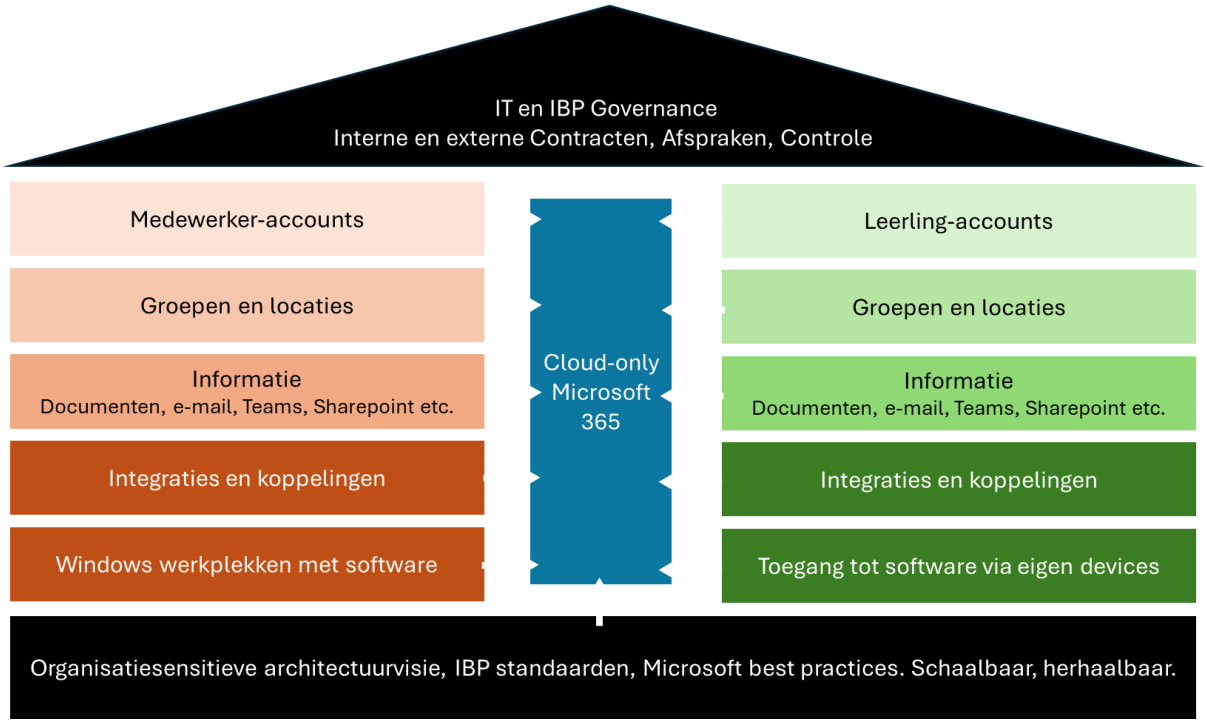
Architectuurkader

Het doel van dit architectuurkader is het vaststellen van richtinggevende kaders en principes voor de inrichting van een toekomstbestendige ICT-infrastructuur. De infrastructuur moet alle scholen binnen de organisatie kunnen faciliteren, met behoud van hun eigen identiteit en autonomie, maar binnen één gezamenlijk beheerd en beveiligd fundament.

De architectuur is visueel weergegeven in onderstaand figuur, waarin de centrale Microsoft 365-omgeving het verbindende fundament vormt tussen medewerkers en leerlingen binnen één governance-structuur.



Kernuitgangspunten

- Greenfield-aanpak: de nieuwe omgeving wordt vanaf nul opgebouwd, zonder afhankelijkheden van legacy-systemen.
- Cloud tenzij: cloud-gebaseerde oplossingen hebben de voorkeur boven on-premises varianten, tenzij aantoonbaar niet passend.
- Security by design en Privacy by design: beveiliging en privacy worden vanaf het ontwerp integraal meegenomen.
- Keep it simple: standaardisatie, eenvoud in beheer en gebruiksvriendelijkheid staan centraal.

- One environment, multiple identities: één centrale omgeving met mogelijkheid voor lokale identiteit (bijv. eigen domein/mailadres per school).
- Compliance: inrichting conform relevante IBP-normenkaders (zoals: het Normenkader IBP FO), Securitybaselines (zoals: de SURF Security Baseline, CIS IG1) en Microsoft best practices.

Functionele en organisatorische kaders

De infrastructuur moet:

- Alle scholen en medewerkers kunnen ondersteunen vanuit één centrale tenant.
- Schaalbaar zijn, zodat eenvoudig nieuwe scholen, gebruikers en diensten toegevoegd kunnen worden.
- Centrale beleidsafspraken afdwingbaar maken via Entra ID en een centrale endpoint managementoplossing, zoals Microsoft Intune of aantoonbaar gelijkwaardig.
- Ondersteuning bieden aan hybride werkomgevingen, met veilige toegang tot applicaties en data op elk type apparaat, ongeacht locatie.
- Toegankelijk zijn voor beheerders via gestandaardiseerde portals en rapportages.
- De inrichting is centraal gestandaardiseerd en uniform waar mogelijk, afwijkingen per school zijn uitsluitend toegestaan indien aantoonbaar noodzakelijk voor het primaire proces en alleen na expliciete besluitvorming binnen de centrale governance.

Technische architectuurprincipes

Identiteit en toegang

- Authenticatie en autorisatie via Microsoft Entra ID (Azure AD).
- Accounts worden als cloud account aangemaakt. Geen hybride constructies, tenzij functioneel noodzakelijk.
- Lifecycle management van accounts (aanmaken, wijzigen, beëindigen) wordt ingericht op basis van betrouwbare bronsystemen, zoals de HR- of leerlingadministratie, waarbij voor medewerkers en leerlingen één of verschillende provisioningsystemen mogelijk zijn.
- Multi-Factor Authentication (MFA) is verplicht voor alle accounts.
- Er wordt zoveel als mogelijk ingezet op het gebruik van Single Sign-On (SSO).
- Role Based Access Control (RBAC) wordt toegepast op beheerfuncties, gevoelige data en gebruikersrechten, gebaseerd op groepen en persona's.

- Beheeraccounts en privileges worden aanvullend beschermd via principes voor privileged access, waaronder gescheiden beheeraccounts waar passend, just in time rolactivatie en noodtoegang (break glass) met streng beheer en monitoring.
- De organisatie hanteert ISO 24760 als referentiekader voor Identity & Access Management. IAM-processen zijn zodanig ingericht dat zij volledig controleerbaar en auditeerbaar zijn. Hierbij wordt gestreefd naar een volwassen vorm van Identity Governance & Administration, zodat toekenning en gebruik van rechten aantoonbaar beheerst verlopen.
- Periodieke herbeoordeling van toegangsrechten (access reviews) wordt ondersteund voor gevoelige rollen, beheerfuncties en externe toegang, zodat rechten aantoonbaar actueel blijven.
- Conditional Access Policies voor toegangscontrole op basis van locatie, apparaatstatus en risicoprofiel.
- Eigen identiteit per school mogelijk door gebruik van meerdere domeinen (bijv. @schoolnaam.nl), gekoppeld aan één tenant.
- De identiteitsvoorziening ondersteunt naast interne accounts ook externe gebruikers, zoals MR leden, externe inhuur, leveranciers en ketenpartners, waarbij de organisatie per doelgroep een passend toegangsmodel kan hanteren.
- Externe toegang kan worden gerealiseerd via beheerde accounts binnen de tenant of via gasttoegang, afhankelijk van risico, duur en benodigde functionaliteit, waarbij de gekozen inrichting centraal beheersbaar, traceerbaar en auditeerbaar is.
- Voor externe toegang worden passende beveiligingsmaatregelen afgedwongen, waaronder MFA, Conditional Access Policies en logging, en geldt dat toegang tot gevoelige gegevens uitsluitend wordt verleend op basis van aantoonbare noodzaak en minimaal benodigde rechten.
- De lifecycle van externe toegang is beheerst ingericht, inclusief registratie, periodieke controle en tijdige intrekking van rechten.

Werkplekken en apparaten

- Alle beheerde werkplekken worden centraal ingericht en beheerd via Microsoft Intune of een aantoonbaar gelijkwaardige endpoint managementoplossing, waarbij beleidsafdwinging, compliance monitoring en rapportage centraal geborgd zijn.
- Alleen geïntegreerde en compliant apparaten hebben toegang tot bedrijfsresources.

- Apparaten worden zero-touch ingericht via Autopilot.
- Bring-Your-Own-Device (BYOD) wordt bij mobiele apparaten enkel toegestaan met Mobile Application Management (MAM)-policies. Overige apparaten (laptops, etc) krijgen toegang via webportalen of beveiligde applicaties zoals MS Teams.
- Alle software-updates, configuraties en applicatieuitrol verlopen centraal via de gekozen beheeroplossing, inclusief monitoring op kwetsbaarheden en updatelevels.

Infrastructuur en hosting

- Primaire omgeving: Microsoft 365.
- Aanvullend gebruik van (Azure of eigen datacenter) Virtual Servers alleen waar functioneel noodzakelijk.
- Geen lokale domeincontrollers, geen hybride join; enkel Entra ID joined devices.
- Storage primair via SharePoint Online, OneDrive en Teams.
- Back-up en retentie ingericht volgens de eisen van het IBP-kader en overige relevante wet- en regelgeving (waar van toepassing), inclusief periodieke hersteltesten en hersteldoelstellingen.
- De aanbestedende dienst beschikt over een lopend contract met AvePoint voor de levering van back-uptooling.

Integraties

- Integratie met onderwijsspecifieke systemen wordt ondersteund zoals Magister, Somtoday en AFAS. Koppelingen moeten gebaseerd zijn op open standaarden (denk aan SCIM, SAML, OAuth 2.0).
- Applicatiecatalogus (goedgekeurde apps, lifecycle en autorisatie).
- Security-governance op API’s (alle API-koppelingen via managed identities of app registrations).

Applicatiebeheer

- Alle “lokale” applicaties worden centraal uitgerold en waar mogelijk geüpdatet via Intune of vergelijkbare thirdparty tooling.
- “lokale” applicaties moeten onderhouden kunnen worden zonder lokale adminrechten.
- Kritieke applicaties worden gemonitord op kwetsbaarheden (CVSS) en update-niveaus.

- Centrale logging en monitoring via Defender for Endpoint en Microsoft 365 Defender.

Informatiebeheer en eigenaarschap

- Informatie volgt de organisatie. SharePoint-sites, Teams-omgevingen en Microsoft 365-groepen worden ingericht op basis van de organisatorische structuur (school, afdeling, project of functie).
- Voor iedere omgeving is een inhouds- en eigendomseigenaar benoemd die verantwoordelijk is voor het beheer van rechten, classificatie en opschoning.
- Beperk wildgroei: aanmaak van Teams en SharePoint-sites verloopt via een gecontroleerd aanvraagproces of sjabloon (governed creation).
- Externe samenwerking en delen van informatie wordt centraal beheerst via vastgestelde deelinstellingen, goedkeuringsmechanismen en periodieke controles, zodat gasttoegang en externe deling beheersbaar blijven.
- Informatieclassificatie en passende beschermingsmaatregelen worden stapsgewijs ingericht, zodat vertrouwelijke informatie herkenbaar is en delen en toegang beheersbaar blijft, passend bij het volwassenheidsniveau van de organisatie en beschikbare licenties.

Beveiliging en compliance

Security by Design

- Zero Trust-architectuur als ontwerpprincipe: nooit automatisch vertrouwen, altijd verifiëren.
- Encryptie by default voor data in rust en in transport.
- Security baselines op systeem- en applicatieniveau verplicht. (Bijv. CIS IG1)
- Baseline configuratie en hardening van Microsoft 365 tenant en workloads (zoals Exchange, SharePoint, OneDrive en Teams) wordt centraal ingericht en periodiek getoetst, passend bij relevante security baselines en best practices (bijv CISA SCuBA).
- Regelmatige kwetsbaarheidsscans en patchmanagement-rapportages verplicht.
- Audit logging, retentie en ondersteuning voor incidentanalyse en forensisch onderzoek zijn geborgd, passend bij het IBP beleid en de risico's van de organisatie.

Privacy by Design

- Verwerking en opslag van persoonsgegevens vindt plaats binnen de EU waar mogelijk en passend binnen de gekozen Microsoft 365 diensten, conform wet en regelgeving en het IBP-beleid.
- Minimale gegevensverwerking, scheiding van rollen en logging van toegang tot persoonsgegevens.
- Privacy-impactanalyses (DPIA's) mogelijk maken door transparantie in architectuur en datastromen.
- Nieuwe functionaliteiten met verhoogde privacy impact, zoals AI assistenten, worden alleen ingezet na passende risicoanalyse, DPIA waar nodig en expliciete besluitvorming.

Eisen aan leveranciers

- De inschrijver moet kunnen aantonen dat:
    - De aangeboden oplossing voldoet aan de bovengenoemde architectuurprincipes.
    - Beheer en implementatie plaatsvinden volgens best practices (Microsoft Cloud Adoption Framework).
    - Er wordt gewerkt conform ISO 27001/27002 of vergelijkbare certificering.
    - Er voorzien wordt in continu beheer en ondersteuning, inclusief security-monitoring en patching.
    - Er continue focus is op hardening en baseline inrichting van de omgeving met oog voor de functionele vereisten vanuit het onderwijs.
    - Rapportages beschikbaar zijn over kwetsbaarheden, updates en compliance.
    - Change- en incidentmanagementprocessen conform IBP-beleid.
    - Focus op een technologische roadmap en lifecyclemanagement voor continue vernieuwing.
- De inschrijver maakt inzichtelijk welke licenties en componenten vereist zijn om de voorgestelde IAM en governance maatregelen (zoals access reviews en externe governance) te realiseren.

Toekomstbestendigheid

- De infrastructuur is modulair en eenvoudig uitbreidbaar.
- Nieuwe technologieën kunnen worden geïntegreerd zonder herontwerp van de basis.

- Gebruik van open standaarden voor interoperabiliteit.
- Voorzien in lifecycle-beheer van hardware, software en accounts.

Referentie-architectuur (voorbeeld)

Hoofdcomponenten:

- Microsoft 365 (Exchange Online, SharePoint Online, Teams, OneDrive)
- Microsoft Entra ID (Azure AD)
- Microsoft Intune
- Defender for Cloud Apps, Defender for Endpoint, Defender for Identity
- (Azure of eigen datacentrum) Virtual Machines (optioneel voor specifieke workloads)
- Log Analytics