruikersrechten stelt dit de medewerker in staat om zijn taken in de applicatie uit te voeren.
Gebruikersrecht	Permission / Privilege	Gebruikersrechten bepalen welke acties een medewerker in een applicatie mag uitvoeren, zoals het bekijken, raadplegen, wijzigen, goedkeuren of muteren van gegevens.
8. Beheer en onderhoud van de Oplossing		
Correctief onderhoud		het herstellen van fouten, gebreken, storingen en kwetsbaarheden in de Oplossing

Begrip	Gangbare IAM-term	Omschrijving
Preventief onderhoud		het proactief voorkomen van verstoringen, beveiligingsrisico's, kwetsbaarheden en mogelijke datalekken
Adaptief onderhoud		aanpassingen noodzakelijk om te blijven voldoen aan geldende wet- en regelgeving en beveiligingsrichtlijnen