# Architectuurprincipes

Voor de aanbesteding relevante principes zijn in onderstaande tabel opgenomen.

| Nr | Principe | Omschrijving |
|---|---|---|
| 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 |
| B6 | Omnichannel | Het resultaat van de dienst is gelijkwaardig, ongeacht het kanaal waarlangs de dienst wordt aangevraagd of geleverd. |
| B8 | Standaard beheerprocessen | De processen met betrekkingen tot het onderhoud en beheer zijn ingericht conform ITIL, ASL en BiSL |
| A1 | Administratie koppelvlakken | Koppelvlakken worden expliciet gedocumenteerd en geregistreerd in een centrale administratie |
| A2 | Best of suite | IT-systemen worden geselecteerd op basis van een best-of-suite aanpak |
| A4 | Centrale administratie identiteiten | Identiteiten, rollen en (grofmazige) autorisaties worden centraal geadministreerd. |
| A7 | Serviceniveau-overeenkomsten | Er zijn serviceniveau-overeenkomsten met externe beheerders van applicaties en infrastructuur. |
| A8 | Rol gebaseerde autorisatie | Toegang tot autorisatieobjecten is gebaseerd op rollen. |
| A9 | Standaard protocollen | Interfaces maken gebruik van actuele en gangbare standaarden voor berichtopmaak en communicatieprotocol. |
| G1 | Opslag bij de bron | Data worden uitsluitend en uniek bij de bron opgeslagen. De bron is de database van de applicatie waar de gegevens ingebracht/aangemaakt worden. |
| G2 | Controle bij de bron | Controle over de invoer, bewaring en houdbaarheid moet sterk gereguleerd worden omdat deze taken verspreid zijn over de verschillende bronapplicaties. |
| G3 | Betrouwbare en herzienbare wijzigingen | Wijzigingen en mutaties moeten betrouwbaar gecommuniceerd worden en zijn herzienbaar. |
| G4 | Standaardisatie van data | Data hanteren een standaard definitie en zijn beschikbaar in een gestandaardiseerd formaat. |
| G5 | Data beschreven en geclassificeerd | Data worden beschreven in een centrale "data-dictionaire" en een "business glossary" en geclassificeerd volgens drie standaard principes: vertrouwelijkheid, integriteit en beschikbaarheid. |
| G8 | Beheer externe gegevens | Externe gegevens – waarvan we niet de eigenaar zijn – worden niet gemuteerd. |
| P1 | Accounts zijn persoonlijk. | Accounts zijn herleidbaar naar natuurlijke personen. |
| P2 | Toegang is centraal ingericht. | Alle toegangsrechten voor medewerkers zijn centraal ingericht en vastgelegd. |
| 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. |
| 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. |

| Nr | Principe | Omschrijving |
|---|---|---|
| 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. |
| 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. |
| 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). |
| P11 | Transparantie | Klanten kunnen inzage krijgen in de procesgegevens en inhoudelijke informatie in hun dossier. |
| T2 | Uniform en beproefd | De technische diversiteit van oplossingen wordt beperkt en er wordt gebruik gemaakt van beproefde technologie. |
| 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. |
| T4 | SAAS, PAAS, IAAS, On-Premise. | Cloud oplossingen hebben de voorkeur boven on Premise oplossingen. |
| T5 | Ondersteunde technologie. | Technologie wordt in lijn gehouden met de richtlijnen van de leverancier voor ondersteuning. |
| 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) |
| T8 | OTAP gescheiden. | Ontwikkel-, test-, en acceptatieomgevingen zijn in ieder geval logisch gescheiden van productieomgevingen. |
| 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. |