Architectuurprincipes

Voor de Informatievoorziening & ICT

ROC van Amsterdam-Flevoland

Versie 0.99 | 23-06-2023

Versiebeheer

Versie	Datum	Wijzigingen	Auteur
0.1	28-02-2022	Eerste opzet en uitwerkingen	G.D.Griffioen, informatie architect
0.2	13-06-2022	Verwerking 1e review door informatiemanager en ISO	G.D.Griffioen
0.3	23-06-2022	Verwerking 1e review werkgroep architectuur	G.D.Griffioen
0.4	06-09-2022	Verwerking feedback werkgroep architectuur en algehele redactie en aanvullingen	G.D.Griffioen
0.5	20-09-2022	Aanvullingen op en aanpassing van de Inleiding	G.D.Griffioen
0.6	12-12-2022	Diverse redactionele aanpassingen	G.D.Griffioen
0.7	16-01-2023	Verwerking feedback directeur OI&I, aanpassing afbeeldingen	G.D.Griffioen
071	30-01-2023	Verwerking feedback manager Informatievoorziening OI&I, aanvullende redactionele aanpassingen	G.D.Griffioen
0.9	24-03-2023	Herziening op onderdelen en deels herindeling, verwerking laatste feedback	G.D.Griffioen
0.91	25-04-2023	Kleine tekstuele aanpassingen van principe 4.4 op basis van feedback afdeling Inkoop	G.D.Griffioen
0.92	17-05-2023	Tekstuele aanscherping van implicaties principe 1.2; Toevoeging afgeleid principe “We voldoen aan onderwijswet- en regelgeving”, andere redactionele en kleine inhoudelijke aanpassingen	G.D.Griffioen
0.93	13-06-2023	Redactionele en inhoudelijke controle en correcties	G.D.Griffioen
0.99	23-06-2023	Geen inhoudelijke wijzigingen, versienummer ten behoeve van besluitvorming MT OI&I	G.D.Griffioen

Inhoudsopgave

1 Inleiding

Dit document bevat de architectuurprincipes van het ROCvA/ROCvF/VOvA (hierna het ROCvA-F). De architectuurprincipes beschrijven de kaders en richtlijnen voor de gehele organisatie waarmee richting gegeven wordt aan oplossingen[1] op het gebied van de informatievoorziening en ICT en fungeren daarmee als toetsingskader. De architectuurprincipes zijn tevens het vertrekpunt om onder architectuur te kunnen werken. Met de term architectuur wordt overigens zowel een proces als een product bedoeld.

Waarom architectuur

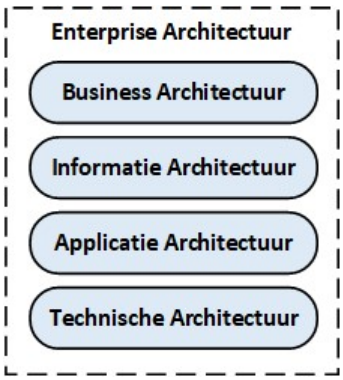
Door gebruik te maken van architectuur tracht men een compleet beeld te krijgen én te houden van de samenhang van de opbouw en besturing van een organisatie en diens processen, informatievoorziening, applicaties en infrastructuur. Door dat inzicht en overzicht kan men vervolgens o.a. beter de impact van veranderingen analyseren en zorgen dat alles zo gecontroleerd mogelijk op elkaar aansluit.

> "Architectuur is een instrument dat instellingen helpt bij het beheersen van risico's in de informatievoorziening en het creëren van de noodzakelijke samenhang en kwaliteit. Het beschrijft de inrichting van organisaties in kaders en modellen. Dat geeft inzichten die gebruikt kunnen worden om de organisatie te verbeteren."[2]

Bij het hoofdprincipe 1, Werken onder architectuur, staat een nadere beschrijving van de rationale van het werken onder architectuur. Kort gezegd helpt architectuur om meer grip te krijgen en te houden én om de organisatie verder te helpen.

Reikwijdte

De architectuurprincipes zijn van toepassing op alle architectuurlagen van de organisatie, namelijk: de business laag (processen, besturing), de informatie laag (data & informatie[3]), de applicatie laag (applicaties) en de technische laag (techniek en infrastructuur). Gezamenlijk vormen ze de Enterprise architectuur van een organisatie.



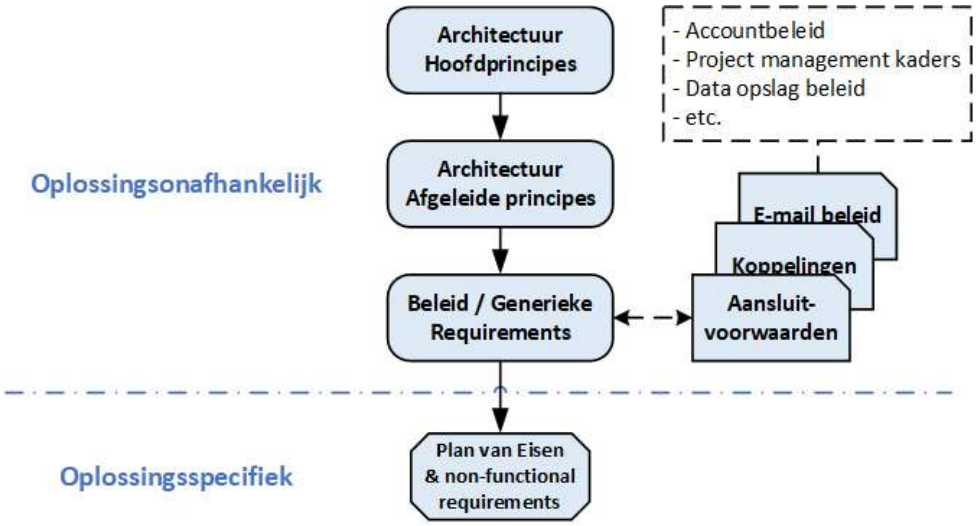
[1] "Oplossingen" moet worden geïnterpreteerd in de brede zin van het woord. Zo kan een oplossing niet alleen een softwaretoepassing zijn, maar ook een procesmatige oplossing of een dienst of een service.

[2] Beschrijving van de toegevoegde waarde van architectuur voor een organisatie, bron: https://hora.surf.nl/index.php/Over_HORA, sept 2022.

[3] Met de term data wordt vastgelegde gegevens bedoeld. Informatie bestaat uit de interpretatie van die data binnen een bepaalde context. Met elkaar samenhangende gegevens kunnen geordend worden in logische dataobjecten en -verzamelingen.

Opbouw en hiërarchie

De principes zijn opgebouwd volgens een getrapte structuur van een aantal hoofdprincipes, met per hoofdprincipe meerdere afgeleide principes. De hoofdprincipes zijn als basis uitgangspunten en beginselen te beschouwen. In de afgeleide principes wordt al meer richting gegeven aan de concrete invulling van oplossingen. Op basis van de hoofd- en afgeleide principes is het mogelijk om meer generiek en op een specifiek deelgebied toegespitst beleid en requirements op te stellen voor oplossingen op het gebied van de informatievoorziening en ICT, zoals bijv. E-mail beleid of Aansluitvoorwaarden. Deze generieke requirements leveren vervolgens weer input voor bijv. het Plan van eisen en non-functional requirements (NFR), op basis waarvan een specifieke oplossing geselecteerd kan worden. Schematisch ziet de getrapte structuur er als volgt uit:



Toepassing

De architectuurprincipes zullen toegepast worden voor alle nieuwe initiatieven binnen het ROCvA-F ten behoeve van oplossingen op het gebied van informatievoorziening en ICT. Voor bestaande oplossingen zullen de principes toegepast worden bij vernieuwings- of vervangingsinitiatieven.

Beheer

Het beheer, de herziening, de doorontwikkeling en het toezicht op naleving van de architectuurprincipes ligt primair bij de architect(en) van het ROCvA-F. Daar waar nodig, in samenwerking met relevante andere disciplines, zoals o.a. informatiemanagement, security & informatiebeveiliging, juridische zaken, e.d. De principes zullen jaarlijks geëvalueerd worden en daar waar nodig aangepast of aangevuld worden.

Verantwoording

De architectuurprincipes zijn tot stand gekomen op basis van de reeds bestaande principes van de Dienst ICT uit 2020, voorbeelden van principes uit referentie architecturen en uit architectuur frameworks (zoals TOGAF) en op basis van *best practices* en inzichten vanuit online architectuur resources. Bij het opstellen is rekening gehouden met de strategische doelstellingen en uitgangspunten van het ROCvA-F en de Dienst OI&I. Daarnaast zijn de principes binnen en buiten de dienst OI&I gedeeld en gereviewd.

2 Overzicht van de hoofdprincipes

Als hoofdprincipes worden de volgende basis uitgangspunten en beginselen gehanteerd:

1. Werken onder architectuur
2. Security & Privacy by design
3. Informatie is een strategisch bedrijfsmiddel
4. Duurzaam en verantwoord
5. Betrouwbare, toegankelijke en flexibele oplossingen

3 Overzicht van de hoofdprincipes met afgeleide principes

1. Werken onder architectuur
   1.1. We gebruiken beschikbare (sector)standaarden
   1.2. Pas toe of leg uit (Comply or explain)
   1.3. Excepties op de architectuur worden centraal geregistreerd
2. Security & Privacy by design
   2.1. Data en informatie worden geclassificeerd
   2.2. Secure authenticatie
   2.3. Beperkte autorisatie
   2.4. Vastlegging van voldoende loginformatie
   2.5. Security by default
   2.6. AVG als basis
3. Informatie is een strategisch bedrijfsmiddel
   3.1. Betrouwbare en bruikbare data en informatie
   3.2. Data heeft één bronsysteem
   3.3. We hanteren FAIR databeleid
   3.4. Digitale transformatie drijft onderwijs en innovatie
   3.5. We nemen bewaartermijnen in acht
4. Duurzaam en verantwoord
   4.1. De toegevoegde waarde wordt benoemd
   4.2. We letten op de TCO (Total Cost of Ownership)
   4.3. Oplossingen worden gedocumenteerd
   4.4. We voldoen aan onderwijswet- en regelgeving
   4.5. We volgen het centrale Inkoopbeleid
   4.6. Wij zijn actief onderdeel van de onderwijssector
   4.7. We adopteren de Sustainable Development Goals
5. Betrouwbare, toegankelijke en flexibele oplossingen
   5.1. Elk moment, elke plaats, elk apparaat
   5.2. Een optimale gebruikerservaring
   5.3. We doen actief aan Life Cycle Management (LCM)

4 Uitwerking van alle principes

Hoofdprincipe 1	**Werken onder architectuur**
Toelichting	Het ROCvA-F werkt met behulp van architectuur op gestructureerde wijze aan oplossingen op het gebied van de informatievoorziening en ICT.
Rationale	Werken onder architectuur zorgt voor inzicht en overzicht van de oplossingen op het gebied van de informatievoorziening en ICT en bevordert de beheersbaarheid en controleerbaarheid ervan. Architectuur waarborgt o.a. door middel van kaders, richtlijnen, modellen, standaarden e.d. dat oplossingen in samenhang gerealiseerd worden en dat deze passen binnen de huidige en beoogde inrichting van de informatievoorziening en het huidige en beoogde ICT landschap. Architectuur bevordert daarmee een consistent kwaliteitsniveau van de oplossingen zelf, alsmede hun onderlinge samenhang en ondersteunt de professionalisering van het ROCvA-F.
Implicaties	• Om succesvol onder architectuur te kunnen werken, dient de toegevoegde waarde ervan onderkend te worden door de organisatie en dient draagvlak gecreëerd te worden voor de toepassing van architectuur. • Architectuur is van toepassing voor de gehele organisatie; voor de business laag (processen, besturing), de informatie laag (data & informatie), de applicatie laag (applicaties) en de technische laag (techniek en infrastructuur). • Oplossingen op het gebied van de informatievoorziening en ICT moeten getoetst worden aan o.a. relevante architectuurprincipes, kaders, richtlijnen en referentiearchitecturen. • De architectuurprincipes worden jaarlijks getoetst op actualiteit en waar nodig vernieuwd, aangevuld of vervangen.

Principe 1.1	**We gebruiken beschikbare (sector)standaarden**
Toelichting	Waar mogelijk gebruiken we beschikbare standaarden, zoals methodieken, frameworks, modellen en referentie architecturen, voor algemeen gebruik of specifiek voor de onderwijssector.
Rationale	Standaarden, zoals methodieken, frameworks, modellen en referentie architecturen, zijn over het algemeen tot stand gekomen op basis van brede kennis en expertise en ervaringen uit de praktijk. Door gebruik te maken van deze gestolde kennis hoeft men niet meer zelf opnieuw het wiel uit te vinden en kan een kwaliteitsslag gemaakt worden voor de informatievoorziening en het ICT landschap van een organisatie.
Implicaties	Standaarden die we (onder andere) gebruiken zijn: • De MORA als referentiearchitectuur voor het MBO en de FORA als referentiearchitectuur voor het VO. • Relevante afspraken van Edustandaard. • Het burcht-stad-landschap metaforenmodel en de bijbehorende systematiek van SURF voor het applicatie- en systeemlandschap.

	• Het IBP/NBA normenkader voor het informatiebeveiligingsbeleid. • De Archimate methodiek voor het modelleren van architectuur. • De BPMN methodiek voor het modelleren van (bedrijfs)processen. • De UML methodiek voor modellering t.b.v. software ontwikkeling. • De Crow's Feet notatiewijze voor ERD data modellen. • Modellen voor beheer, zoals het 9-vlaksmodel van Maes, ITIL, ASL en BiSL. • Projectmanagement methodieken. • De NCSC Cybersecurity maatregelen voor security.

Principe 1.2	**Pas toe of leg uit (Comply or explain)**
Toelichting	Architectuur kaders, richtlijnen, modellen, standaarden e.d. dienen toegepast te worden bij alle oplossingen op het gebied van informatievoorziening en ICT. Wanneer dit (deels) niet mogelijk is, moet dat expliciet gemotiveerd worden.
Rationale	Om het overzicht en de controle en beheersbaarheid van oplossingen op het gebied van informatievoorziening en ICT te behouden, is het noodzakelijk om te weten waar de architectuur (nog) niet voldoet aan de gewenste situatie. Om die reden dienen afwijkingen expliciet inzichtelijk gemaakt te worden.
Implicaties	• Bij mogelijke afwijkingen van de architectuur (excepties), dient advies gevraagd te worden over mogelijke impact en eventuele risico's aan de architect(en) en evt. de Information Security Officer en de Privacy Officer. • Excepties kunnen alleen worden toegestaan na advisering en met een gemotiveerde onderbouwing, waarbij eventuele bijbehorende risico's expliciet door de business geaccepteerd dienen te worden. • Bepaalde voorwaarden kunnen van toepassing zijn voordat een exceptie kan worden toegestaan. • Uitgangspunt is dat excepties van tijdelijke aard zijn en zo snel mogelijk alsnog opgelost moeten worden.

Principe 1.3	**Excepties op de architectuur worden centraal geregistreerd**
Toelichting	Uitzonderingen op de architectuur dienen centraal geregistreerd te zijn om deze te kunnen monitoren en zicht te houden op bewust genomen en beargumenteerde risico's.
Rationale	Om te voorkomen dat excepties op de architectuur uit beeld verdwijnen en te faciliteren dat ze periodiek gecontroleerd kunnen worden op mogelijke oplosbaarheid, validiteit en aanvaardbaarheid (risico management), is het noodzakelijk om centraal inzicht te hebben in de excepties.
Implicaties	• Uitzonderingen op de architectuur dienen in een centraal exceptieregister te worden vastgelegd en worden beheerd door de architect(en). • Periodiek dient gecontroleerd te worden of excepties in de loop van de tijd alsnog opgelost kunnen worden.

	• Periodiek dient gecontroleerd te worden of excepties nog acceptabel zijn van uit het oogpunt van risicomanagement.

Hoofdprincipe 2	**Security & Privacy by design**
Toelichting	Security & Privacy zijn opgenomen in het ontwerp van een gekozen oplossing.
Rationale	Om er zeker van te zijn dat een oplossing van meet af aan zo veilig mogelijk is en de privacy respecteert, dienen security, informatiebeveiliging en privacywaarborgen integraal meegenomen te worden bij het ontwerp, de keuze en de inrichting van oplossingen op het gebied van de informatievoorziening en ICT.
Implicaties	• Voor elke nieuwe oplossing op het gebied van de informatievoorziening en ICT, dienen de BIV-dataclassificatie en de daarbij behorende security en privacy maatregelen in het projectplan of in vergelijkbare documentatie beschreven te worden. • Oplossingen op het gebied van de informatievoorziening en ICT moeten getoetst worden aan relevante principes, kaders en richtlijnen op het gebied van security door de Information Security Officer (ISO) en architectuur. • Oplossingen op het gebied van de informatievoorziening en ICT, waarbij met persoonsgegevens wordt gewerkt, moeten getoetst worden aan relevante wet- en regelgeving, zoals de AVG, door de Privacy Officer (PO) en/of de Functionaris Gegevensbescherming (FG). • De PO en de FG dienen in een zo'n vroeg mogelijk stadium geïnformeerd en betrokken te worden bij initiatieven waarbij persoonsgegevens verwerkt gaan worden. Tevens moet vastgelegd worden wat met een eventueel door de FG en/of PO gegeven advies t.a.v. het initiatief gedaan is. • Voor reeds bestaande oplossingen op het gebied van de informatievoorziening en ICT dient een analyse uitgevoerd te worden van mogelijke *gaps* tussen de bestaande situatie en de vernieuwde principes op het gebied van security en privacy. • Om te controleren op de naleving van wet- en regelgeving, vereisten en maatregelen op security en privacy gebied, dienen periodieke interne en externe audits uitgevoerd te worden. • Naast technische en organisatorische maatregelen op het gebied van security, moet ook de menskant geadresseerd worden. Dat betekent dat alle medewerkers van het ROCvA-F bewust gemaakt moeten worden van de mogelijke gevaren op het gebied van security, informatiebeveiliging en privacy en gemotiveerd moeten worden om hun bijdrage te leveren door veilig te werken.

Principe 2.1	**Data en informatie zijn geclassificeerd**
Toelichting	Data en informatie zijn beoordeeld en geclassificeerd volgens een gestructureerde methode.

Rationale	Om het juiste vereiste beveiligingsniveau voor data en informatie (i.c. data objecten en dataverzamelingen) te kunnen bepalen dient op gestructureerde wijze een beoordeling en classificatie van de te beveiligen data en informatie uitgevoerd te worden.
Implicaties	• Voor elke oplossing op het gebied van de informatievoorziening en ICT wordt een BIV-dataclassificatie opgesteld voor de data op de aspecten Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). • Het is de verantwoordelijkheid van de data eigenaar dat een BIV-dataclassificatie wordt opgesteld. • Op basis van de BIV-dataclassificatie en het informatiebeveiligingsbeleid worden (technische) vereisten en te nemen maatregelen gedefinieerd voor de beveiliging van informatie (data objecten en dataverzamelingen), applicatieve toepassingen (applicaties, interfaces, services, etc.) en infrastructurele toepassingen (netwerk(en), cloud tenants, servers, etc.). Voorbeelden van vereisten en maatregelen zijn bijvoorbeeld toegangsbeveiliging, het *hardenen* van servers, compartimenteren van het netwerk in segmenten, restricties op de rechten die API's krijgen, back-up, patching, encryptie, etc. • Maatregelen worden mede gebaseerd op een risicoanalyse vanuit het perspectief van het bedrijfsproces dat met de data wordt ondersteund. • De BIV-dataclassificaties dienen centraal vastgelegd te worden en raadpleegbaar te zijn voor relevante stakeholders.

Principe 2.2	**Secure authenticatie**
Toelichting	De authenticatie van gebruikers en systeemaccounts gebeurt op veilige wijze.
Rationale	Om het risico op misbruik van systemen en data tegen te gaan, dient de (digitale) identiteit van gebruikers of systemen, op veilige wijze geverifieerd te worden.
Implicaties	• Iedere gebruiker van systemen van het ROCvA-F krijgt een digitale identiteit toegekend met een daarbij behorend op naam gestelde gebruikersaccount. • Indien een gebruiker ook beheerstaken moet uitvoeren, wordt daarvoor een apart op naam gesteld beheerdersaccount toegekend. • Alle digitale identiteiten en accounts worden beheerd middels een centrale Identity & Access Management (IAM) voorziening. • Waar nodig is multi-factor authenticatie vereist bij het inloggen voor gebruikers. • Het gebruik van elke op naam gestelde gebruikersaccount valt te allen tijde onder de verantwoordelijkheid van de gebruiker. • De gebruiker is ervoor verantwoordelijk dat niemand het wachtwoord van zijn/haar op naam gestelde account kent. • Het door een gebruiker gekozen wachtwoord dient te voldoen aan het interne wachtwoordbeleid. • De gebruiker mag alleen zijn/haar eigen op naam gestelde account(s) gebruiken.

	• Niet op naam gestelde accounts, zoals functionele accounts of service accounts t.b.v. applicatieve en infrastructurele toepassingen, zijn onderworpen aan een streng beleid. Deze accounts worden alleen toegestaan wanneer ze strikt noodzakelijk zijn en ze dienen periodiek getoetst te worden. • Zogenaamde groepsaccounts (bijv. niet op naam gestelde accounts of op afdelingsnaam gestelde accounts), die door meerdere medewerkers gebruikt worden, zijn **niet** toegestaan. De reden daarvoor is dat bij het gebruik van een groepsaccount de toegang tot bepaalde data en eventueel gemaakte mutaties in die data niet herleidbaar is (audit trail) naar een natuurlijk persoon.

Principe 2.3	**Beperkte autorisatie**
Toelichting	Toestemming (autorisatie) voor het gebruik van systemen en data is beperkt tot datgene wat strikt noodzakelijk is.
Rationale	Geef medewerkers alleen toegang tot de data en systemen die nodig zijn voor het uitvoeren van hun taak. Dit geldt zowel voor accounts als voor fysieke toegang. Dit beperkt de handelingen die een aanvaller kan uitvoeren indien deze zich toegang verschaft. Ook beperkt het de gevolgen van eventuele fouten van gebruikers.

Implicaties	• Autorisatie van gebruikers én beheerders, alsmede functionele accounts of service accounts, vind plaats op basis van security principes zoals:
	  ○ *least-privilege*
	  ○ *need-to-know*
	  ○ *just-enough*
	• We streven ernaar om de Autorisatie van gebruikers en beheerders rol-gebaseerd in te richten, ook wel bekend als *role-based access* (RBAC).

Principe 2.4	**Vastlegging van voldoende loginformatie**
Toelichting	Van alle toegang tot en het gebruik van systemen en de daar in vastgelegde data, door een gebruiker of door een ander systeem, wordt een doelmatig logbestand opgeslagen en bijgehouden.
Rationale	Om zicht te houden op wie toegang heeft gehad tot belangrijke systemen en vertrouwelijke data en wat daarmee gedaan is, is het noodzakelijk om dit middels logbestanden vast te leggen en daarmee een audit trail te creëren. Daarnaast spelen logbestanden een sleutelrol in het detecteren van aanvallen en het afhandelen van incidenten. Ook daarvoor is het van belang dat applicaties en systemen voldoende loginformatie genereren. De logbestanden dienen wel doelmatig te zijn, omdat logbestanden opslagruimte in beslag nemen en mogelijk privacygevoelige informatie bevatten.
Implicaties	• Afhankelijk van de BIV-score dient het gebruik van bepaalde systemen en bepaalde data vastgelegd te worden in een audit trail (wie, wat, wanneer).

	• Vastgesteld moet worden welke soort logging noodzakelijk en doelmatig is in welke situatie, zoals bijv. systeemlogging, netwerklogging, applicatielogging, cloudlogging, etc. • Logbestanden dienen in een bruikbaar bestandsformaat opgeslagen te worden. • De opgenomen tijdsinformatie dient nauwkeurig te zijn en in de juiste tijdzone ingesteld zijn. • De toegang tot logbestanden dient beperkt te zijn tot een specifieke groep medewerkers en in een apart netwerksegment opgeslagen te worden. • De ISO stelt in overleg met o.a. Juridische Zaken beleid op over welke rol en functie op welk moment geautoriseerd is om welke soort logbestand in te zien. • Waar nodig dient *alerting* ingericht te worden. Denk hierbij bijvoorbeeld aan notificaties van verdachte inlogpogingen op basis van een analyse van logbestanden.

Principe 2.5	**Security by default**
Toelichting	De inrichting en configuratie van applicatieve toepassingen (applicaties, interfaces, services) en infrastructurele toepassingen (netwerk, servers, koppelvlakken) start met de meest veilige instellingen die mogelijk zijn.
Rationale	De meest veilige inrichting en configuratie is om géén enkel recht op toegang te verlenen. Wanneer dat als vertrekpunt wordt gekozen en vervolgens welbewust toegangsrechten worden verleend en functionaliteiten beschikbaar worden gesteld, levert dat in de basis een zo veilig mogelijke inrichting en configuratie op.

Implicaties	• De inrichting en de configuratie van applicatieve en van infrastructurele toepassingen vindt plaats op basis van security principes zoals:
	  ○ *default-deny*
	  ○ *zero trust*
	  ○ *secure connections*

Principe 2.6	**De AVG als basis**
Toelichting	De vereisten vanuit de Algemene Verordening Gegevensbescherming (AVG) worden integraal meegenomen bij het ontwerp, de keuze en de inrichting van oplossingen op het gebied van de informatievoorziening en ICT.
Rationale	Op basis van de AVG dient aan een aantal specifieke vereisten voldaan te worden wanneer met persoonsgegevens gewerkt wordt. Oplossingen op het gebied van de informatievoorziening en ICT dienen in dat geval expliciet getoetst te worden en te beantwoorden aan die vereisten.

Implicaties	• Bij het gebruik van persoonsgegevens moet getoetst worden op:
	  ○ Rechtmatigheid,
	  ○ Doelbinding,
	  ○ Vertrouwelijkheid,

	○ Dataminimalisatie, ○ Opslagbeperking. De uitkomst en de onderbouwing van deze toets dient beschreven te worden. • Bij het gebruik van persoonsgegevens moet geborgd worden: ○ Het recht op inzage, ○ Het recht op correctie, ○ Het recht op verwijdering en 'het recht om vergeten te worden', ○ Het recht op beperking, ○ Het recht op overdraagbaarheid. • Bij het gebruik van persoonsgegevens dient een DPIA (Data Protection Impact Assessment) opgesteld te worden na consultatie van de Privacy Officer (PO). • Indien persoonsgegevens door een derde partij verwerkt zullen worden, dient een Verwerkersovereenkomst opgesteld en ondertekend te worden. • Datalekken dienen voorkomen te worden. Maatregelen ter voorkoming daarvan moeten integraal onderdeel zijn van de implementatie van een ICT oplossing. • Privacy by default; anonimisering of pseudonimisering van persoonsgegevens waar mogelijk en strikt beperkte toegang (autorisatie) tot persoonsgegevens.

Hoofdprincipe 3	**Informatie is een strategisch bedrijfsmiddel**
Toelichting	Informatie en de er aan ten grondslag liggende data en gegevens zijn van strategisch belang en zijn als een essentieel bedrijfsmiddel (resource) te beschouwen.
Rationale	Informatie en de onderliggende gegevens (data) bepalen in sterke mate de productiviteit van organisaties; zonder data en informatie kunnen processen niet worden uitgevoerd. Voor onderwijsinstellingen geldt dit zo mogelijk nog sterker, omdat het primaire proces van het onderwijs bestaat uit de overdracht van informatie en kennis aan studenten, bedrijven en de maatschappij. Data ligt in veel gevallen ten grondslag aan de informatie en kennis die het onderwijs overdraagt of is noodzakelijk voor een effectieve en efficiënte ondersteuning van het onderwijsproces zelf.
Implicaties	• Data en informatie dienen in overeenstemming met hun waarde en strategische belang behandeld en beheerd te worden. Dat betekent o.a. dat alle gebruikers van data en informatie binnen het ROCvA-F meer bewust gemaakt moeten worden van de waarde en het belang van de data en informatie. • Data en informatie dienen in principe beschikbaar te zijn voor (her)gebruik binnen de gehele organisatie. Toegang en gebruik van de data en informatie wordt geregeld middels duidelijke afspraken en goed beheer. • Bij gecentraliseerde dataverzamelingen (op één fysieke locatie) dient er een verantwoorde logische en fysieke segmentering

	aangebracht, dan wel aanwezig te zijn, om verschillende autorisatieniveau 's te kunnen waarborgen. • Data van het ROCvA-F blijft altijd eigendom van het ROCvA-F, ongeacht de locatie waar de data wordt opgeslagen en de vorm en het medium waarin het wordt opgeslagen. Dit dient contractueel vastgelegd te worden met leveranciers van producten en diensten waar data van het ROCvA-F wordt ondergebracht.

Principe 3.1	**Betrouwbare en bruikbare data en informatie**
Toelichting	Data en informatie moeten van een goede kwaliteit zijn om betrouwbaar en bruikbaar te zijn.
Rationale	Data kwaliteit is een bepalende factor voor de kwaliteit van de dienstverlening naar interne en externe stakeholders zoals studenten, medewerkers, stagebedrijven en overheidsinstanties. Daarnaast hebben het management en de bestuurders eveneens kwalitatief hoogwaardige stuurinformatie nodig om de organisatie te kunnen besturen. Kwaliteit van data kent vele dimensies zoals accuraat, compleet, actueel, beschikbaar en integer. De kwaliteit van data moet vooral optimaal aansluiten bij het doel waarvoor de data gebruikt zal worden.

Implicaties	• Om actief te kunnen sturen op betrouwbare en bruikbare data richten we Data Governance in. Dit betekent o.a.:
	  ○ Elke data verzameling heeft een eigenaar.
	  ○ Het bewaken van de data kwaliteit en het coördineren, dan wel nemen van acties, om de data kwaliteit te verbeteren waar dat nodig is, is een taak die expliciet belegd moet worden. Die taak wordt in principe belegd bij de rol van data steward.
	  ○ Er wordt gebruikersbeheer van data ingericht.
	  ○ Voor ieder relevant gegeven is er een eenduidige en gemeenschappelijke datadefinitie.
	  ○ Prestatie indicatoren worden vastgesteld die aansluiten bij de vraag naar stuurinformatie.

Principe 3.2	**Data heeft één bronsysteem**
Toelichting	Data van een logische dataverzameling heeft één bronsysteem.
Rationale	Wanneer je voor elke logische dataverzameling één bronsysteem gebruikt, is voor iedereen duidelijk waar de juiste en meest actuele data is opgeslagen. Tevens voorkom je problemen met dubbele invoer van gegevens of met versiebeheer.
Implicaties	• Data wordt gecreëerd in één systeem, het bronsysteem, ook wel aangeduid met Single Source of Truth (SSoT). • Voor elke logische gegevensverzameling wordt een dataregister/dossier opgesteld, waarin de oorsprong (het bronsysteem), de inhoud en het toepassingsgebied van de gegevensverzameling beschreven staan en welke toepassingen gebruik maken van die gegevensverzameling.

	• Data uit een bronsysteem die voor andere toepassingen nodig is, wordt in principe telkens opnieuw vanuit het bronsysteem opgehaald. Dat betekent dat het werken met een kopie van een kopie van de brondata in principe niet toegestaan is.

Principe 3.3	**We hanteren FAIR databeleid**
Toelichting	We streven ernaar dat data vindbaar, toegankelijk, uitwisselbaar en herbruikbaar is.
Rationale	Data is vanzelfsprekend alleen van waarde als ze gevonden kan worden en toegankelijk is en wanneer die data uitgewisseld kan worden en ook herbruikbaar is. Vanuit gebruikersperspectief is het daarom goed om dit expliciet te maken en gebruik te maken van de FAIR standaard die hiervoor is opgesteld. Dit draagt tevens bij aan een meer data-gedreven organisatie.

Implicaties	• **Findable (vindbaar)**; data moet gevonden kunnen worden.
	  ○ Metadatering van data
	  ○ Indexering en doorzoekbaarheid
	  ○ Data dictionary/register
	  ○ Data modellen
	• **Accessible (toegankelijk)**; data moet toegankelijk zijn.
	  ○ Data is een gedeelde resource (stakeholders moeten kunnen beschikken over organisatie brede data, wat betekent dat data uit silo's moet worden gehaald indien van toepassing).
	  ○ Oplossingen dienen te voldoen aan de Web Content Accessibility Guidelines (WCAG).
	• **Interoperable (uitwisselbaar)**; data dient gedeeld en uitgewisseld te kunnen worden .
	  ○ We sturen op geautomatiseerde interfaces en het gebruik van API's.
	  ○ Data dient praktisch gezien eenvoudig te exporteren zijn ten behoeve van o.a. datamigratie en data analyse toepassingen.
	  ○ Data dient in een gangbaar bestandstype opgeslagen dan wel geëxporteerd te kunnen worden.
	• **Reusable (herbruikbaar)**; data dient herbruikbaar te zijn, op zowel korte als langere termijn en binnen verschillende oplossingen en toepassingen.

Principe 3.4	**Digitale transformatie drijft onderwijs en innovatie**
Toelichting	Digitale transformatie biedt nieuwe (innovatieve) mogelijkheden ter verbetering van het onderwijs zelf en de ondersteunende onderwijslogistiek en bedrijfsvoering.
Rationale	Om een digitale transformatie van de organisatie mogelijk te maken dient o.a. digitalisering van op papier gestelde gegevens en informatie plaats te vinden. Daarmee ontsluit men deze informatie voor mogelijke bredere inzetbaarheid binnen de organisatie en kunnen data en informatie potentieel met elkaar gecombineerd worden voor nieuwe toepassingen en

	inzichten. Daarnaast dienen ook processen verdergaand geautomatiseerd en gedigitaliseerd te worden. Daardoor verbetert het inzicht in en de beheersbaarheid van deze processen en is het mogelijk om deze processen als gevolg daarvan efficiënter en effectiever in te richten. Mede op basis hiervan is een digitale transformatie mogelijk, waarmee nieuwe (innovatieve) mogelijkheden ontstaan om het onderwijs en de ondersteuning ervan te verbeteren.
Implicaties	• Waar mogelijk en waar het zinvol is, dienen op papier gestelde data en informatie gedigitaliseerd en ontsloten te worden. • Waar mogelijk en waar het zinvol is, dienen processen geautomatiseerd en gedigitaliseerd te worden. • Medewerkers van het ROCvA-F dienen door middel van bijvoorbeeld trainingen ondersteund te worden om succesvol mee te gaan in het proces van verdere digitalisering en de digitale transformatie van het ROCvA-F.

Principe 3.5	**We nemen bewaartermijnen in acht**
Toelichting	We voldoen aan de wettelijke bewaartermijnen
Rationale	Vanuit de Archiefwet volgen vereisten ten aanzien van de bewaartermijn van bepaalde data. Oplossingen op het gebied van de informatievoorziening en ICT dienen expliciet getoetst te worden en te beantwoorden aan die vereisten.
Implicaties	• De opslagduur van data wordt op grond van wettelijke bewaartermijnen bepaald (zie ook bij 2.6 AVG; opslagbeperking). • De bewaartermijnen voor persoonsgegevens worden vastgelegd in het register van verwerkingsactiviteiten (dataregister, volgens Kennisnet (https://aanpakibp.kennisnet.nl/bewaartermijnen/)). • De bewaartermijn voor overige gegevens moet worden vastgelegd in het dataregister/dossier [4] van de desbetreffende gegevensverzameling. • Naast wettelijke bewaartermijnen zijn voor MBO instellingen de selectielijst en het model documentair structuurplan (DSP) van de MBO Raad van toepassing voor overige bewaartermijnen voor documenten en gegevens (zie selectielijst_mbo_per_1-8-2017.pdf (mboraad.nl) en Model documentair structuurplan mbo | MBO Raad , “model_dsp_mbo_definitief_1-6-2020_0.xlsx”). • PM: Voor het VO is een selectielijst in voorbereiding. Deze wordt in 2023 verwacht. • Na afloop van de bewaartermijn, dient de data vernietigd te worden OF volledig geanonimiseerd te worden, voor zover vernietiging dan wel anonimisering niet strijdig is met een wettelijke bepaling. • Met leveranciers moeten contractuele afspraken gemaakt worden over bewaartermijnen en vernietiging dan wel anonimisering.

[4] Met een dataregister/dossier wordt hier bedoeld een beschrijving van de inhoud en het toepassingsgebied van een logische gegevensverzameling en welke toepassingen gebruik maken van die gegevensverzameling,

Hoofdprincipe 4	**Duurzaam en verantwoord**
Toelichting	We gaan op een duurzame en verantwoorde manier om met mensen, de aan ons toevertrouwde middelen en informatie.
Rationale	Het ROCvA-F wordt vanuit de overheid gefinancierd met publiek geld. Daardoor hebben we de verantwoordelijkheid naar de Nederlandse samenleving toe om duurzaam en verantwoord om te gaan met dat geld. Daarnaast heeft het ROCvA-F als onderwijsinstelling ook als taak om studenten mede voor te bereiden op hun positie in de Nederlandse samenleving en heeft daardoor tevens een voorbeeldfunctie. Deze voorbeeldfunctie wordt versterkt door de druk door menselijk handelen op de aarde voor wat betreft klimaat en hulpbronnen die steeds actueler wordt. Ook daardoor dient het ROCvA-F duurzaam en verantwoord om te gaan met mensen, middelen en informatie.
Implicaties	• Oplossingen op het gebied van informatievoorziening en ICT moeten in algemene zin direct of indirect bijdragen aan verbeteringen of besparingen voor het ROCvA-F of de onderwijssector. • Om verantwoorde keuzes te maken en de toegevoegde waarde expliciet te kunnen maken voor wijzigingen in oplossingen op het gebied van informatievoorziening en ICT, dient er bij aanvang van elk initiatief altijd een goede analyse gedaan te worden van het probleem of de vraag. Dat betekent onder andere dat er bij elk initiatief voldoende analysecapaciteit ingezet kan worden. Zo zouden bijv. business of informatie analisten een vast onderdeel van een projectorganisatie dienen te zijn. • We gebruiken waar mogelijk relevante en beschikbare referentie architecturen, standaarden, modellen, frameworks, etc. die reeds door derde partijen ontwikkeld zijn, indien deze een bijdrage kunnen leveren aan de verbetering van het onderwijs, de onderwijslogistiek of de bedrijfsvoering van het ROCvA-F. • De menselijke maat dient niet vergeten te worden bij oplossingen op het gebied van informatievoorziening en ICT.

Principe 4.1	**De toegevoegde waarde wordt benoemd**
Toelichting	De toegevoegde waarde wordt expliciet benoemd.
Rationale	Door de toegevoegde waarde van een oplossing op het gebied van informatievoorziening en ICT expliciet te benoemen denkt men er bewust over na. Dat kan alsnog tot een ander inzicht leiden. Daarnaast zorgt het ervoor dat de keuze verantwoord wordt en dat in een later stadium de rationale terug te halen is.
Implicaties	• De toegevoegde waarde van een oplossing in kwalitatieve of kwantitative zin dient altijd expliciet gemaakt te worden, door het opstellen van een business case. • Oplossingen op het gebied van informatievoorziening en ICT t.b.v. het primaire proces dienen aan te sluiten bij een behoefte vanuit de business (i.c. het onderwijs). • Wanneer een initiatief de implementatie of vervanging van een oplossing voor het onderwijs of de onderwijslogistiek betreft, dient

	een vertegenwoordiging vanuit het onderwijs te participeren in dat initiatief, dan wel in het voortraject geconsulteerd te worden. • Oplossingen op het gebied van informatievoorziening en ICT t.b.v. het primaire of secundaire proces moeten direct [of indirect] bijdragen aan een verbetering van het onderwijs zelf of de onderwijslogistiek of algemene bedrijfsvoering in geldelijke dan wel in kwalitatieve zin of een efficiëntie voordeel opleveren.

Principe 4.2	**We letten op de TCO (Total Cost of Ownership)**
Toelichting	We letten op de totale kosten van een oplossing (Total Cost of Ownership).
Rationale	Door niet alleen op de aanschafkosten van een oplossing te letten, maar ook de kosten mee te nemen van de implementatie en het beheer, krijgt men een realistischer beeld van de totale kosten.

Implicaties	• We kopen de oplossingen/diensten in i.p.v. deze zelf te ontwikkelen;
	  ○ Leidraad: “Saas, before reuse, before buy, before make”
	• We kiezen voor gestandaardiseerde en bewezen collectieve oplossingen/diensten, zoals o.a.:
	  ○ het gebruik van SURF diensten,
	  ○ keuze voor Microsoft producten, tenzij…
	  ○ standaard ‘bouwblokken’
	• Technisch beheer en applicatie beheer worden waar mogelijk extern belegd.
	• We voeren een actief Life Cycle Management (LCM) van ICT oplossingen (software & hardware).

Principe 4.3	**Oplossingen worden gedocumenteerd**
Toelichting	Oplossingen op het gebied van informatievoorziening en ICT worden beschreven voor wat betreft de inhoud en de actuele stand van zaken.
Rationale	Door oplossingen qua inhoud en de actuele stand van zaken te beschrijven en deze beschrijvingen bij te werken wanneer er iets gewijzigd wordt, ben je meer *in control*. Daardoor gaat bijvoorbeeld geen of minder tijd verloren met het in kaart brengen en analyseren van de bestaande situatie, wanneer oplossingen aangepast of vernieuwd moeten worden. Als gevolg daarvan kan een impactanalyse sneller en kwalitatief beter gemaakt worden en is men duurzaam en verantwoord bezig.
Implicaties	• Oplossingen moeten worden beschreven in een basis set aan documentatie (bijvoorbeeld in de vorm van; start architectuur, high level design, low level design of solution design, procesmodellen, datadefinities, etc.).

Principe 4.4	**We voldoen aan onderwijswet- en regelgeving**
Toelichting	Oplossingen op het gebied van informatievoorziening en ICT dienen te voldoen aan relevante onderwijswet- en regelgeving.

Rationale	Het spreekt voor zich dat iedere burger en organisatie zich aan de wet dient te houden. Uit bepaalde wet- en regelgeving, zoals specifieke wet- en regelgeving voor de onderwijssector, kunnen echter vereisten voortvloeien die meegenomen dienen te worden bij de keuze en inrichting van oplossingen op het gebied van de informatievoorziening en ICT.
Implicaties	• Oplossingen op het gebied van de informatievoorziening en ICT moeten getoetst worden aan relevante wet- en regelgeving voor de onderwijssector. • Om te controleren op de naleving van wet- en regelgeving dienen periodieke interne en externe audits uitgevoerd te worden.

Principe 4.5	**We volgen het centrale inkoopbeleid**
Toelichting	De aanschaf van oplossingen op het gebied van informatievoorziening en ICT wordt conform het centrale Inkoopbeleid van de ROCvA-F gedaan.
Rationale	Door bij de aanschaf het inkoopbeleid van de ROCvA-F te volgen en de afdeling Inkoop & Contractmanagement te consulteren dan wel te betrekken, zorgen we er voor dat we ook in die zin op een duurzame en rechtmatige manier oplossingen aanschaffen. De afdeling Inkoop & Contractmanagement zorgt er bijvoorbeeld voor dat we bij de aanschaf onder meer rekening houden met eventuele wettelijke vereisten, dat contracten gecontroleerd worden en niet nadelig uit kunnen pakken voor het ROCvA-F en dat indien nodig op contractuele bepalingen gestuurd kan worden in de relatie met leveranciers.
Implicaties	• Bij elk initiatief voor de aanschaf van oplossingen op het gebied van informatievoorziening en ICT dient de afdeling Inkoop geconsulteerd te worden, dan wel betrokken te zijn. • Wanneer een oplossing op het gebied van informatievoorziening en ICT aangeschaft dient te worden, dient nagegaan te worden of de oplossing door een van de reeds gecontracteerde leveranciers geleverd kan worden. • Wanneer de aanschaf een investering van meer dan 214.000 euro over de gehele maximale contractduur betreft, dient een aanbestedingsprocedure gestart te worden samen met de afdeling Inkoop. • Wanneer de aanschaf een investering tussen 70.000 en 214.000 euro over de gehele maximale contractduur betreft, dient een Meervoudig Onderhandse aanbestedingsprocedure gestart te worden, in overleg met de afdeling Inkoop.

Principe 4.6	**Wij zijn actief onderdeel van de onderwijssector**
Toelichting	Wij zijn onderdeel van de onderwijssector en leren van en samen met andere onderwijsinstellingen.
Rationale	Samen weet je meer dan alleen. Wanneer onderwijsinstellingen onderling kennis en ervaringen uitwisselen met elkaar, hoeft niet elke onderwijsinstelling zelf steeds het wiel uit te vinden of leergeld te betalen.

	Dit bevordert de professionalisering, de kwaliteit en het duurzaam gebruik van mensen en middelen.
Implicaties	• Actieve participatie in diverse gremia binnen de onderwijssector om van en met elkaar te leren.

Principe 4.7	**We adopteren de Sustainable Development Goals**
Toelichting	We willen actief bijdragen aan de realisatie van de Sustainable Development Goals van de VN.
Rationale	Het ROCvA-F vindt dat ze naast een maatschappelijke taak als onderwijsinstelling ook een afgeleide voorbeeldfunctie heeft en wil daarom ook zoveel mogelijk actief bijdragen aan een duurzame toekomst voor de wereld. Het ROCvA-F richt zich in dit kader met name op de SDG “Quality Education”.
Implicaties	• Bij de beoordeling van meerdere mogelijke oplossingsrichtingen dient de duurzaamheid en impact op SDG’s expliciet in de afweging meegenomen te worden. • Ook een eventuele negatieve impact van een oplossing op een SDG dient expliciet gemaakt te worden.

Hoofdprincipe 5	**Betrouwbare, toegankelijke en flexibele oplossingen**
Toelichting	Oplossingen op het gebied van informatievoorziening en ICT dienen betrouwbaar en toegankelijk te zijn en waar nodig flexibel te zijn.
Rationale	Om studenten en medewerkers optimaal te ondersteunen bij hun opleiding en hun werkzaamheden, dienen ze gebruik te kunnen maken van betrouwbare, gebruikersvriendelijke en waar nodig flexibele oplossingen op het gebied van informatievoorziening en ICT.
Implicaties	• De beschikbaarheid van oplossingen op het gebied van informatievoorziening en ICT is van primair belang, daarna volgen respectievelijk de toegankelijkheid (secundair) en de flexibiliteit (tertiair) van oplossingen. • Toegankelijkheid en flexibiliteit mogen geen veiligheidsrisico’s opleveren voor het landschap van het ROCvA-F of misbruik van informatie in de hand werken. • We streven naar *loosely coupled* systemen voor een betere flexibiliteit. • We werken aan geïntegreerde oplossingen, zoals op het gebied van de informatievoorziening.

Principe 5.1	**Elk moment, elke plaats, elk apparaat**
Toelichting	Gebruikers dienen oplossingen op het gebied van informatievoorziening en ICT te kunnen gebruiken onafhankelijk van het moment, op welke plaats en met welk *device* (apparaat).

Rationale	Gebruikers zijn tegenwoordig gewend om overal de beschikking te hebben over internet middels 4G en toegang te hebben tot diensten via smartphones, laptops en tablets vanuit huis, onderweg in bijv. het OV en op vakantie.
Implicaties	• Studenten en medewerkers worden voorzien van een geschikte werkomgeving, dan wel een geschikte werkplek. • De inrichting van het netwerk en de beveiliging ervan gaat ervan uit dat het niet uitmaakt of gebruikers zich op het interne netwerk van het ROCvA-F bevinden of op een externe locatie. • Op de locaties van het ROCvA-F is een draadloos netwerk beschikbaar, met een vergelijkbare kwaliteit en capaciteit als het vaste netwerk.

Principe 5.2	**Een optimale gebruikerservaring**
Toelichting	Tijdens het gebruik van oplossingen op het gebied van informatievoorziening en ICT, dient de gebruikerservaring zo optimaal mogelijk te verlopen.
Rationale	Om gebruikers effectief te kunnen ondersteunen, moeten oplossingen op het gebied van informatievoorziening en ICT zo toegankelijk, gebruiksvriendelijk en intuïtief als mogelijk is werken.
Implicaties	• Bij alle oplossingen op het gebied van informatievoorziening en ICT, dienen de toegankelijkheid, het gebruiksgemak en de gebruikersinteractie een actief punt van aandacht (bijv. een selectiecriterium) te zijn. • SaaS toepassingen dienen een Responsive Design of een app te hebben, om op meerdere soorten *devices* gebruikt te kunnen worden. • Applicaties worden in het Nederlands aangeboden en waar nodig en mogelijk ook meertalig aangeboden. • Applicaties dienen zoveel mogelijk toegankelijk en bruikbaar te zijn voor visueel gehandicapten, door bijvoorbeeld screenreader ondersteuning.

Principe 5.3	**We doen actief aan Life Cycle Management (LCM)**
Toelichting	We werken actief aan het up-to-date houden van oplossingen op het gebied van informatievoorziening en ICT.
Rationale	Om betrouwbare oplossingen te kunnen bieden, is het van belang om je oplossingen up-to-date te houden. Daarmee voorkom je dat je technische achterstanden gaat opbouwen, die later alsnog tegen hogere kosten in tijd en geld moeten worden opgelost. Daarnaast profiteer je ook van de laatste ontwikkelingen wanneer je up-to-date bent.
Implicaties	• Software loopt in de regel maximaal 1 release achter (N-1) op de actuele versie.

Links

- MORA (MORA (mbodigitaal.nl)) referentiearchitectuur voor het MBO
- FORA (https://fora.wikixl.nl/index.php/Hoofdpagina) referentiearchitectuur voor het VO
- Edustandaard (https://www.edustandaard.nl/)
- Burchtmodel SURF: https://www.surf.nl/files/2019-01/flexibele-en-persoonlijke-leeromgeving---een-functioneel-model_web.pdf
- Burchtmodel bij het ROCvA-F: https://talnet.sharepoint.com/sites/De-digitale-leeromgeving/SitePages/Home.aspx)
- NCSC security maatregelen: https://www.ncsc.nl/onderwerpen/basismaatregelen

ROC van Amsterdam – ROC van Flevoland