

Annex V-A ICT-Landschap van Stichting Catent

1. Inleiding

Het ICT-landschap van Stichting Catent is ingericht om onderwijs en beheer te ondersteunen, met een focus op gebruiksvriendelijkheid, veiligheid en innovatie. De inzet van technologie richt zich op het versterken van het leerproces, het faciliteren van samenwerking en het efficiënt beheren van de organisatie.

2. Technologische infrastructuur

De ICT-infrastructuur binnen Catent bestaat uit:

a. Netwerk en connectiviteit

- Gebruik van een hybride netwerk met bekabelde en draadloze infrastructuur (Wi-Fi 6/5).
- Ruckus WaaS (Wifi as a Service)
- Internettoegang via een centraal beheerde firewall met webfiltering en monitoring.
- VPN-toegang voor medewerkers die op afstand werken.
- Implementatie van VLAN's voor gescheiden netwerken (administratie, onderwijs, gastnetwerk).
- Beheerde router (Fortigate) op elke school/locatie.
- Bij een aantal scholen zit er nog een router met modem functie voor geïnstalleerd

b. Werkplekken en devices

- Alle medewerkers beschikken over een beheerde laptop of desktop (Windows/MacOS).
- Leerlingen maken gebruik van Chromebooks/iPads, afhankelijk van de onderwijsbehoefte.
- Centrally managed Mobile Device Management (MDM) systeem voor beheer en beveiliging (Jamf, Apparaatbeheer Cloudwise).

c. Servers en opslag

- Cloud-first strategie met Microsoft 365 als kernplatform.
- Beveiligde dataopslag en toegangsbeheer via Microsoft OneDrive en SharePoint.

3. Software en applicaties

a. Onderwijsapplicaties

- Google Workspace for Education en Microsoft 365.

- Educatieve software voor taal, rekenen en digitale geletterdheid (Gynzy, Snappet, Basispoort/MOO).
- ParnaSsys en LOVS

b. Administratieve software

- HRM-systemen Youko en Visma
- Tobias voor begroting en rapportages.
- Planning en communicatie via Microsoft Teams en Outlook.

c. Beveiliging en compliance tools

- Microsoft Defender for Endpoint voor endpoint security en threat detection.
- implementatie van het normenkader informatiebeveiliging en privacy (IBP).
- Two-Factor Authentication (2FA)* en Single Sign-On (SSO) voor O365.

* alleen buiten schoollocaties

4. Beveiliging en privacy

De organisatie hanteert een strikt beleid op het gebied van informatiebeveiliging en privacy, gebaseerd op het normenkader IBP:

- Regelmatige awareness-trainingen voor medewerkers en leerlingen.
- Periodieke audits en penetratietesten met Microsoft Defender E5.
- Data Protection Officer (DPO) en Functionaris Gegevensbescherming (FG) betrokken bij compliance.
- Incident response plan/Desaster recovery plan en dataherstelstrategieën voor crisissituaties.

5. Ondersteuning en beheer

- Een centrale ICT-helpdesk voor ondersteuning van medewerkers en leerlingen (Cloudwise).
- Gebruik van remote management tools zoals Intune voor devicebeheer.
- Een laag over Intune (apparaatbeheer) om beheer toegankelijk te maken voor scholen/locaties
- Regelmatige evaluatie en upgrades van de infrastructuur.