

Enterprise Architectuur

Colofon

Documentnaam Bijlage 6.3 Enterprise Architectuur

Titel Enterprise Architectuur @voCampus

Referentienummer

Versie en datum 28-3-2023

Referentie

Samengesteld door

Gerelateerde documenten

Titel	Versie	Auteur	Onderwerp

Versiebeheer

Datum	Status	Versie	Auteur	Omschrijving
30/11/22	Draft	0.1	JvdP	Eerste opzet referentie architectuur
16/12/22	Concept	0.2	JvdP	Definitief concept ter interne beoordeling @voCampus.
03/04/23	Definitief	1.0	BS	

INHOUDSOPGAVE

1.1	Uitleg van de Principes:.....	4
1.2	Rollen en verantwoordelijkheden.....	4
2	ORGANISATIE.....	7
3	ALGEMEEN	8
4	IDENTITEITEN.....	12
5	BEVEILIGING	18
6	DATA	21
7	APPLICATIES	23
8	WERKPLEK	25
9	INFRASTRUCTUUR.....	28

Pijlers waarop de infrastructuur wordt gebouwd:

- | | |
|----------------------|--|
| 1. Veiligheid: | - integraal toegepaste (cyber)security/ compliance |
| 2. Continuïteit: | - capaciteit en beschikbaarheid |
| 3. Financieel (IST): | - investeringen vs. operationele kosten? |
| 4. Kwaliteit: | - performance, flexibiliteit, incidenten |
| 5. Efficiëntie: | - standaardisatie |

Dit document beschrijft de overkoepelende (Enterprise) Architectuur. De input hiervoor is opgehaald in de workshop op 14 november 2022 beschrijft de kaders en regels waaraan de inrichting van de ICT-infrastructuur binnen @voCampus moet voldoen. Het gaat dan om het samenspel van ICT-fundament en de onderwijs specifieke ICT-toepassingen. De uitgangspunten van de EA zijn gebaseerd op de ICT-strategie die is afgeleid van de organisatie-strategie. Dit document is in domeinen opgedeeld. En biedt daarmee een kapstok voor domeinarchitectuur(en).

1.1 Uitleg van de Principles:

Dit document is opgedeeld in domeinen. Per domein zijn er richtlijnen geformuleerd. Daar wordt het volgende kader voor gebruikt:

1. Omschrijving van het architectuur principe + volgnummer.	Actief: ja / nee. Indien dit principe is opgevolgd door een nieuwe, voegen we de verwijzing naar dat principe toe. We behouden ook de oude principes om hiermee de ontwikkeling c.q. context te duiden.
<i>Rationele: Waarom er gekozen is voor dit principe. Met eventueel extra context om het principe beter te kunnen duiden.</i>	
<i>Bronnen: Optioneel. Verwijzing naar documenten.</i>	

1.2 Rollen en verantwoordelijkheden

De volgende rollen worden geïdentificeerd voor het succesvol uit kunnen oefenen van een hoogwaardige IT-organisatie:

Enterprise Architect. Is verantwoordelijk voor het uitwerken van de 'Visie & Strategie' op bedrijfsniveau; heeft kennis en ervaring met alle architecturaspecten en de consistentie en aansluiting tussen die aspecten bewaakt.

Veiligheidsadviseur. Zorgt voor technische en organisatorische maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie te garanderen.

Financieel verantwoordelijke. Is verantwoordelijk voor de financiële doelstellingen van een bedrijf en is verantwoordelijk voor de budgetten.

IT (Operations) manager. Eindverantwoordelijke voor de specifieke IT-organisatie. Stelt een overkoepelende IT-visie en strategie op. Verankerd deze in de organisatie.

Domein architect. Een domeinarchitect heeft diepgaande kennis over een gekaderd stuk, bijvoorbeeld *Werkplekken*. Een domeinarchitect verzorgt de afstemming met de *Enterprise Architectuur (EA)* en het overeenkomen met de *Enterprise Architectuur* standaarden & richtlijnen. De Domein Architect definieert aanvullende voorwaarden op basis van de EA voor haar domein.

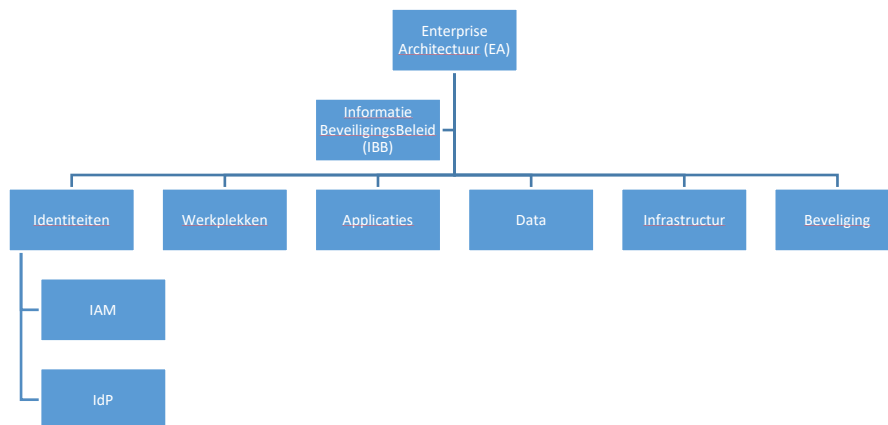
(Principal) Engineer. Letterlijk: technisch voorman. Is het centrale aanspreekpunt voor alle technisch gerelateerde zaken. Heeft vergaande kennis van de technische inrichting van de omgeving. Is een spreekbuis tussen de organisatie en de techniek.

Adoptie/ Communicatie consultant. Slaat een brug tussen de gebruiker en de techniek. Vertelt over de *Waarom* en *Hoe*. Weet mensen te bereiken en hen mee te nemen in veranderingen. Haalt ervaringen en inzichten uit het werkveld op. En neemt deze mee naar de organisatie als bron voor verdere ontwikkelingen.

1.3 Opbouw domeinen

De IT-omgeving in haar geheel van processen, technieken, kennis, etc. is opgedeeld in domeinen. Alles wat we doen, zal rond deze domeinen georganiseerd worden. Denk hierbij aan eigenaar, beheerder, werkgroep, technische realisatie, etc. Het volgende diagram geeft de relatie van de tot nu toe benoemde domeinen weer.

Een domein is een specifiek gekaderd stuk functionaliteit. Voor de werkbaarheid worden **domeinen** opgedeeld in sub-domeinen. In onderstaand diagram is voor het domein Identiteiten dit als voorbeeld weergegeven met de **subdomeinen** IAM en IdP.



1.4 Uitwerking domeinen

De inhoud van een domein zal schriftelijk worden vastgelegd. Dit heeft als doel aansluiting met de Enterprise Architectuur te houden.

1. Het **PSA (Project Start Architectuur)** is het document dat helpt de juiste zaken te benoemen én te toetsen alvorens een project tot uitvoer over gaat. Het tot een finale versie van de PSA komen, kent een duidelijk *go/no go* moment waarbij het advies van de Enterprise Architect bindend is.
2. **Domein Architectuur Visual**. Er is per domein een grafische weergave waarin de technische systemen en haar verhouding weergegeven is. De Domein Architect is eigenaar van deze visual. Deze plaat is hoog-over: Details worden verder uitgewerkt in een *High Level Design (HLD)*.
3. **Domein High Level Design (HLD)**. Per (deel)domein is er een algemeen *High Level Design (HLD)*. Het HLD geeft op basis van aannames, uitgangspunten, eisen en beslissingen weer welke inrichtingskeuzes zijn gemaakt. De eigenaar van dit document is de Domein Architect.
4. **Domein Low Level Design (LLD)**. Per (technische) oplossing wordt er een *Low Level Design* opgeleverd. Dit is de *achter de komma* documentatie. Hierin wordt beschreven welke technische instellingen zijn gemaakt, zoals ze zijn gemaakt. De technische uitvoerder levert de het *Low Level Design*.

Alle documentatie wordt in de centrale bibliotheek van @voCampus opgeslagen.

2 ORGANISATIE

1. De Enterprise Architectuur is leidend. Rationele: Er is een centrale set van instrumenten en instructies die aangeven wat wenselijk is. Deze Architectuur heeft specifiek betrekking op de inrichting van organisatie, processen en informatievoorziening. Ze verwoorden wat belangrijk is bij deze inrichting en zijn relatief stabiel. Bronnen: -	Actief: ja
2. Bij wijzigingen aan de omgeving wordt een Programma Start Architectuur (PSA) opgesteld. Rationele: Om bewust bezig te zijn, werken we op een gestructureerde wijze. Er is een standaardset aan vragen om bewust te worden van de 'wat, waarom, wanneer en de hoe' van de oplossing. Bronnen: <link naar document op SP/teams>	Actief: ja
3. Er is een centraal orgaan dat de continuïteit en kwaliteit van de omgeving borgt. Rationele: De dagelijkse operatie is sterk afhankelijk van de IT-oplossing. Om kwaliteit en continuïteit te borgen is er een centraal orgaan waarin de status, wijzigingen en aanvragen van de IT-omgeving geborgd zijn. Bronnen	Actief: ja
4. Personeel is opgeleid om met de systemen te werken. Daarbij is aandacht voor kennis en competenties. Rationele: Zowel als op strategisch, zakelijk, technisch als communicatief vlak bezit het personeel dat met IT werkt de kennis en competenties om een kwalitatief hoogwaardige oplossing te ondersteunen, consumeren én door te ontwikkelen. Bronnen	Actief: ja

3 ALGEMEEN

1. Er wordt samengewerkt in één centrale omgeving. Rationele: Met het gebruik van één omgeving benut het bedrijf de middelen die de Cloud op het gebied van samenwerken biedt. Eén omgeving prefereert vanuit kosten- en efficiencyredenen. Het creëert een hoge mate van mobiliteit over de scholen heen. Bijvoorbeeld: collega's eenvoudig kunnen vinden in één adresboek. Of: eenvoudig op een veilige manier bestanden delen. Bronnen	Actief: ja
2. Voor elke technische oplossing geldt: 'SaaS boven PaaS boven IaaS'. Rationele: Bij SaaS heb je enkel focus op de inhoud (data) die in het systeem gaat. De leverancier neemt alle andere werk uit handen. Daarmee focus je op wat belangrijk is. Bij IaaS ben je zelf verantwoordelijk voor het onderhouden van de onderliggende componenten. Bronnen: https://azure.microsoft.com/nl-nl/resources/cloud-computing-dictionary/what-is-iaas	Actief: ja
3. Er zijn geen lokale IT-oplossingen. Rationele: Het doel is één centrale omgeving. Lokale oplossingen wijken daarvan af. Een centrale omgeving is efficiënter, goedkoper en stabiel. Bronnen	Actief: ja
4. De digitale omgeving ondersteunt een grote mate van zelfredzaamheid. Rationele: Wij bevorderen de zelfredzaamheid van medewerkers en leerlingen door een omgeving te faciliteren waarbij zo min mogelijk acties gevolgd worden om een doel te bereiken. Bronnen	Actief: ja

5. De digitale omgeving is gebruikersvriendelijk en intuïtief.	Actief: ja
Rationele: de IT-omgeving moet simpel zijn. En makkelijk te begrijpen. Het aantal handelingen om tot resultaat te komen, wordt tot een minimum beperkt.	
Bronnen	

6. Maatwerk wordt actief vermeden.	Actief: ja
Rationele: We kiezen standaardoplossingen in de techniek die voldoen aan onze functionele eisen. Maatwerk betekent een grote mate van afhankelijkheid en complexiteit.	
Bronnen	

7. Technische beleid wordt bedrijf breed toegepast.	Actief: ja
Rationele: Voor elk scenario wordt een standaard set technologie ingezet. Dit bevordert de herkenbaarheid richting de afnemer. En vermindert de complexiteit en beheerlast op de organisatie.	
Bronnen	

8. De aanbevelingen en 'common practices' van leveranciers worden zo veel mogelijk nageleefd.	Actief: ja
Rationele: Leveranciers ontwikkelen hun product met een gedachte. Om de kracht van de oplossing ten volste te benutten nemen we de aanbevelingen van de leverancier over.	
Bronnen	

9. Oplossingen worden getoetst tegen bedrijfscontinuïteitsvereisten.	Actief: ja
Rationele: Oplossingen worden getoetst tegen de eisen die het bedrijf stelt ten aanzien van de beschikbaarheid van de oplossing. Hierin wordt uitgewerkt wat het risico van de oplossing m.b.t. de continuïteit van het onderwijs heeft. En hoe dat risico gemitigeerd wordt.	
Bronnen	

10. Door fabrikanten en leveranciers ondersteunde diensten worden ingezet.	Actief: ja
Rationele: Fabrikanten eisen dat afnemers een ondersteund product gebruiken. Bijvoorbeeld voor het leveren van ondersteuning of om in staat te zijn naar nieuwe versie bij te werken.	
Bronnen	

11. De standaard naamconventie wordt nageleefd.	Actief: ja
Rationele: Om herkenbaarheid en beheersbaarheid te bevorderen wordt een centrale naamconventie gehanteerd.	
Bronnen: < link naar document op SP>	

12. Er vindt gedelegeerd beheer op de omgeving plaats. Hierbij wordt algemene componenten centraal beheerd. Schoolspecifieke componenten zijn ook door de schoolspecifieke IT-dienst te beheren volgens centraal beleid.	Actief: ja
Rationele: De IT-omgeving zal grofweg bestaan uit twee lagen: een centrale en een schoolspecifieke laag. In de centrale laag worden configuraties beheerd die voor alle scholen gelden. In de schoolspecifieke laag worden enkel configuraties geplaatst die gelden voor een specifieke school. Het uitgangspunt is dat een school centrale diensten afneemt. En daar zelf zijn 'kleur' in definieert. Om conflicten tussen scholen (en dus 'kleuren') te vermijden wordt enkel beheer toegestaan op specifieke configuraties.	
Bronnen	

13. Er wordt pas aan een technisch systeem gewerkt als het design goedgekeurd is door de stakeholders (Build by design).	Actief: ja
Rationele: We bouwen aan een oplossing als deze door de Enterprise Architect, Domein Architect en business owner goedgekeurd is. Hiermee voorkomen we dat er gebouwd wordt alvorens de impact geborgd is.	
Bronnen:	

14. Oplossingen (en wijzigingen) worden op een standaardwijze gedocumenteerd en centraal opgeslagen.	Actief: ja
Rationele: We leggen vast wat we doen en waarom we dat doen en hoe we dat gedaan hebben. Er is een eigenaar van de documentatie die deze overziet en beheerd.	
Bronnen:	

4 IDENTITEITEN

1. Elke gebruiker heeft een digitale identiteit.	Actief: ja
Rationele: Om de gebruiker van de digitale omgeving (medewerkers, leerlingen, gasten, digitale systemen) te kunnen identificeren is het noodzakelijk dat ze beschikken over een digitale identiteit. Op basis van onder andere de digitale identiteit wordt toegang verleend tot data.	
Bronnen	
2. Digitale identiteiten worden in één centraal identiteitsplatform (IdP) beheerd.	Actief: ja
Rationele: Het identiteitsplatform (IDP) is de kern, het kloppend hart, van de digitale omgeving. Het IDP faciliteert dat mensen en systemen op een veilige manier aan kunnen melden. Het IDP biedt het fundament om andere IT-componenten actief te kunnen faciliteren. Bijvoorbeeld veiligheidssystemen, SaaS-applicaties en werkplekken. Om één kern (waarheid van gebruikers) te hebben is één IDP de standaard.	
Bronnen	
3. Digitale identiteiten zijn herleidbaar tot het gebruikte systeem of fysieke persoon.	Actief: ja
Rationele: Vanuit veiligheidsoverweging moet vanuit een logregel herleidbaar zijn wie een digitale identiteit toebehoort. Zo kan in veiligheidssituaties contact op worden genomen met de gebruiker van die identiteit.	
Bronnen: < Link naar IBB>	

4. Gedeelde accounts worden vermeden.	Actief: ja
Rationele: Wij gebruiker primair het Microsoft Cloud Platform. Vanuit de SLA op Microsoft 365 is voorgeschreven dat digitale identiteiten niet onderling uitgewisseld mogen worden, tenzij schriftelijk bevestigd door Microsoft. Gedeelde accounts zijn in strijd met regel 4.3.	
Bronnen	

5. Het identiteitsplatform wordt gevoed door (1) één centraal HR-systeem en (2) door één LAS (specifiek voor leerlingen).	Actief: ja
Rationele: Door standaardbronnen te gebruiken worden digitale identiteiten op een gestandaardiseerde wijze gevoed en beheerd in het IdP.	
Bronnen	

6. Bij een functiewissel worden rechten ontnomen, waarna een nieuwe rechteiset wordt toegekend.	Actief: ja
Rationele: Om te borgen dat digitale identiteiten de juiste rechten in het systeem hebben worden rechten altijd ontnomen. En eventueel weer toegevoegd. Hierdoor ontstaat een logtrail over de acties van het toewijzen van rechten. En is dit proces aantoonbaar voor probleemoplossing en/of een audit.	
Bronnen	

7. Er is een centraal Identity & Access Management (IAM) pakket dat informatie uit bronnen met het Centrale IdP synchroniseert.	Actief: ja
Rationele: Een centrale IAM-oplossing stelt ons in staat om digitale identiteiten op een geautomatiseerde wijze te creëren én functionaliteit toe te kennen. Bovendien creëert de IAM-oplossing één portaal waar beheerders centraal beheer uitvoeren. En daarbij niet op verschillende plaatsen, in continu veranderende portalen, werk uitvoeren. Waarmee complexiteit (en dus de kans op onbedoelde fouten) aanzienlijk vermindert. Hiermee wordt maatwerk (vaak in de vorm van scripts) en handwerk vermeden.	
Bronnen:	

8. Beheeractiviteiten worden onder een separaat beheeraccount uitgevoerd.	Actief: ja
Rationele: Persoonsaccounts dienen vanuit risicomanagement te worden gescheiden van accounts met beheerrechten, hierdoor kan worden voorkomen dat als een specifiek persoonsaccount wordt gecompromitteerd de impact hiervan is gelimiteerd tot de persoonlijke omgeving en niet de beheeromgeving	
Bronnen	

9. Beheerrechten worden via het 'least privilege' principe toegekend.	Actief: ja
Rationele: Digitale identiteiten hebben enkel de permissies in de digitale omgeving die ze nodig hebben om hun functie succesvol uit te kunnen voeren. Hiermee wordt de kans op (onbedoelde) fouten voorkomen.	
Bronnen: https://learn.microsoft.com/en-us/azure/active-directory/roles/best-practices#1-manage-to-least-privilege	

10. Beheerrechten worden via een proces aan een beheeraccount toegekend.	Actief: ja
Rationele: Door grip te krijgen op de veiligheid van de digitale omgeving worden permissies die nodig zijn om een taak uit te voeren, bewust aangevraagd. Op basis van het risico van de aangevraagde rechten kunnen additionele eisen gesteld worden alvorens de rechten toegekend worden.	
Bronnen	
11. Bij het aanvragen van beheerrechten wordt vastgelegd: a. Wie de rechten aanvraagt. b. Welke rechten worden aangevraagd. c. Om welke reden de rechten worden aangevraagd. d. Ticketnummer dat refereert naar het ITSM. e. Wie de rechtenaanvraag heeft gekeurd. f. Bovenstaande informatie wordt voor tenminste 30 dagen bewaard. g. De tijdsduur voor de periode van het toekennen van de rechten.	Actief: ja
Rationele: Om in staat te zijn te herleiden welke acties er in de digitale omgeving zijn uitgevoerd dient deze informatie aanwezig te zijn. Bijvoorbeeld in het geval van een datalek, het opstellen van een RCA of audit is deze informatie essentieel.	
Bronnen	
12. Beheerrechten worden voor een periode actief gemaakt. En na die periode automatisch ontnomen.	Actief: ja
Rationele: De rechten die worden aangevraagd zijn een beperkte periode actief voor die digitale identiteit. Hiermee wordt een sluitend logboek gerealiseerd. En blijft het werken met extra privileges een actie die bewustwording creëert bij de beheerder.	
Bronnen	
13. Er zijn minder dan vijf beheeraccounts met het hoogste rechteenniveau (Global Admin).	Actief: ja
Rationele: Een <i>Global Admin</i> heeft alle rechten in de omgeving. En heeft daarmee onbeperkte vrijheid. Voor het alledaagse beheer volstaan de individuele beheerrollen (of een combinatie daarvan) om taken	

succesvol uit te voeren. Er is daarmee geen reden om een beheerder de hoogste beheer rechten te geven.	
Bronnen: https://learn.microsoft.com/en-us/azure/active-directory/roles/best-practices#5-limit-the-number-of-global-administrators-to-less-than-5	

14. De identiteiten voor noodtoegang zijn niet herleidbaar voor deze toepassing.	Actief: ja
Rationele: Er dienen minimaal twee accounts aanwezig te zijn voor noodtoegang. Dit zijn accounts met de hoogste beheerrechten (Global Admin) die gebruikt worden in het geval van uitval van kritieke systemen (bv uitval MFA of DNS) of andere onvoorziene situaties.	
Bronnen: https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access	

15. Van een aanmeldpoging wordt tenminste de volgende informatie voor 30 dagen bewaard: a. Gebruikte account (digitale identiteit). b. Aanmeldlocatie. c. Platform waartoe toegang aangevraagd wordt. d. IP-adres. e. Aanmeldtijdstip. f. Status van de aanmelding. g. Gebruikte applicatie. h. Gebruikte protocol. i. Geldende beveiligingsregels.	Actief: ja
Rationele: Om in het geval van een veiligheidsincident of probleemoplossing over voldoende informatie te beschikken wordt deze informatie centraal opgeslagen.	
Bronnen	

5 BEVEILIGING

1. Het gebruik van wachtwoorden wordt actief vermeden. Het gebruik van biometrische authenticatie of aanmelden met een digitale sleutel prefereert.	Actief: ja
Rationele: Wachtwoorden zijn overdraagbaar en relatief eenvoudig te kraken. Het is noodzakelijk om naast een 2e factor ook biometrische aspecten toe te voegen om de identiteit van een persoon vast te stellen.	
Bronnen: Microsoft Cloud Adoption Framework	
2. Beheeractiviteiten en 'kantoor c.q. lesgevende' activiteiten worden op gescheiden systemen uitgevoerd.	Actief: ja
Rationele: Beheerders zijn het grootste veiligheidsrisico voor de organisatie vanwege het ontvreemden van data, hun permissies, etc. Om het contactoppervlak met de buitenwereld zo veilig en klein mogelijk te maken wordt een apart systeem voor beheerdoeleinden gebruikt. Een beheerwerkplek is een veiliger werkplek, die enkel bedoeld is voor beheer. En geen connectie heeft met andere diensten (ook op het internet).	
Bronnen: https://github.com/microsoft/SecCon-Framework/blob/master/windows-security-configuration-framework.md	
3. Medewerkers hebben standaard geen beheerrechten op systemen.	Actief: ja
Rationele: Common Practice van Microsoft. Met beheerrechten kan een gebruikers in potentie alles uitvoeren en wijzigen op een werkplek. Ook onbedoeld door een kwaadwillende (lees: virus, hack, etc.). En is daarmee ook een van de meest gebruikte tactieken om een bedrijf digitaal binnen te komen.	
Bronnen: https://www.beyondtrust.com/blog/entry/5-reasons-to-keep-admin-rights-off-your-pc	

4. Het gebruik van een extra aanmeldfactor (MFA) is verplicht. SMS- en telefoonauthenticatie worden uitgesloten.	Actief: ja
Rationele: MFA is de marktstandaard voor een extra beveiligingslaag voor de digitale identiteit. De opties SMS en telefoon worden expliciet uitgesloten daar die extra gevoelig zijn voor misbruik door derden.	
Bronnen:	
5. Zakelijke data worden versleuteld opgeslagen volgens een op dat moment als algemeen veilig beschouwd versleutelingsmechanisme.	Actief: ja
Rationele: Zakelijke data worden versleuteld zodat de organisatie te allen tijde in staat is data op afstand onklaar te maken.	
Bronnen: IBB	
6. Toegang wordt op basis van de context verleend. Bij context wordt gekeken naar minimaal: a. Digitale identiteit van de medewerker b. Identiteit van het apparaat. c. Aanmeldgedrag d. Autorisatie e. Gebruikte applicatie f. Locatie van aanmelding g. Beveiligingsstatus van het gebruikte apparaat.	Actief: ja
Rationele: Door een granulair toegangsbeleid te implementeren zijn we in staat een hoge mate van beveiliging toe te passen met een zo hoog mogelijk gebruikersgemak.	
Bronnen:	

7. Zogenaamde service-accounts melden aan op basis van een digitale sleutel. Als dit niet mogelijk is: a. Geldt een (sterk¹)wachtwoord van 24 tekens dat elk half jaar rouleert én b. De aanmelding enkel via een vooraf bekende locatie (lees: IP-adres) plaats vindt.	Actief: ja
Rationele: Serviceaccounts zijn een risico voor de beveiliging van een organisatie omdat ze eenmaal ingeregeld, snel worden vergeten. Een digitale sleutel is een sterke manier van authenticatie. Als dat om technische redenen niet toepasbaar is wordt voor een sterk wachtwoord gekozen dat rouleert.	
Bronnen:	

8. Er is een proces voor noodtoegang ingeregeld. Verantwoordelijke rollen en systemen zijn daarop voorbereid.	Actief: ja
Rationele: Verwijzing naar 5.14. Als een van deze accounts wordt gebruikt is er een proces waarmee het gebruik, herstel en zichtbaarheid geborgd is.	
Bronnen: zie 5.14	

9. Het proces voor noodtoegang wordt jaarlijks getest op werkzaamheid. Bevindingen worden in het centrale IT-overleg gepresenteerd.	Actief: ja
Rationele: om bewust bezig te zijn met een 'disaster scenario' wordt deze eenmaal per jaar geoefend. Hiermee worden mensen bewust van de handelingen en procedures die gepaard gaan met een noodscenario.	
Bronnen:	

¹ Sterk is gedefinieerd als: minimaal 24 tekens, bestaande uit een combinatie van kleine letters, hoofdletters, cijfers en leestekens.

6 DATA

1. Data hebben altijd een eigenaar.	Actief: ja
Rationele: Er zijn (minimaal) twee personen verantwoordelijk voor specifieke data binnen de organisatie.	
Bronnen:	
2. Data zijn geclassificeerd volgens het informatiebeveiligingsbeleid.	Actief: ja
Rationele: De digitale data met het platform is geclassificeerd volgens het IBB. Dit stelt de IT-organisatie in staat passende maatregelen omtrent een dienst te faciliteren te nemen zoals het IBB voorschrijft.	
Bronnen:	
3. Toegang tot data in relatie tot het classificatieniveau wordt adequaat ingericht.	Actief: ja
Rationele: De IT-omgeving voorziet in het feit dat specifieke data veilig worden aangeboden en beheerd volgens de voorwaarden van het IBB.	
Bronnen:	
4. Toegang tot data wordt periodiek gecontroleerd.	Actief: ja
Rationele: Er is een proces dat voorschrijft wanneer gecontroleerd wordt of het voor een digitale identiteit nog toegestaan is toegang te hebben tot de data.	
Bronnen:	
5. Data worden opgeslagen in het daartoe bedoelde systeem.	Actief: ja
Rationele: Data worden opgeslagen in het daarvoor bedoelde platform. Hier wordt schaduw-IT actief ontmoedigt. Gebruikers worden actief betrokken in de bewustwording van professioneel werken met zakelijke data.	
Bronnen:	

6. Enkel centraal goedgekeurde applicaties krijgen toegang tot zakelijke data.	Actief: ja
Rationele: Om een veilige en productieve IT-omgeving te borgen worden tactische applicaties gevoerd. Deze applicaties zijn getest, getoetst en worden actief ondersteund door de organisatie.	
Bronnen:	

7. Data worden volgens het centraal geldende bewaartermijn opgeslagen.	Actief: ja
Rationele: Data in het digitale systeem worden volgens de algemeen geldende bewaartermijnen opgeslagen. Indien gewenst kan deze informatie door rechthebbenden opgevraagd worden ter inzage. Na de verplichte bewaartermijn worden de data verwijderd.	
Bronnen: IBB	

7 APPLICATIONS

1. Applicaties hebben een eigenaar.	Actief: ja
Rationele: Er zijn altijd (minimaal) twee medewerkers eigenaar van een applicatie.	
Bronnen:	

2. Er is een overzicht van strategisch gekozen applicaties die bedrijf breed worden ingezet.	Actief: ja
Rationele: Om tot een gecontroleerd applicatielandschap te geraken is een centrale lijst beschikbaar met strategische applicaties. Deze lijst maakt inzichtelijk welke functionaliteit met welke applicatie ingevuld wordt.	
Bronnen:	

3. Applicaties ondersteunen een modern authenticatieprotocol (SAML 2.0 of OpenID-connect).	Actief: ja
Rationele: Het centrale identiteitsplatform wordt gebruikt om aanmeldpogingen te valideren. Om in staat te zijn een applicatie technisch te koppelen aan een IDP voeren we de moderne markstandaarden op dit gebied.	
Bronnen: https://learn.microsoft.com/en-us/previous-versions/azure/dn151124(v=azure.100)	

4. Applicaties ondersteunen een modern protocol voor het opvoeren en beheren van digitale identiteiten (bv SCIM v2).	Actief: ja
Rationele: Gebruikersgegevens zoals de Voor- en achternaam zijn opgeslagen in het centrale IDP. Voor het technisch koppelen van applicaties zodat deze gebruikersgegevens naar de applicatie gesynchroniseerd worden, hanteren we de marktstandaard SCIMv2.	
Bronnen: https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/how-provisioning-works	

5. Toegang tot applicaties wordt periodiek gecontroleerd door de applicatie-eigenaar.	Actief: ja
Rationele: De applicatie-eigenaar is verantwoordelijk voor welke gebruikers toegang heeft tot haar applicatie (en de daarmee gepaarde data). Om die reden is er een proces waarin beschreven staat op welke wijze periodiek gecontroleerd wordt of toegang tot de applicatie valide is.	
Bronnen:	
6. Elke applicatie is geclassificeerd naar het interne Informatiebeveiligingsbeleid.	Actief: ja
Rationele: Om adequate beveiligingsmaatregelen én de juiste processen te faciliteren is elke technische applicatie geclassificeerd volgens het IBB.	
Bronnen:	
7. Applicaties worden centraal beheerd, geïnstalleerd en bijgewerkt.	Actief: ja
Rationele: Om beschikbaarheid, vertrouwelijkheid en integriteit van de IT-omgeving te kunnen borgen is het noodzakelijk dat er een centraal proces is voor het beschikbaar maken van applicaties. Hiermee behoudt men grip en controle op waar zakelijke data 'heen stroomt'.	
Bronnen:	
8. Applicaties die door meer dan vijf medewerkers worden gebruikt, worden gepackaged.	Actief: ja
Rationele: Als er applicaties zijn die lokaal geïnstalleerd worden op een werkstation is de grens dat vanaf vijf (5) installaties deze centraal aangeboden worden.	
Bronnen:	

8 WERKPLEK

1. Er worden eisen gesteld aan de werkplek die wordt gebruikt. a. 64 bit-processor architectuur b. Min. 8 GB geheugen c. Min. TPM 2.0 chip (of vergelijkbaar voor Apple Mac) d. Min. UEFI 2.3.1 BIOS e. Actieve ondersteuning door de fabrikant voor updates, drivers, etc.	Actief: ja
Rationele: voor beheerde werkplekken geldt er een minimumaantal eisen om het apparaat te kunnen ondersteunen. Dit heeft o.a. te maken met de beveiligingstechnieken die toegepast worden én de mate van ondersteuning vanuit onze technische partners.	
Bronnen:	
2. Alleen zakelijk aangekochte apparaten worden in beheer genomen (Device Management).	Actief: ja
Rationele: om grip en controle op het apparaatlandschap te houden nemen we alleen zakelijk aangekochte apparaten in beheer. Hiermee wordt de beheerlast voorspelbaar en daarmee kwalitatief geborgd.	
Bronnen:	
3. Op onbeheerde apparaten wordt primair via de browser gewerkt.	Actief: ja
Rationele: Op onbeheerde apparaten om invloed op het apparaat uit te oefenen. Het is daarom belangrijk geen zakelijke data op het apparaten toe te staan. Met het werken via de browser wordt de kans dat data bewust op de onbeheerde machine wordt geplaatst verkleind.	
Bronnen:	

4. Op mobiele apparaten (Telefoons & tablets) worden zakelijke data in apps actief versleuteld (applicatie management).	Actief: ja
Rationele: Om grip en controle op zakelijke data in mobiele apps te faciliteren worden er eisen gesteld aan de mobiele applicaties. Zakelijke data worden versleuteld opgeslagen en er vindt toegangscontrole tot de mobiele data plaats.	
Bronnen:	
5. Als voertaal geldt de Nederlandse taal.	Actief: ja
Rationele: Standaard wordt de Nederlandse taal gekozen, zodat er herkenbaarheid in de omgeving ontstaat.	
Bronnen:	
6. Ondersteunde besturingssystemen zijn besturingssystemen Windows, iOS en Android volgens het N-1 principe.	Actief: ja
Rationele: De digitale omgeving ondersteund van bovenstaande besturingssystemen de laatste en een-na-laatste versie.	
Bronnen:	
7. Het opnieuw uitrollen van een werkplek is een bewuste actie.	Actief: ja
Rationele:	
Bronnen:	
8. Software (d.w.z. besturingssysteem, applicaties, bios, drivers, etc.) op werkplekken wordt actief bijgewerkt volgens een vaste methodiek.	Actief: ja
Rationele: er is een gestandaardiseerd proces voor het bijwerken van software in de digitale omgeving. Dit proces borgt de bedrijfscontinuïteit.	
Bronnen:	

9. Er is een overzicht met welke type werkplekscenario's er gevoerd wordt.	Actief: ja
Rationele: Om standaardisatie binnen de technische omgeving te realiseren is er een 'menukaart' van werkplekconcepten dat gefaciliteerd wordt. Hiermee voorkomt men dat er maatwerk op maatwerk ontstaat en de daarmee gepaarde complexiteit.	
Bronnen: Link naar menukaart *hieronder weghalen)	

1. De volgende werkplektypen zijn gedefinieerd

	Persoonlijk	Kantoor (gedeeld)	BYOD	Grafisch Werkstation	Mobiel zakelijk	Examen
Beheerd	ja	ja	nee	ja	ja	ja
Werkstijl	Lokaal	Primair Web	Primair Web	Lokaal	Primair Web	Lokaal
Dataopslag	Onedrive	Onedrive	Onedrive	Onedrive + lokaal	Onedrive	Lokaal
Netwerkauthenticatie	Certificaat	Certificaat	Gebruikersnaam + Wachtwoord	Certificaat	Certificaat	
x						
y						
z						

9 INFRASTRUCTUUR

1. De infrastructuur volgt het Zero-trust principe. Rationele: Werken in de Cloud betekent dat de veiligheidsperimeter het internet is. Cloud Componenten zijn gebouwd op het Zero-trust principe: Vertrouw niemand, tenzij. Wij adopteren dit algemene architectuurprincipe om een kwalitatief hoogwaardige oplossing te faciliteren. Bronnen: https://www.microsoft.com/nl-nl/security/business/zero-trust	Actief: ja
2. Het gebruikte netwerk is open (v.w.b. proxy, routing, caching, etc.), tenzij Rationele: We volgen de aanbevelingen van onze leveranciers die stellen dat een directe ontsluiting naar het internet te prefereren valt. Bronnen:	Actief: ja
3. Er is een centrale beveiligingslaag op netwerkniveau dat diensten naar prioriteit voorrang geeft. Rationele: Bronnen:	Actief: ja
4. Het netwerk is opgedeeld naar gebruiksscenario. Rationele: Het netwerk is opgedeeld in segmenten waarin apparaten worden opgedeeld zodat er een optimale beveiliging en stabiliteit van het netwerk gegarandeerd wordt. Bronnen:	Actief: ja
5. Voor het succesvol aanmelden op een zakelijk netwerk is authenticatie verplicht. Rationele: Eerst certificaat, daarna wachtwoord. Bronnen:	Actief: ja

6. Aan toegang tot specifieke hoog-risico netwerken kan aanvullende authenticatie vereist worden als het scenario dat verplicht.	Actief: ja
Rationele:	
Bronnen:	

7. Het beheer van de componenten van infrastructuur kan enkel uitgevoerd worden vanaf het centrale beheerplatform.	Actief: ja
Rationele: Het beheer aan kritieke infrastructuur kan enkel vanaf geselecteerde machines in specifieke netwerksegmenten uitgevoerd worden. Hiermee verkleint men het veiligheidsrisico.	
Bronnen:	

8. VPN-oplossingen worden actief vermeden.	Actief: ja
Rationele: VPN is een techniek om via een 'tunnel' een werkplek (o.i.d.) aan een intern bedrijfsnetwerk te koppelen. Bij een VPN wordt wél geauthentiseerd, maar is onzeker welke data er door de tunnel gaat. Daarbij is het eenvoudig voor een kwaadwillende om de netwerken aan beide kanten van tunnel met elkaar te verbinden. Daarmee zijn bedrijfsnetwerken vatbaar voor malware, DDoS en Spoofing.	
Bronnen: https://www.securelink.com/blog/vpn-problems/	

9. Netwerkontsluiting richting het internet is hoogbeschikbaar uitgevoerd.	Actief: ja
Rationele: Met het consumeren van clouddiensten is een hoogbeschikbare én van voldoende bandbreedte voorziene internetverbinding noodzakelijk.	
Bronnen:	

10. De veiligheidssystemen op de endpoints integreren met de veiligheidssystemen op netwerkniveau.	Actief: ja
Rationele: De veiligheidsstatus van de eindpunten (servers, werkplekken, etc.) is geïntegreerd in de veiligheidssystemen op netwerkniveau. Hiermee krijgen we grip en controle op het toegang verlenen voor medewerkers tot netwerken én data op basis van de veiligheidsstatus van werkplekken.	

Bronnen:	
----------	--

11. Het beheer van de componenten van infrastructuur kan enkel uitgevoerd worden vanaf het centrale beheerplatform.	Actief: ja
Rationele: Het beheer aan kritieke infrastructuur kan enkel vanaf geselecteerde machines in specifieke netwerksegmenten uitgevoerd worden. Hiermee verkleint men het veiligheidsrisico.	
Bronnen:	