Nr	Principe	Omschrijving	Rationale	Implicaties	Hardheid	Architectuurlaag
B1	Beheersbaar	HJL is betrouwbaar, risicomijdend en zo nodig risico mitigerend. HJL streeft naar een beheersbare en controleerbare situatie op alle producten, diensten, dienstverlening, processen en IT middelen	HJL levert kwaliteit en betrouwbaarheid en streeft naar maximale veiligheid. Door continu onderhouden en verbeteren van beheersbaarheid wordt voorkomen dat er ongewenste situaties ontstaan: • Onnodige complexiteit • Onbetrouwbare installaties • Onbetrouwbare IT-middelen en voorzieningen • Onbetrouwbare informatie Hiermee ontstaat een veilige situatie, en een stabiele en voorspelbare informatievoorziening.	Veranderingen worden planmatig uitgevoerd. Automatiseren is geen doel op zich. Er wordt gekozen voor een juiste verhouding tussen wendbaarheid, flexibiliteit en kosteneffectiviteit bij het automatiseren van functies en processen. HJL is altijd in regie over de IT middelen en in control over de informatievoorziening. De datakwaliteit is in orde.	Eis	Bedrijfsarchitectuur
B8	Standaard beheerprocessen	De processen met betrekkingen tot het onderhoud en beheer zijn ingericht conform ITIL, ASL en BiSL	Gebruik maken van standaarden voorkomt het opnieuw uitvinden van het wiel. Bovendien maakt dit het eenvoudiger om nieuwe medewerkers of externen in te zetten op beheertaken.	Beheerprocessen volgen de standaarden in ITIL, ASL en BiSL ITIL: Information Technology Infrastructure Library ASL: Application Services Library BiSL: Business Information Services Library Medewerkers in beheerfuncties worden opgeleid in deze standaarden. Bij werving van beheermedewerkers is kennis van deze standaarden een pré.	Advies	Bedrijfsarchitectuur
A2	Best of suite	IT-systemen worden geselecteerd op basis van een best-of-suite aanpak	Een suite van IT systemen van één leverancier biedt het hoogste niveau van integratie en integratieproblemen die optreden moeten worden opgelost door de leverancier. Het kopen van een suite van een leverancier biedt ook de mogelijkheid op additionele korting.	Er wordt gekozen voor een beperkt aantal strategische leveranciers die brede suites aanbieden. Mensen en kennis worden zoveel mogelijk gericht op de geselecteerde suites. Nieuwe functionaliteit wordt gerealiseerd met het verantwoordelijke IT systeem in de suite.	Advies	Applicatiearchitectuur
A3	Generieke processen en systemen	Er wordt gebruik gemaakt van generieke processen en systemen.	Door te denken in generieke processen en systemen wordt maatwerk voorkomen en worden kosten bespaard. Hierdoor kan eenvoudiger gebruik worden gemaakt van standaardprocessen en oplossingen die beschikbaar zijn in de markt.	Processen worden gebaseerd op generieke procesmodellen. Bij het specificeren van functionaliteit wordt een goede balans gezocht tussen generiticiteit en voldoende procesondersteuning. Processen en systemen worden niet ingericht op uitzonderingen. Organisatie specifieke keuzes worden uitgedrukt in (beleids)regels die binnen de generieke processen en functionaliteiten gehanteerd kunnen worden. Er zijn soms concessies nodig bij het inrichten van processen en systemen om maatwerk te voorkomen. Als er standaard oplossingen beschikbaar zijn dan wordt daar gebruik van gemaakt om zo organisatie specifieke oplossingen te voorkomen.	Advies	Applicatiearchitectuur
A4	Centrale administratie identiteiten	Identiteiten, rollen en (grofmazige) autorisaties worden centraal geadministreerd.	Het is efficiënter om identiteiten, rollen en autorisaties centraal vast te leggen en beheren. Het zorgt er ook voor dat er centraal zicht is op identiteiten, dat functiescheidingsregels kunnen worden gecontroleerd en dat gebruik van applicaties kan worden herleid naar specifieke gebruikers. Daarnaast is het een randvoorwaarde om gebruikers minder vaak in te laten loggen. Zij kunnen hun identiteit en inloggegevens voor meerdere applicaties gebruiken.	Gegevens over identiteiten, rollen en autorisaties en wijzigingen hierin worden gekoppeld naar doelsystemen die hiervan gebruik maken. De koppeling met autorisatiebronnen en doelsystemen is bij voorkeur geautomatiseerd zodat wijzigingen direct effectief zijn (gebruikers snel toegang hebben, autorisaties snel kunnen worden ingetrokken). Er is in het proces geborgd dat gebruikers snel geregistreerd worden, zodat ze vervolgens snel toegang kunnen krijgen tot systemen en applicaties. Idealiter worden er geen persoonsgebonden accounts handmatig aangemaakt, maar gebeurt bij voorkeur automatisch vanuit de centrale administratie. Applicaties hebben bij voorkeur zelf geen wachtwoordadministratie.	Eis	Applicatiearchitectuur
A5	Beschikbaarheid	Bedrijfsprocessen worden niet verstoord door de implementatie van veranderingen.	Bedrijfsprocessen zijn de kern van de organisatie en verstoringen hierin hebben een grote impact op de organisatie. Organisaties veranderen continu en frequente verstoringen zijn onacceptabel.	Nieuwe processen en systemen worden niet geïmplementeerd tenzij ze volgens een afgesproken methodiek (vb. TMap) zijn getest en goedgekeurd. Het niet kunnen beschikken over applicaties wordt geminimaliseerd gedurende installatie of vervanging, en wordt bij voorkeur buiten kantooruren uitgevoerd. Rekening houden met servicewindows.	Eis	Applicatiearchitectuur
A7	Serviceniveau-overeenkomsten	Er zijn serviceniveau-overeenkomsten met externe beheerders van applicaties en infrastructuur.	Medewerkers verwachten in het algemeen dat zij hun werk kunnen doen en dat de daarvoor benodigde serviceniveaus expliciet worden bewaakt. Als applicaties en infrastructuur door externe partijen worden beheerd is het belangrijk dat er goede afspraken worden gemaakt met de leverancier over het bewaken van deze serviceniveaus. Dit voorkomt dat de leverancier zijn verantwoordelijkheid hierin naar IV/Regie afschuift.	Het is bij de IT-afdeling bekend welke applicaties de organisatie zelf beheert en welke applicaties door externe partijen worden beheerd. De serviceniveaus van de applicaties en infrastructuur die intern en extern worden beheerd zijn expliciet in kaart gebracht. De business behoefte achter deze SLA's is duidelijk bij IV/Regie.	Eis	Applicatiearchitectuur
A8	Rol gebaseerd autorisatie	Toegang tot autorisatieobjecten is gebaseerd op rollen.	Het hebben van een identiteit is niet voldoende om toegang te krijgen tot een systeem, er is ook een autorisatie noodzakelijk. Door autorisaties te baseren op de rol van de gebruiker hoeven autorisaties niet noodzakelijkerwijs op individueel niveau te worden toegekend, waardoor autorisatiebeheer efficiënter kan plaats vinden. Hierdoor is de organisatie ook beter in staat om de rechtmatigheid van uitgegeven autorisaties te controleren.	Er is centraal een aantal rollen benoemd, gedifferentieerd naar de functies, processen, afdelingen/opleidingen van gebruikers. Autorisaties worden zoveel mogelijk gebaseerd op rollen en niet op individuele gebruikers. Mogelijk dat in de bepaalde applicaties nog fijnmazig geautoriseerd moet worden.	Eis	Applicatiearchitectuur
A9	Standaard protocollen	Interfaces maken gebruik van actuele en gangbare standaarden voor berichtopmaak en communicatieprotocol.	Standaard pakketten, ontwikkelsuites en integratieplatforms ondersteunen over het algemeen de meest gangbare standaarden. Gebruikmaken hiervan houdt in dat op basis van bestaande functionaliteit gekoppeld kan worden. Het vervangen van componenten binnen het applicatielandschap is eenvoudiger als deze geïntegreerd zijn met gebruikmaking van actuele en gangbare standaarden. Standaarden zijn veelal goed doordacht en daardoor robuust qua performance en security.	Bij selectie van standaard IT-voorzieningen is het ondersteunen van standaarden een belangrijk criterium. Bij het ontwikkelen van koppelingen worden afspraken gemaakt over de te gebruiken standaarden. Tijdens onderhoud en beheer worden koppelingen die gebaseerd zijn op achterhaalde standaarden vervangen door actuele standaarden. Forumstandaardisatie.nl biedt de overheidsstandaarden.	Eis	Applicatiearchitectuur

Nr	Principe	Omschrijving	Rationale	Implicaties	Hardheid	Architectuurlaag
G3	Betrouwbare en herzienbare wijzigingen	Wijzigingen en mutaties moeten betrouwbaar gecommuniceerd worden en zijn herzienbaar.	Wijzigingen mogen niet zomaar verloren gaan. Gebruikers dienen erop te kunnen vertrouwen dat de wijzigingen die zij aanbrengen, worden doorgevoerd in alle relevante administraties. Er worden daarom hoge eisen gesteld aan de wijze waarop wijzigingen worden gecommuniceerd.	Berichten die gericht zijn op het melden van mutaties worden verstuurd via een transportmechanisme dat een garantie op aflevering biedt zoals een "message queue". Alle schakels in de communicatie van mutaties zijn transactioneel, ook de gebruikte message queues. Als er geen gebruik kan worden gemaakt van transactionaliteit dan moeten services idempotent zijn, zodat ze net zolang kunnen worden aangeroepen totdat er een bevestiging is ontvangen. Indien er fouten optreden in de verwerking van mutatieberichten is dit de verantwoordelijkheid van de ontvangende applicatie. Protocollen tot wijzigingen moeten ingevoerd worden.	Eis	Gegevensarchitectuur
G4	Standaardisatie van data	Data hanteren een standaard definitie en zijn beschikbaar in een gestandaardiseerd formaat.	Om gegevens goed te kunnen uitwisselen, is het belangrijk dat het helder is wat hun structuur en definitie is. Door deze definities te standaardiseren wordt een uniforme interpretatie mogelijk en wordt afhankelijkheid van specifieke apllicaties of leveranciers voorkomen. Daarbij is de vorm (formaat) relevant, omdat anders gegevens mogelijk nog steeds niet toegankelijk zijn. Een standaard definitie en formaat maakt zowel integratie tussen applicaties als migraties naar nieuwere versies van bestaand applicaties of nieuwe applicaties veel eenvoudiger.	Er zijn standaard gegevensdefinities en formaten vastgesteld voor de verschillende soorten gegevens, waarbij maximaal wordt aangesloten bij bestaande standaarden zoals aangegeven in de lijst van het Forum Standaardisatie. Applicaties worden geselecteerd op ondersteuning van de geselecteerde gegevensdefinities en formaten.	Advies	Gegevensarchitectuur
G7	Data Governance	Data Governance wordt gedefinieerd als het uitoefenen van gezag en controle (plannen, monitoren en handhaving) over alle datamanagement aspecten.	Data Governance zorg ervoor dat data beheerd worden volgens beleid en best practices. Waar DM duiding geeft over wat en hoe er iets moet gebeuren, geeft DG duiding over het waarom en door wie. Data Management kan alleen goed uitgevoerd worden onder de correcte autoriteit van Data Governance.	Data Governance wordt ingericht voor alle beheerde data.	Advies	Gegevensarchitectuur
P1	Accounts zijn persoonlijk.	Accounts zijn herleidbaar naar natuurlijke personen.	Voor het zinvol loggen van activiteit is het van belang dat het account herleidbaar is naar een natuurlijk persoon.	Alle accounts waarmee kan worden ingelogd op een apparaat voor medewerkers zijn gekoppeld aan een specifieke medewerker en kan ook alleen gebruikt worden door die specifieke medewerker.	Eis	Privacy en security architectuur
P2	Toegang is centraal ingericht.	Alle toegangsrechten voor medewerkers zijn centraal ingericht en vastgelegd.	Toegangsrechten wordt éénmalig gedefinieerd voor onderhoudbaarheid en consistentie redenen. Medewerkers hoeven maar 1x in te loggen.	Toegangsrechten worden ingericht en vastgelegd in de centrale directory en applicaties worden gekoppeld met de centrale directory. Nieuwe voorzieningen maken altijd gebruik van de centrale directory (knock-out criterium).	Eis	Privacy en security architectuur
P3	Privacy & Security by Design.	In elke fase van aanschaf of ontwikkelen van producten en diensten zijn bescherming van gegevens een integraal onderdeel, dit zonder afbreuk te doen aan de functionaliteit daarvan. Vooral persoons- en andere vertrouwelijke gegevens moeten goed worden beschermd.	Door privacy en security tijdens de aanschaf of ontwikkeling als onderdeel mee te nemen wordt de kwaliteit van de oplossing hoger door er te zorgen dat privacy en security risico's zo klein mogelijk blijven. Dit door vroegtijdig al over deze risico's na te denken, maatregelen te treffen en besluit te nemen. Het voorkomen van privacy en security risico's staan centraal.	Risico analyses bij start van elk project/traject waar informatievoorziening een rol speelt (al dan niet geautomatiseerd). DPIA wordt uitgevoerd. Doel van verwerking van persoonsgegevens is duidelijk en de verwerking is daarmee verenigbaar. Daarbij worden persoonsgegevens niet langer bewaard dan nodig is voor het doel van de verwerking. BIA wordt uitgevoerd. Afspraken over risico's en maatregelen worden vastgelegd en getoetst. Bij derden afgenomen diensten en producten worden ook de verdere afspraken over kwaliteitscriteria altijd vastgelegd.	Eis	Privacy en security architectuur
P4	Zero Trust.	Zero Trust is een beveiligingsmodel met set basisprincipes* dat uitgaat van 'Never trust, always verify': het netwerk is in principe vijandig en elk request moet geverifieerd/gevalideerd zijn. Het maakt gebruik van fijnmazige netwerksegmentatie en biedt dreigingspreventie op de randen van segmenten. Met een gedetailleerde conditionele gebruikerstoegangscontrole.	Veranderingen als plaats-, tijd en apparaat onafhankelijk werken hebben een grote impact op de exacte randen van het hJL netwerk; deze worden steeds diffuser. Enerzijds wordt deze opgerekt door gebruik van cloud & hosting oplossingen waarbij niet alles meer in één datacenter staat en binnen een datacenter ook infrastructuur wordt gedeeld met andere organisaties, anderzijds komen binnen het netwerk steeds meer 'vreemde' dan wel slechts deels door de organisatie beheerde apparatuur voor. Horizontale bewegingen binnen een netwerk moeten zoveel als mogelijk beperkt worden.	Zero Trust behelst een aantal basisprincipes. Volledige implementatie is een grote stap, daarom bij elke vervanging of uitbreiding deze principes als uitgangspunt te nemen. De principes zijn verwoord in P5 tot en met P9. Bij aanschaf/vernieuwing wordt gekeken naar services en producten die ontworpen zijn vanuit zero trust.	Eis	Privacy en security architectuur
P5	Identificeer de te beschermen onderdelen van de IT-infrastructuur en beveilig alle paden er naartoe	Breng alle Data, Assets, Applicaties, Services en Gebruikers in de infrastructuur in kaart. Ken de identiteiten van de elementen. Breng alle transactiestromen op basis van de interacties tussen deze elementen in kaart. Beveilig deze transactiestromen.	Om zero trust toe te kunnen passen is het noodzakelijk om alle componenten die een rol spelen in de infrastructuur te kennen en herkennen. Dit helpt om onderlinge afhankelijkheden tussen gevoelige gegevens, applicaties (bijvoorbeeld web-, applicatie-, en databaseservers), netwerkservices en gebruiker te achterhalen en begrijpen. De key resources te identificeren, waarbij resources een brede categorie is met ook SaaS, IoT en evt. ook BYOD devices.	Elk element in de IT infrastructuur is bekend en geïdentificeerd, ook tijdelijke, gast, etc. Verwacht gedrag van deze elementen is in kaart gebracht. Key elementen en belangrijkste risico's worden benoemd en 'legacy' elementen die zero trust niet ondersteunen in eigen segmenten opgenomen. Netwerksegmentatie is zo klein als mogelijk; functionele, losstaande omgevingen met een eigen perimeter en toegangscontrole.	Eis	Privacy en security architectuur
P6	Verschaf alleen toegang tot informatie via beveiligde verbindingen, ongeacht de locatie	Toegang tot assets en communicatie in de hJL eigen netwerk omgeving moeten voldoen aan dezelfde beveiligingseisen als die vanuit een niet hJL eigen netwerk. Alle communicatie moet worden gedaan op de meest veilige manier die beschikbaar is, de vertrouwelijkheid en integriteit beveiligd en de bron authentiseert.	Zero trust betekent dat ook een eigen netwerk locatie niet per definitie veilig is. Vertrouw geen enkel netwerk, ook het eigen netwerk niet. In andere woorden vertrouwen moet niet automatisch toegekend worden omdat een device in de hJL netwerk infrastructuur aanwezig is.	Alle connecties zijn geauthentiseerd en alle verkeer is geencrypt.	Eis	Privacy en security architectuur
P7	Handhaaf strikte toegangscontrole op een need-to-know-basis	Authentiseer en autoriseer alles. Toegang tot individuele resources wordt toegekend per sessie en gebaseerd de minste rechten ('least privilige') nodig om de taak uit te voeren waarbij authenticatie voor toegang is geëvalueerd. Toegang tot een resource betekent niet automatisch toegang tot een andere resource.	Een sterke controle op identiteit van de aanvrager van een verzoek is nodig om te bepalen of de aanvrager te 'vertrouwen' is. Daarbij moet de aanvrager ook het recht hebben om het specifieke verzoek te doen. Waarbij voorwaardelijke toegang en beperking van sessierisico's een verdere beperking van mogelijk misbruik verkleinen.	De gebruiker alleen toegang krijgt tot tools, data en segmenten die daadwerkelijk nodig zijn voor het werk dat diegene doet. Gebruikers koppelen aan vooropgestelde rollen en groepen, helpt om dit inzichtelijk te maken. Een centrale identiteitsprovider die open standaarden ondersteunt is nodig voor bepalen van de identiteit. Toegang van services is beperkt tot data en segmenten die nodig zijn voor de specifieke taak van de service en de toegang is klein als mogelijk tot resources; geen generieke accounts die een groot aantal taken kan uitvoeren.	Eis	Privacy en security architectuur

Nr	Principe	Omschrijving	Rationale	Implicaties	Hardheid	Architectuurlaag
P8	Bepaal de toegangsrechten op basis van mate van vertrouwen die afgeleid wordt uit verschillende attributen van de toegangsaanvraag. (Conditional access)	Toegangsrechten worden bepaald op basis van een dynamische policy inclusief identiteit, apparaat, IP adres, locatie, applicatie/service inclusief eventuele gedrags- en omgevingsvariabelen.	Zero trust vraagt om risico gebaseerd toegang geven waarbij een combinatie van attributen bepaald hoe vertrouwd een aanvraag is en daarmee welke resources benadert mogen worden. Dit geeft meer flexibiliteit waarbij ook specifieke resources gedeeld kunnen worden met gast gebruikers of partner organisaties. Business behoeften en geaccepteerd risiconiveau bepalen de attributen en policies.	Ontwikkel autorisatie policies vanuit de “Kipling-vragen”: wie, wat, wanneer, waar, waarom en hoe moet er al dan niet toegang verleend worden. Elke aanvraag voor data of services moet geauthentiseerd worden tegen een policy. Conditional access en multifactor authenticatie zijn belangrijke componenten in deze.	Eis	Privacy en security architectuur
P9	Zorg voor uitgebreide monitoring en logging.	Verzamel zo veel informatie als mogelijk over de status van alle assets, infrastructuur en communicatie hiertussen om de beveiliging continue te verbeteren. Bewaak en onderhoud het geheel door het analyseren van de informatiestromen van het netwerk, systemen, applicaties en de cloud. Monitor en meet de integriteit en beveiligingsstatus van alle componenten, signaleer als er afwijkingen zijn. Leg de gebeurtenissen vast (logging).	Continue controle van alle dataverkeer en assets is nodig om te veiligheidsstatus van alle componenten die op het netwerk actief zijn vast te stellen. Alleen op die manier kan in een dynamische netwerkomgeving de beveiliging geborgd worden en een eventuele inbreuk gedetecteerd worden zodat impact beperkt kan worden. Logging is is essentieel om indien nodig de juiste interventies te doen en maatregelen te nemen. Daarnaast om vanuit controle perspectief noodzakelijk om achteraf vastte stellen wat er heeft plaatsgevonden en wie toegang heeft gehad tot welke data.	De focus van monitoring gaat naar het gedrag van gebruikers, devices en services. Monitoring van dat gedrag moet vertaald worden naar de 'gezondheid' van het netwerk. Automatisering van de monitoring gegevensstromen is essentieel om de belangrijkste hits als eerst te krijgen. Zorg dat verzamelde loggegevens en informatiestromen samen komen op een punt en maak onderscheid tussen normaal en abnormaal gedrag. Bepaal de privacy gevoelige informatie in logging en stem maatregelen (o.a. toegang en bewaren hierop af)	Eis	Privacy en security architectuur
T1	Voorzieningen zijn plaats en tijd onafhankelijk.	De voorzieningen zijn plaats- en tijdonafhankelijk beschikbaar	Medewerkers willen op allerlei plaatsen en momenten toegang kunnen krijgen tot de voor hen geautoriseerde ICT voorzieningen	Medewerkers hebben alleen een webbrowser en Internetverbinding nodig op een door HJL gemanaged apparaat om toegang te krijgen tot functionaliteit en gegevens die door de organisatie wordt aangeboden. De voorzieningen zijn ook ‘s avonds en in het weekend beschikbaar. Er is binnen de organisatie op iedere vestiging een draadloos netwerk met toegang tot het bedrijfsnetwerk.	Advies	Technische architectuur
T2	Uniform en beproefd	De technische diversiteit van oplossingen wordt beperkt en er wordt gebruik gemaakt van beproefde technologie.	Vanuit efficiëntie is het van belang te uniformeren en research te beperken. Het beperken van diversiteit van oplossingen beperkt de complexiteit.	Nieuwe technische wensen worden ingepast in bestaande oplossingen. Nieuwe voorzieningen worden geselecteerd op basis van beproefde technologie.	Eis	Technische architectuur
T3	Hergebruik voor kopen voor bouwen.	Hergebruik van bestaande IT voorzieningen heeft de voorkeur boven het kopen van IT voorzieningen. Het kopen van IT voorzieningen heeft de voorkeur boven bouwen.	Vanuit efficiëntie is het van belang zoveel mogelijk voorzieningen her te gebruiken. Voorzieningen standaard aanschaffen is veel efficiënter dan voorzieningen –laten-bouwen.	Voor het verwerven van nieuwe voorzieningen zal eerst worden nagegaan of er al bestaande voorzieningen beschikbaar zijn welke kunnen worden hergebruikt. Als dat niet het geval is wordt nagegaan of de voorziening (min of meer kant en klaar) te koop is. Pas nadat ook dat niet het geval is wordt de voorziening (al dan niet in huis) gebouwd.	Eis	Technische architectuur
T4	SAAS, PAAS, IAAS, On-Premise.	Cloud oplossingen hebben de voorkeur boven on-premise oplossingen.	Online (cloud) dienstverlening biedt voornamelijk flexibiliteit en schaalbaarheid voordelen. Ook biedt online dienstverlening voordelen bij zaken als geautomatiseerd beheer.	Voor het verwerven van nieuwe voorzieningen zal eerst worden nagegaan of de voorziening middels SAAS gerealiseerd kan worden. Als dat niet het geval is wordt nagegaan of de voorziening middels PAAS gerealiseerd kan worden. Als dat niet het geval is wordt nagegaan of de voorziening middels IAAS gerealiseerd kan worden. Pas nadat ook dat niet het geval is wordt de voorziening on-premise gerealiseerd.	Eis	Technische architectuur
T5	Ondersteunde technologie.	Technologie wordt in lijn gehouden met de richtlijnen van de leverancier voor ondersteuning.	Dit garandeert de toekomstige ondersteuning van de leverancier. Het voorkomt dat er grootschalige technologiemigraties moeten plaats vinden op momenten waarop het niet uit komt. Daarnaast kan gebruik gemaakt worden van nieuwe functionaliteiten in technologie.	Technologie voldoet altijd aan de voorwaarden voor de verlening van service en onderhoud van de leverancier. Technologie-upgrades worden ingepland op basis van het releaseschema van leveranciers, zonder dat hier behoeften van gebruikers aan ten grondslag liggen. Er is een standaard budget beschikbaar voor technologie-upgrades.	Eis	Technische architectuur
T7	Ontkoppeld.	Een component dient zoveel mogelijk ontkoppeld te zijn van zijn omgeving. De functionaliteiten van een component hebben een hoge cohesie (er is een logische samenhang tussen de functionaliteiten). De interfaces tussen de componenten zijn helder gedefinieerd, standaard en zo minimaal mogelijk (loosely coupled)	Door het beperken van de onderlinge afhankelijkheid tussen componenten en het standaardiseren van de interfaces kunnen componenten onafhankelijk van elkaar aangepast en vervangen worden. Hiermee wordt de wendbaarheid en flexibiliteit verhoogd, worden (open) innovaties ondersteund, zodat (samen met andere partijen) proactief op veranderingen in de markt kan worden ingespeeld.	Veranderingen dragen bij aan het ontkoppelen. Design for change: bij het ontwerpen, inrichten en uitvoeren van activiteiten wordt rekening gehouden met (on)voorziene veranderingen en worden duidelijke koppelvlakken benoemd en gedocumenteerd. Standaardisatie op koppelvlakken (IT-)systemen zijn modulair ontworpen en ingericht. Dat betekent dat elementaire functies worden ontworpen en deze vervolgens zelfstandig	Eis	Technische architectuur
T8	OTAP gescheiden.	Ontwikkel-, test-, en acceptatieomgevingen zijn in ieder geval logisch gescheiden van productieomgevingen.	OTAP omgevingen mogen elkaar niet beïnvloeden en bij gebruik dient duidelijk te zijn of het een ontwikkel-, test-, acceptatie of productie omgeving betreft.	Ontwikkel en test omgevingen bevinden zich fysiek bij de leverancier. Binnen de omgevingen van HJL (zowel on-prem als in de cloud) bevinden zich uitsluitend acceptatie en productie omgevingen. Acceptatie en productie omgevingen zijn minimaal op server niveau gescheiden. Acceptatie omgevingen zijn duidelijk herkenbaar en worden slechts beperkt beschikbaar gesteld. Ten behoeve van opleidingen kan er een specifieke data set worden gekoppeld en beschikbaar worden gesteld. Opleiding omgevingen zijn duidelijk herkenbaar en worden slechts voor opleidingen beschikbaar gesteld.	Eis	Technische architectuur
T9	Standaard in productie name.	Voorzieningen worden uitsluitend na acceptatie middels de standaard/geautomatiseerde uitrol mechanismes van IT infra leverancier uitgerold op apparatuur bedoeld voor medewerkers.	Apparatuur voor medewerkers is en blijft standaard ingericht. Daarmee ontstaat een gecontroleerde en efficiënte omgeving.	Alvorens een voorziening of een aanpassing op een voorziening wordt uitgerold vind er een acceptatie plaats conform een vastgesteld acceptatie protocol. De IT infra leverancier van HJL gebruikt geautomatiseerde uitrol mechanismen. In overleg met de IT infra leverancier kan een specifiek geautomatiseerd uitrol mechanisme worden toegepast (bv Azure devops of Octopus)	Eis	Technische architectuur
T10	Ontwerp en documentatie	Van elke oplossing is een goedgekeurd ontwerp (incl requirements) en documentatie beschikbaar	Documentatie zorgt voor beheersbare en betrouwbare oplossingen.	Een vernieuwingstraject (nieuwbouw, onderhoud) krijgt pas decharge als de documentatie ook op orde is. Goedgekeurde documentatie is daarmee een acceptatiecriterium.	Eis	Technische architectuur