Koninklijke Kentalis

Kentalis Enterprise Architectuur
Architectuurprincipes
Draft v 1.13

Kentalis Enterprise Architectuur

V1.12 Draft
Menno Gresnigt, Raphael Maes, Joris Sikkema, Albert Wijbenga, Han van Loenhout,

Juli 2025

Versie historie

Versie	Datum	Auteur(s)	Samenvatting van de wijzigingen
1.0	30-11-2021	Han van Loenhout en Jacco Vlijm	Goedgekeurde versie
1.1	04-05-2022	Menno Gresnigt, Rob van Dun, Jacco Vlijm, Han van Loenhout	Update principes
1.11	16-03-2023	Han van Loenhout	Kleine correcties en textuele aanpassingen Correctie nummering infra & cloud principes Toevoeging beheerprincipes
1.12	03-04-2025/ 26-06-2025	Raphael Maes, Albert Wijbenga, Han van Loenhout, Menno Gresnigt	Toevoeging AI-principes Review door virtueel architectuurteam, Leoni Dols en Sebastiaan Dekker.
1.13	10 september 2025	Menno Gresnigt	Suggesties van MT ICT leden verwerkt, APP08 toegevoegd
2.0	22 oktober 2025	Menno Gresnigt	Versie nummer verhoogd na vaststelling door MT ICT

Doel en Gebruik

Doel en gebruik van architectuurprincipes

Architectuurprincipes zijn van nut bij het nemen van beslissingen daar waar bij het opstellen van de Kentalis Enterprise architectuur en onderliggende domein & project architecturen keuzes gemaakt moeten worden.

Kentalis Enterprise architectuur (KEA):

- **Randvoorwaarden** | Zijn “hard”, niet onderhandelbaar, daar moet een architectuur aan voldoen, bijv. wet en regelgeving.
- **Standaarden** | Vastgestelde normen en eisen waaraan oplossingen moeten voldoen
- **Principes**
  - Geven aan wat belangrijk gevonden wordt door Kentalis, waar vooral op gelet moet worden bij het opstellen van een architectuur en keuzes voor oplossingen
  - De Ideale oplossing; Idealiter voldoet een architectuur volledig aan alle principes
  - In de praktijk valt dat vaak tegen: afwegingen en keuzes moeten gemaakt worden tussen alternatieven

Gebruik architectuur principes:

- als leidraad bij het opstellen en onderhouden van een architectuur;
- bij applicatie intake en bij het beoordelen van scenario's en maken van keuze;
- ‘Pas toe of leg uit’ : De principes zijn van toepassing op alle onderdelen van Kentalis. Iedereen is verplicht om deze principes na te leven of uit te leggen waarom men niet kan of wil voldoen. De implicatie van afwijking is een grotere complexiteit van ICT-diensten van/aan Kentalis en die leiden tot hogere kosten ervan. De implicatie kan ook zijn een geringere veiligheid. Een voorgestelde oplossing kan op onderdelen afwijken van de architectuurprincipes, mits expliciet onderbouwd en goedgekeurd door management ICT. Als de implicatie van de afwijking het informatiebeveiliging en/of privacy raakt moeten CISO en FG vooraf betrokken zijn.

BRON:
ICT Strategie | Principes – We werken vanuit architectuur principes (waaronder keuze voor geïntegreerde en gerationaliseerde oplossingen)

ICT Strategie | Van ambitie naar principes

ICT Strategie: Van ambitie naar principes, op weg naar digitale transformatie onderwijs en zorg

Informatietechnologie draagt bij aan het beste onderwijs en de beste zorg én maakt onderdeel uit van de waardenketens van Kentalis

Informatietechnologie wordt ingezet vanuit **focus** op de primaire processen, vanuit **expertise** op het gebied van digitalisering en **eenduidig** binnen de sectoren en over de organisatie

Paradigma-shift
De rol van Kentalis verschuift van "zorgen voor" naar "zorgen dat", de leerling ontwikkelt 21ste-eeuwse vaardigheden, de cliënt participeert

Communicatie steeds belangrijker
Formele en informele informatieoverdracht binnen de organisatie, met leerlingen, cliënten en hun wettelijk vertegenwoordigers en met ketenpartners is steeds belangrijker

Processen verder verbeteren
Technologie wordt steeds professioneler en breder toepasbaar: onderwijs- en zorg op afstand, apps, portalen, self service, sociale media, e-learning, eHealth etc. Druk op budgetten blijft bestaan.

Iedereen, overal en altijd
Alle leerlingen, cliënten en medewerkers moeten toegang hebben tot ICT. Plaats-, tijd- en apparaat-onafhankelijk. Veiligheid en betrouwbaarheid van data is essentieel. Schaalbaarheid is belangrijk.

Doelstellingen

- **Informatietechnologie is van toegevoegde waarde**
  Functioneel **meerwaarde** leverende ICT ondersteuning voor onderwijs- en zorgprocessen (e-learning, eHealth, zorgtechnologie, robotisering, ...)
- **Oplossingen zijn integraal**
  Verbeteren van **ketenondersteuning** en digitale **participatie** leerlingen/ cliënten
- **Informatietechnologie is doelmatig**
  Producten en diensten leveren **toegevoegde waarde** , **schaalbaarheid** en **flexibiliteit** worden vergroot, tegen **optimale kosten** en in relatie tot verbruik en **eenduidige** toepassing
- **We hebben een goed beheerste IT**
  Verhoging van het volwassenheidsniveau en voorspelbare kwaliteit en kosten
- **Informatietechnologie is compliant**
  Voldoet aan wet- & regelgeving en 'best practices'; data is veilig, integer en betrouwbaar

Uitgangspunten ("gedifferentieerd eenduidig")

- Informatietechnologie is onderdeel van de waardenketens van (en met) Kentalis, wordt ingezet om toegevoegde waarde te leveren voor leerling en cliënt
- Kentalis is onderscheidend op het gebied van onderwijs en zorg voor haar doelgroep
- Ondersteunende bedrijfsprocessen zijn niet onderscheidend
- Ook primaire processen kunnen in hoge mate volgens 'best practices' worden ingericht en ondersteund
  - We kiezen *product leadership* voor onderscheidende ICT
  - We kiezen *customer intimacy* voor onderscheidende processen
  - We kiezen voor *operational excellence* voor niet-onderscheidende processen
- Uitbesteden doen we waar dit verantwoord kan en vanuit een beheersbare situatie.

Principes

- Er moet altijd een **businesscase** zijn (batenmanagement)
- We werken vanuit **architectuur principes** (waaronder keuze voor geïntegreerde en gerationaliseerde oplossingen)
- De toepassing van informatietechnologie is '**diensten** georiënteerd', we nemen diensten af
- We richten in volgens '**best practices**' en **standaarden**
- Voor unieke diensten/processen maken we zoveel mogelijk gebruik van **bewezen** technologie en alleen maatwerk als dit echt onvermijdelijk is
- Voor voorwaardenscheppende ICT zetten we bewezen oplossingen eenduidig in (geen maatwerk of zelfbouw)
- **Platforms** (bijv. Microsoft) worden maximaal en optimaal benut
- **Veilig** is dé norm
- **Data**/-management is op orde (waaronder data-eigenaarschap, eenduidigheid, één bron, datakwaliteit)
- "Alleen **Cloud**"
  1. Software als een Service (SaaS)
  2. Platform als een Service (PaaS)
  3. Infrastructuur als en Service (IaaS)
- **Mobiel**, tenzij

Versie 24-2-2021 • Voor intern gebruik

Koninklijke Kentalis

Kentalis EA: Algemene Architectuurprincipes

- ALG01: Harmonisatie van bedrijfsprocessen
- ALG02: Per proces één eigenaar
- ALG03: Standaardisatie van werkwijzen en middelen
- ALG04: ICT innovatie door bewezen ICT
- ALG05: Betaal naar gebruik
- ALG06: Maximale ontkoppeling
- ALG07: Hergebruik boven kopen boven maken
- ALG08: Rol-gebaseerd werken
- ALG09: Data gedreven expertise center
- ALG10: De Kentalis primaire dienstverlening ingeval van disruptie adequaat hersteld

Harmonisatie van bedrijfsprocessen

Principe : Harmonisatie van bedrijfsprocessen

Nummer: ALG01

Harmoniseer bedrijfsprocessen binnen Kentalis: hergebruik soortgelijke werkwijzen.

Rationale

Harmoniseer de bedrijfsprocessen binnen Kentalis. Maak daarbij onderscheid in:

- Processen voor de primaire bedrijfsdomeinen Onderwijs, Zorg en Academie:
  - Deze zijn leidend en maken Kentalis uniek: maximale gerichtheid op passende processen en procesketens;
- Ondersteunende, generieke, processen:
  - zijn ondersteunend en niet uniek voor Kentalis: standaardiseer conform sector en/of industrie "*best practices*";
  - bijv. Personeel en Organisatie, Financiële administratie, ICT, Communicatie, Inkoop en voorraadbeheer, Kwaliteit, veiligheid, Arbo en Milieu, etc.

Implicaties

Zorg, Onderwijs en Academie zijn specifieke bedrijfsdomeinen binnen Kentalis met ieder hun specifieke merites, context en wetgeving.

Bron:

ICT Strategie |	*Uitgangspunten –*	*We kiezen customer intimacy voor onderscheidende processen*
			We kiezen voor operational excellence voor niet onderscheidende processen
		Doelstellingen –	*Oplossingen zijn integraal. Verbeteren van ketenondersteuning*

Per proces één eigenaar
Id: ALG02

Principe: Per proces één eigenaar

Nummer: ALG02

Elk bedrijfsproces heeft één eigenaar

Rationale

Elk bedrijfsproces binnen Kentalis heeft precies één eigenaar ("*Business Owner*").

Het eigenaarschap van bedrijfsprocessen en generiek ondersteunende processen binnen Kentalis is eenduidig belegd bij een rol.

Implicaties

Het eigenaarschap van alle bedrijfsprocessen en generieke processen moet binnen Kentalis belegd worden en blijven: dit vergt actief beheer van het Kentalis bedrijfsprocesmodel.

De eigenaar van een bedrijfsproces is eindverantwoordelijk voor dat proces:

- Voor het verloop van het proces, van begin tot eind;
- Voor een goede beschrijving;
- Voor een juiste uitvoering van dat proces;
- Bewaakt de kwaliteit van het proces;
- Signaleert inefficiënties of verspillingen en initieert verbeteringen;.
- Zorgt dat het proces voldoen aan interne richtlijnen en standaarden, en aan wet en regelgeving;
- Rapporteert over procesprestaties.

Standaardisatie van werkwijzen en middelen

Principe: Standaardisatie van werkwijzen en middelen

Nummer: ALG03

Gebruik standaarden en standaard werkwijzen

Gebruik middelen (business processen, ICT systemen) enkel waar deze middelen primair voor bedoeld zijn

Rationale

Gebruik branche modellen en standaarden (wanneer beschikbaar)

Gebruik de-facto standaarden: gebruik bewezen ('proven') industrie- en sector-standaarden; volg de markt.

Gebruik middelen enkel waar middelen primair voor bedoeld zijn: conformeer aan standaard gebruik van standaard middelen uit de markt of al binnen Kentalis ontwikkelde componenten.

Primaire diensten zijn Kentalis-specifiek; worden opgebouwd uit standaard verkrijgbare producten en diensten tenzij.

Ondersteunende diensten zijn niet Kentalis-specifiek; worden enkel opgebouwd uit standaard verkrijgbare producten en diensten.

Implicaties

Pas de Kentalis bedrijfsprocessen aan aan de applicaties (wijzig processen daar waar vereist voor een standaard gebruik van standaard in de markt beschikbare applicaties).

Geen oneigenlijk gebruik van processen en applicaties.

Geen maatwerk; geen modificaties, specifiek voor Kentalis.

- Alleen in uiterste noodzaak een applicatie aanpassen aan specifiek Kentalis gebruik, leg uit (uitzondering; Kentalis-specifieke aanpassing wordt onderdeel van *roadmap* leverancier)

Onze cliënten, leerlingen en patiënten zijn uniek, onze processen niet. (dit principe kan vooral gebruikt worden in het ondersteunende diensten domein)

Bron: ICT Strategie | Principe | We richten in volgens "best practices" en standaarden

Uitgangspunten - Ook primaire processen kunnen in hoge mate volgens "best practices" worden ingericht en ondersteund

ICT innovatie door bewezen ICT

Principe: ICT innovatie door bewezen ICT

Nummer: ALG04

Innoveer door gebruik van bewezen ('*proven*') ICT. Kentalis innoveert op vlak van ICT door de markt te volgen.

Rationale

Kentalis innoveert op het vlak van ICT door te volgen, door te kiezen voor bewezen ICT oplossingen, algemeen beschikbaar in de markt.

ICT oplossingen voor Kentalis zijn daarom opgebouwd uit standaard ICT bouwstenen en diensten, standaard beschikbaar in de markt.

Implicaties

Kentalis kiest niet voor de nieuwste technologie die zich nog moet bewijzen in de markt.

Kentalis kiest bij voorkeur niet voor niche oplossingen tenzij daarmee een bijzondere doelgroep bediend kan worden.

Bron:

ICT Strategie | Principes | Voor unieke diensten/processen maken we zoveel gebruik van bewezen technologie en alleen maatwerk als dit echt onvermijdelijk is.
Voor voorwaardenscheppende ICT zetten we bewezen oplossingen eenduidig in (geen maatwerk of zelfbouw)

Betaal naar gebruik van externe diensten

Principe: Betaal naar gebruik

Nummer: ALG05

"*Pay for usage*": betaal alleen voor gebruik van externe diensten, betaal naar rato van afgenomen externe dienst.

Kentalis streeft naar schaalbare oplossingen om kosteneffectief te kunnen opereren.

Rationale

Kentalis beweegt van langjarige investeringen naar betalen voor gebruik van diensten van externe leveranciers ("*Pay for usage*"):

- Een voordeel is het beter kunnen schalen van door Kentalis geboden dienstverlening naar de actuele vraag van dat moment
- Risico's van langjarige investeringen worden vermeden, kosten worden voorspelbaarder.

"*pay for usage*", het betalen van door Kentalis bij haar externe leveranciers afgenomen diensten in plaats van zelf diensten op te zetten en te exploiteren impliceert een verschuiving van kostensoort van *capex* naar *opex* (waarbij de *opex*-kosten naar rato van afgenomen diensten zijn). Dit vraagt een verandering van budget naar *chargeback.* Bij een wisselende vraag (zorg: een continue wisselende vraag; onderwijs: een jaarlijks wisselende vraag) draagt dit bij aan een voorspelbare, kosten-efficiënte dienstverlening.

Implicaties

De directe afhankelijkheid van externe leveranciers wordt groter.

Leveranciers moeten aangeboden diensten aanbieden volgens "*pay for usage*".

Kentalis moet scherp op gebruik sturen. Het niet continue bewaken van daadwerkelijk gebruik van diensten impliceert financiële risico's. Kentalis moet periodiek de TCO evalueren en goed SLM uitvoeren.

(dit principe zegt enkel iets over extern afgenomen diensten; niet: intern afgenomen diensten, niet: door Kentalis geleverde diensten)

Bron:

ICT Strategie | Principes - De toepassing van informatietechnologie is "diensten georiënteerd", we nemen diensten af

Maximale ontkoppeling, standaard koppelvlakken

Principe: Maximale ontkoppeling

Nummer: ALG06

Zorg voor maximale ontkoppeling van systemen en systeemcomponenten. Gebruik standaard koppelingen waar gekoppeld moet worden, gebruik anders de ESB.

Rationale

Ontkoppeling van systemen en systeemcomponenten (diensten, processen, applicaties, ICT-infrastructuur) biedt meer flexibiliteit en schaalbaarheid, complexiteitsreductie, lagere kosten van onderhoud en beheer en voorkomt vendor lock inn. Componenten kunnen gemakkelijker uit de Cloud gehaald worden.

De onderdelen van een systeem, maar ook de systemen onderling, zijn minimaal aan elkaar gekoppeld en hebben elk een maximale interne samenhang. Dat leidt tot autonome systeemcomponenten en systemen die niet afhankelijk zijn van de interne inrichting van andere systemen. Daar waar gekoppeld moet worden, worden standaard koppelingen en koppelvlakken gebruikt. De systeemcomponenten en systemen wisselen asynchroon berichten uit op basis van gestandaardiseerde communicatieprotocollen.

Maximale ontkoppeling maakt het mogelijk systeemcomponenten en systemen los van elkaar in onderhoud te nemen of te vervangen zonder dat het functioneren van het geheel wordt verstoord.

Implicaties

Applicaties worden veelal uit de markt gehaald of afgenomen (SaaS) waarbij de applicatie-architectuur door de leverancier bepaald wordt.

Streven naar maximale ontkoppeling vereist een goed overzicht van het ICT landschap (incl. alle koppelvlakken en toegepaste *security controls*); één applicatie integratie-platform dat integreert middels standaard (communicatie)protocollen en API's (interoperabiliteit).

Het vereist daarnaast een sterk leveranciersmanagement (multi-leverancierscontracten; ingerichte incident, probleem en verander-processen met leveranciers).

Hergebruik boven kopen boven maken

Principe: Hergebruik boven kopen boven maken

Nummer: ALG07

Kentalis kiest voor hergebruik van bestaande producten/diensten boven het kopen ervan.

Kopen gaat boven het zelf (laten) maken van een product/dienst.

Rationale

Kentalis hanteert het principe van hergebruik van reeds aanwezige oplossingen of afgenomen diensten om het aantal verschillende oplossingen/diensten te beperken en wildgroei te voorkomen.

Ingeval een nieuwe ICT-oplossing nodig blijkt wordt eerst gekeken naar aangeboden volwassen en volledige producten/diensten die gekocht kunnen worden. Pas als dit niet mogelijk blijkt wordt bouw overwogen.

Implicaties

Hergebruik van een al aanwezige oplossing betekent vaak dat deze niet maximaal aan alle eisen en wensen voldoet, maar wel meteen beschikbaar is, tegen lage kosten (*opex/capex*) en al ingeregeld beheer. Hergebruik gaat hier boven maximale fit.

Eenzelfde overweging geldt voor de afweging kopen versus bouwen.

Bron:

ICT Strategie | Principes - Voor unieke diensten/processen maken wij gebruik van bewezen technologie en alleen maatwerk als dit echt onvermijdelijk is.

Rol-gebaseerd werken

Principe: Rol-gebaseerd werken

Nummer: ALG08

Binnen Kentalis werken we rol-gebaseerd.

Rationale

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 op individueel niveau te worden toegekend, waardoor autorisatiebeheer efficiënter en kan plaats vinden. Hierdoor is de organisatie ook beter in staat om de rechtmatigheid van uitgegeven autorisaties te controleren.

Toegang tot informatie is gebaseerd op 'need-to-know'. Rolbeschrijvingen omvatten daarom richtlijnen en kaders welke rol welke types data mag inzien of bewerken (bewerken: creëren, wijzigen, verwijderen).

Implicaties

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. Provisioning van accounts naar doelsystemen leidt niet automatisch tot toegang tot een systeem; hiertoe moet additioneel nog een autorisatie worden toegekend op basis van een rol.

Dit vereist vastlegging van rollen en verantwoordelijkheden, bovendien een mapping van functies op rollen.

Bron:

ICT Strategie | Principes – Veilig is de norm.

Data gedreven expertise center

Principe: Data gedreven expertise center

Nummer: ALG09

Kentalis gebruikt data om haar expertise verder te ontwikkelen.

Rationale

Evidence based of *informed based* werken is gebaseerd op feiten die door middel van data worden vastgelegd. Op basis van data kunnen al dan niet met toepassing van geavanceerde analyse technieken en AI operationele processen ondersteund worden bij diagnostiek en behandeling.
Data analyse levert bovendien een bijdrage aan het ontwikkelen van nieuwe methoden. De beschikking over omvangrijk basismateriaal is randvoorwaardelijk.

Implicaties

Kentalis stelt voor alle data vast of deze uitsluitend een operationeel belang heeft of dat de data tevens van belang kan zijn voor ontwikkeling van expertise. Binnen de kaders van wet- en regelgeving worden deze gegevens bewaard op een wijze die geschikt is voor toepassing van data-analyse.

Dit principe onderscheidt zich van het principe “Analyse en rapportage over meerdere gebieden via Kentalis informatieplatform“ waar data analyse bedoeld is ten behoeve van rapportages voor besturing van de organisatie.

Bron:
ICT Strategie | Principes – Veilig is de norm.

Principe: BC

Nummer: ALG10

De Kentalis primaire dienstverlening wordt zo opgezet dat deze ingeval van een disruptie tijdig, adequaat en voldoende hersteld kan worden.

Rationale

Alle door Kentalis verleende diensten aan haar clienten en leerlingen worden getoetst op eisen t.a.v. beschikbaarheid en continuiteit. Business continuity eisen worden vastgesteld waarin het geheel van bedrijfsprocessen, en ondersteunende processen en diensten (als bijv. facilitair, ICT, centrale admin etc.) moet voorzien.

Per geboden dienst zullen andere eisen gelden voor mate en snelheid van herstel van primaire dienstverlening en daarmee in maatregelen voorzien moet worden (extra voorzieningen, procedures, redundantie, communicatie, ..).

Implicaties

Dit vraagt per primaire dienst een wederkerende BIV / BC analyse over alle aspecten ervan: processen en organisatie, informatievoorziening, ICT(-redundantie), informatieveiligheid. Ook vraagt dit om een goede en gedeelde uiteenzetting van wat de primaire dienstverlening precies inhoudt. Wat verstaan we hier onder, welke onderdelen betreft dit, welke diensten zijn hieraan gekoppeld etc. om vervolgens aan te geven hoe de continuïteit van deze specifieke diensten is geborgd.

Bron:

2025 aandacht voor business continuity

Kentalis EA: Informatie Architectuurprincipes

- INF01: Elk dataobject heeft één bronsysteem
- INF02: Analyse en rapportage via Kentalis informatieplatform
- INF03: Correcte vastlegging van inkomende gegevens
- INF04: Data heeft waarde
- INF05: Elk data object heeft één eigenaar
- INF06: Data is direct benaderbaar aan de bron
- INF07: Data is veilig / alle data is geclassificeerd

Elk dataobject heeft één bronsysteem

Principe; elk dataobject heeft één bronsysteem

Nummer: INF01

Data wordt eenmalig opgeslagen binnen Kentalis in het betreffende bronsysteem, de applicatie waartoe de specifieke data behoort.

Rationale

Elk dataobject behoort tot één bronsysteem, wordt eenduidig opgeslagen in het bronsysteem waartoe die data behoort. Mutaties vinden plaats in dit bronsysteem.

Elk dataobject heeft ook één vindplaats: het betreffende bronsysteem.

Datakwaliteit wordt primair in het betreffende bronsysteem geborgd.

Implicaties

Data enkel bij de bron halen, niet bij ander systeem wat zelf de data bij de betreffende bron heeft opgehaald.

Ingekochte standaardapplicaties of SaaS-diensten hebben hun eigen gebruik van data, hun eigen datamodel. Deze applicaties moeten ingepast worden in het geheel aan Kentalis systemen. Daarbij zullen redundante dataopslag en data-uitwisseling en -vertaling tussen applicaties deels onvermijdelijk zijn. Dan geldt wel: “leg uit”.

Datamanagement moet dan borgen dat data overeen blijft stemmen tussen systemen.

Voorbeeld: van een server wordt de financiële data (attributen, bijv. aankoopprijs, economische levensduur) vastgelegd in het inkoopsysteem, onderdeel van ERP; de configuratiegegevens (bijv. storage capaciteit, technische levensduur, periode gedurende welke standaard en evt. “extended” support geleverd wordt, wie te contacteren bij een storing) worden vastgelegd in de CMDB.

Bron:
ICT Strategie – Principes -Data/-management is op orde (één bron)

Analyse en rapportage via Kentalis informatieplatform

Principe; Analyse en rapportage over meerdere gebieden via Kentalis informatieplatform

Nummer: INF02

Analyse en rapportage over afgeleide en geïntegreerde gegevens vindt plaats vanuit het Kentalis informatieplatform.

Rationale

Het Kentalis Informatieplatform heeft de functionaliteit van gegevensverzameling en -integratie (datawarehouse) en gegevensuitlevering (datamart voor analyse en rapportages voor specifieke doelgroepen).

Afgeleide gegevens zijn niet aanwezig in het bronsysteem maar (indien aanwezig) wel in het datawarehouse. Het datawarehouse en de datamarts zijn geoptimaliseerd voor verwerking en presentatie van data.

Daar waar een primair/bronsysteem WEL de rapportages kan bieden ter ondersteuning van de operationele bedrijfsvoering, deze gebruiken. Daar waar een bronsysteem tekort schiet wordt via de Kentalis standaard rapportage tools gerapporteerd.

Implicatie

Analyse en rapportage van afgeleide gegevens vindt enkel plaats vanuit een datamart en niet direct vanuit het datawarehouse. Een datamart gebruikt een gegevensstructuur die is geoptimaliseerd voor bevragingen (dimensioneel model).

Een datamart kan met een voorgedefinieerd toegangspad (met geselecteerde tools) benaderd worden.

Bron:
ICT Strategie – Principes -Data/-management is op orde (één bron)

Correcte vastlegging van inkomende gegevens

Principe: Correcte vastlegging van inkomende gegevens

Nummer: INF03

Inkomende, gemuteerde of gegenereerde gegevens worden direct correct vastgelegd.

Rationale

Bij Kentalis binnenkomende gegevens (data) en mutaties daarop worden direct vastgelegd, in het bijbehorende systeem (bronsysteem). Dit geldt ook voor binnen Kentalis gegenereerde data, bijvoorbeeld meetgegevens of analyse data.

Inkomende data wordt eenmalig vastgelegd en/of gemuteerd. Dat gebeurt bovendien in het bronsysteem/applicatie. Data wordt alleen gedeeld met andere applicaties binnen Kentalis waar vereist. De applicatie voert maximale controle uit op de correctheid van de inkomende data.

Implicaties

Per informatie entiteit moet één bronsysteem zijn vastgesteld, dit is in een apart principe vastgelegd.

Dit vereist een structuur van vastlegging van data en omgang met data. Actief datamanagement moet dit borgen

Afhankelijk van mutatiegraad richt je het proces van wijzigen/updaten in; bepaal je hoe de data wordt aangepast in andere systemen waar data als afgeleide data opgeslagen wordt. Handmatige vastlegging van inkomende gegevens vermijden.

De kwaliteit van de (ingekomen) data moet periodiek gemeten worden; dit is een verantwoordelijkheid van de data eigenaar.

Bron:
ICT Strategie – Principes - Data/-management is op orde (eenduidigheid)

Data heeft economische waarde

Principe: Data heeft waarde
Nummer: INF04
Kentalis gaat met data om als economische waarde.

Rationale
Data heeft economische waarde. Kentalis gaat met data om als een economisch waardevol bezit.

Data heeft waarde:
- Economische waarde

Implicaties
Ga met data om als een asset. Kentalis voert actief datamanagement over haar data.
Kentalis neemt de verrijking van data over verschillende bronnen in eigen hand, met een eigen datawarehouse.
Kentalis beschermt de data tegen ongeoorloofde gebruik of manipulatie, tegen verlies of diefstal.
Historische data moet beschikbaar zijn indien leverancier dit niet kan faciliteren moet Kentalis dit verzorgen.
Kentalis gebruikt data ook voor eigen onderzoek (Kentalis Academie).

Bron:
ICT Strategie – Principes - Data/-management is op orde (datakwaliteit)

Elk data object heeft één eigenaar

Principe: Elk data object heeft één eigenaar
Nummer: INF05
Elk data object of gegevensentiteit heeft één business eigenaar binnen Kentalis.

Rationale
Elk data object of gegevensentiteit heeft een business eigenaar ("*Business Owner*") binnen Kentalis die verantwoordelijk is voor de kwaliteit ervan, het beheer en de bescherming tegen ongeoorloofd gebruik, diefstal of manipulatie.

Implicaties
In de praktijk zal dit principe gecombineerd met het principe "elke data heeft één bronsysteem" leiden tot een business eigenaar die zowel verantwoordelijk is voor een applicatie (een "bronsysteem") als de daarbij behorende data ("brondata").
Actief datamanagement moet toepassing van dit principe borgen binnen Kentalis (niet alleen datamanagement maar vooral ook datamanagement).

Bron:
ICT Strategie | Principes | Data/-management is op orde (data eigenaarschap)

Data is direct benaderbaar aan de bron

Principe: Data is direct benaderbaar aan de bron

Nummer: INF06

Data behorende bij een (bron)applicatie is direct benaderbaar voor gebruik elders binnen Kentalis.

Rationale

Data moet toegankelijk zijn (leesrecht) voor gebruik binnen Kentalis. De bronapplicatie moet in (bulk-) ontsluiting van data kunnen voorzien.

Kentalis streeft naar gebruik van SaaS geleverd door Cloud applicatieproviders. Voor Kentalis van essentieel belang is het veilig kunnen borgen van data ingeval de betreffende SaaS-dienst wegvalt, bijv. door een calamiteit bij de provider, faillissement van provider of een dispuut met provider.

Implicaties

Dit stelt eisen aan selectie, inrichting en gebruik van applicaties voor wat betreft data (inclusief datarelaties), data-ontsluiting en eventueel daarbij behorende business rules. Data-ontsluiting vindt plaats via een data-ontkoppelpunt, een goed gedefinieerde interface (API).

Ingeval van wegvallen van de SaaS-dienst moet de data en eventuele business rules beschikbaar blijven voor Kentalis. Dat vereist concrete acties als bijvoorbeeld een frequente back-up van data, waarbij na restore gebruik van data mogelijk is zonder beschikbaarheid van de betreffende SaaS-dienst.

Kentalis heeft een wettelijke bewaarplicht voor data, deze verschilt per type data. In alle geval moet Kentalis borgen dat data beschikbaar blijft gedurende deze periode ongeacht wijzigingen van het betreffende bronsysteem, een SaaS-dienst, of het wegvallen van of wisselen van SaaS-provider.

Na de wettelijke bewaarplicht moet Kentalis de vastgelegde data verwijderen.

Data is veilig / alle data is geclassificeerd

Principe: Data is veilig

Nummer: INF07

Data van Kentalis moet veilig zijn en geclassificeerd.

Rationale

Wij beveiligen niet alleen de fileserver maar ook de Word documenten, etc. .
Alle data moet geclassificeerd zijn en voorzien van een retentietermijn en vertrouwelijkheidsniveau.
Dit wordt ook afgedwongen door wetgeving (AVG, NEN7510, etc.)

Implicaties

De classificatie van een data type bepaalt de te nemen maatregelen voor beveiliging ervan.
Daarvoor is een data classificatie en data retentie datamanager een vereiste.
Kentalis gaat uit van “zero trust” / “least privilege” en RBAC als het gaat om toegang tot data.

Bron:
ICT Strategie – Principes - Veilig is dé norm

Kentalis EA: Applicatie Architectuurprincipes

- APP01: Per geboden functionaliteit één applicatie
- APP02: Suite in plaats van producten
- APP03: Per applicatie één eigenaar
- APP04: Scheiding presentatie en gegevensverwerking
- APP05: Maximale applicatie-ontkoppeling
- APP06: Applicaties koppelen via het standaard applicatie-integratieplatform
- APP07: Een applicatie koppelt haar brondata direct naar een externe partij
- APP08: Er is geen voorkeur voor Open Source of Propriety software

Per geboden functionaliteit één applicatie

Principe : Per geboden functionaliteit één applicatie

Nummer: APP01

Een applicatie-functionaliteit wordt geboden door één applicatie.

Rationale

Harmoniseer bedrijfsapplicaties en generieke applicaties binnen Kentalis:

- Een gevraagde applicatie functionaliteit wordt door één applicatie geleverd, binnen een sector of domein en over sectoren/domeinen
- Geldt voor specifieke bedrijfsapplicaties als *(bijv. ECD, USER; geldt ook voor generieke, algemeen ondersteunende, applicaties als bijv. Microsoft Teams of Topdesk)*
- Daar waar bedrijfsprocessen (en daarmee gevraagde ondersteunende applicatiefunctionaliteit, gedifferentieerd zijn *(bijv. zorg: audiologische, extramurale, intramurale zorg)* blijft het gemeenschappelijke deel ondersteund door één applicatie (of eventueel een aparte instantie van dezelfde applicatie: dan wel “leg uit”)

Het doel is een integraal applicatielandschap met minimale overlap qua functionaliteit tussen applicaties.

Dit principe heeft sterke verwantschap met: harmonisatie van bedrijfsprocessen: ondersteun eenzelfde soort bedrijfsprocessen door dezelfde applicatie.

Implicaties

Waar mogelijk integraal voor geheel Kentalis, anders integraal per domein: gestreefd wordt dan naar, in ieder geval per bedrijfsdomein, een integraal applicatielandschap.

Suite in plaats van losse producten

Principe: Suite i.p.v. losse producten
Nummer: APP02
Applicatie integratie gaat voor functionaliteit

Rationale
Ingeval van te maken keuzes gaat een goede applicatie-integratie voor volledige applicatie-functionaliteit.
Dit geldt voor bedrijfsapplicaties, maar zeker ook voor generieke (Kentalis-breed ondersteunende) applicaties.

Kentalis vindt het naast functionaliteit vooral belangrijk dat applicaties passen in het Kentalis applicatielandschap:
- Goed op elkaar aansluiten v.w.b. functionaliteit en datagebruik
- Met zo min mogelijk overlap qua functionaliteit
- Eenduidigheid vanuit eindgebruikers perspectief
- Met de juiste applicatiefunctionaliteit om de gebruikers kosteneffectief te bedienen

Kentalis kiest bij te maken keuzes niet perse voor die applicatie die de meeste functionaliteit biedt, maar de applicatie die het beste past in het Kentalis ICT-landschap.
Dit is vooral van belang voor de ondersteunende bedrijfsapplicaties en generieke applicaties.

Implicaties
Volledige (volledig passende) functionaliteit is vooral van belang voor Kentalis primaire bedrijfsapplicaties. Dit heeft soms consequenties voor integratie binnen het Kentalis applicatielandschap en met koppelingen naar derde partijen.

Bron:
ICT Strategie | Principes | Platforms(bijv. Microsoft) worden maximaal en optimaal benut

Per applicatie één eigenaar

Principe: Per applicatie één eigenaar

Nummer: APP03

Elke applicatie heeft één eigenaar

Rationale

Elke applicatie binnen Kentalis heeft een eigenaar ("*Business Owner*") binnen Kentalis.

Het eigenaarschap van bedrijfsapplicaties en ook generieke applicaties binnen Kentalis is eenduidig belegd bij een rol:

- Zorgen dat de applicatie werkt zoals bedoeld, op basis van de behoeften van de eindgebruikers;
- Bepalen wie toegang heeft tot de applicatie en toezien op correct gebruik;
- Levenscyclusbeheer;
- Kostenbewaking;
- Bewaken van de kwaliteit en continuïteit;

Implicaties

Het functioneel eigenaarschap van alle bedrijfsapplicaties en generieke applicaties moet binnen Kentalis belegd worden en blijven: dit vergt actief beheer van het applicatielandschap.

Dit principe heeft sterke verwantschap met het principe "elk data object heeft één eigenaar".

Scheiding presentatie en gegevensverwerking

Principe: Scheiding van presentatie en gegevensverwerking

Nummer: APP04

Alleen presentatie van data en functionaliteit op de apparaten van eindgebruikers. Bedrijfsdata blijft in de backend.

Rationale

De browser of de app is de cliënt: maximale variatie in ondersteunde apparaten van eindgebruikers met minimale variatie in de gebruikte techniek en componenten. Web- en app-*based* ontsluiten van functionaliteit en data is de exit strategie voor complexe, dure desktop virtualisatieoplossingen.

Bedrijfsdata en applicatiefunctionaliteit is veilig in de backend datacenter of cloud, dit zijn gecontroleerde omgevingen.

Applicatiefunctionaliteit wordt zodanig aangeboden dat de bedrijfsdata niet op het end-device achterblijft of anderszins toegankelijk is voor gebruik buiten de daarvoor bedoelde applicatie.

Maakt het gemakkelijker om applicatiefunctionaliteit toegankelijk te maken ongeacht het type apparaat van een eindgebruiker.

Implicaties

Stelt eisen aan de wijze van ontsluiten van applicatiefunctionaliteit via een toestel van een eindgebruiker.

Applicaties koppelen via het standaard applicatie-integratieplatform

Principe: Applicaties koppelen bij voorkeur via standaard beschikbare koppeling en anders via de ESB.

Nummer: APP06

Kentalis applicaties koppelen via het Kentalis applicatie-integratieplatform (ESB) of via standaard beschikbare koppeling

Rationale

Alle Kentalis applicaties, zowel on-premise als SaaS-applicaties, koppelen op standaard wijze via het Kentalis applicatie-integratieplatform: de Kentalis Enterprise Service Bus (ESB). Dat leidt tot autonome applicatiekoppelvlakken die niet afhankelijk zijn van, wijzigingen aan, koppelvlakken van andere applicaties.

Daar waar tussen twee Kentalis applicaties al standaard koppelingen aanwezig zijn (standaard aangeboden worden door de applicatieleveranciers) wordt per koppeling beslist of deze gebruikt kan worden (voorkeur) of toch via het integratieplatform gekoppeld moet worden. Overwegingen daarbij zijn: extra data-vertaling vereist, mogelijkheid van hergebruik van uitgewisselde data voor andere toepassing/koppeling, kosten van realisatie.

Indien een koppeling hoe dan ook maatwerk vereist wordt gekoppeld via de ESB.

Implicaties

Gebruik van een ESB vereist een betrouwbaar en veelzijdig applicatie-integratieplatform wat eenvoudig en flexibel kan koppelen met applicaties en daartoe alle gangbare applicatiekoppelmechanismes standaard ondersteunt.

Een SaaS-applicatie koppelt brondata direct naar externe partij

Principe: Een SaaS-applicatie koppelt voor haar brondata direct aan een externe partij, ingeval van een standaard koppeling .

Nummer: APP07

Een Kentalis applicatie koppelt direct naar een externe partij voor uitwisseling van data voor zover het brondata is en voor zover een standaard uitwisseling van brondata aan een externe partij standaard onderdeel is van de SaaS-dienst.

Rationale

Een Kentalis (SaaS)applicatie die uitwisseling van data met een externe partij als standaard onderdeel van haar core functionaliteit heeft; daarvoor ook een standaard applicatiekoppeling met die externe partij heeft; en als enige Kentalis applicatie met die partij data uitwisselt, koppelt direct.

Implicaties

Het Kentalis applicatie-integratieplatform kan deze koppeling niet monitoren en loggen. Dit vereist aanvullende mitigerende maatregelen hiervoor.

Er is geen voorkeur voor open source of propriety software

Principe: Er is geen voorkeur voor open source of propriety software.
Nummer: APP08

Zolang aan de eisen van Kentalis voldaan wordt staat Kentalis neutraal tegenover de keuze voor Open

Rationale

De functionele en nonfunctionele eigenschappen en de overige eisen die aan het gebruik en het beheer van een applicatie gesteld worden zijn doorslaggevend voor de toepassing binnen Kentalis. Hierbij is het irrelevant of het Open Source betreft.

Implicaties

In geval van open source moet extra aandacht besteed worden aan het borgen van de support.

DRAFT

Kentalis EA: AI Architectuurprincipes

- AI01: Gebruik alleen door Kentalis goedgekeurde AI-applicaties
- AI02: Geef gebruik van AI expliciet aan
- AI03: Valideer door AI gegenereerde output
- AI04: Gebruik AI conform (inter)nationale wet- en regelgeving
- AI05: AI-oplossingen zijn modulair en flexibel

Gebruik alleen door Kentalis goedgekeurde AI-applicaties

Principe: Gebruik persoonsgegevens en bedrijfsgevoelige gegevens alleen in door Kentalis goedgekeurde AI apllicaties
Nummer: AI01

Gebruik persoonsgegevens en bedrijfsgevoelige informatie alleen in door Kentalis goedgekeurde AI-applicaties

Rationale

Bij niet expliciet door Kentalis goedgekeurde AI toepassingen is het ons niet bekend of de veiligheid en privacy gewaarborgd is. Dit is wel een ethisch vereiste vanuit Kentalis en wordt ook afgedwongen door wetgeving (AI act en AVG).

Implicaties

Kentalis maakt een risico inschatting bij de intake van AI applicaties. Slechts expliciet hiervoor goedgekeurde AI applicaties mogen gebruikt worden voor het verwerken van persoonsgegevens of anderszins vertrouwelijke gegevens.

Geef gebruik van AI expliciet aan

Principe: Geef gebruik van AI expliciet aan

Nummer: AI02

Geef expliciet aan wanneer AI gebruikt wordt ter ondersteuning van medewerkers

Rationale

Dit is het transparantieprincipe uit de AI act.

Implicaties

Het moet voor de eindgebruiker (client, patient, medewerker, leerling, ouder.....) altijd duidelijk zijn of hij/zij met een mens of een machine interacteert. Bijvoorbeeld bij telefoongesprekken of bij een chatbot mag een medewerker niet ten onrechte denken dat hij met een mens communiceert terwijl dat niet zo is.

Valideer door AI gegenereerde output

DRAFT

Principe: Valideer door AI gegenereerde output

Nummer: AI03

Valideer alle met AI gegenereerde output, zoals bijvoorbeeld teksten en beelden, voor vrijgave of verder gebruik.

Rationale

Vertrouw output dat gegenereerd wordt met behulp van AI nooit zonder validatie, zonder zelf na te denken over de juistheid ervan. Elke medewerker is zelf verantwoordelijk voor de juistheid van de informatie. Kan men de juistheid niet zelf controleren, of laten controleren door een expert, dan mag men de output niet gebruiken. Wees alert op eventuele informatie die door AI is “verzonnen” (hallucinaties).

Explainable AI (XAI) technieken maken beslisregels van een AI transparant. Een professional kan de uitkomst en het proces om tot die uitkomst te komen inzien en controleren.

Implicaties

Gebruik van AI vereist de nodige waarborgen voor juist gebruik van ingevoerde gegevens, en controle van alle door AI gegenereerde teksten en beelden.
AI-systemen moeten transparant en uitlegbaar zijn zodat eindgebruikers de uitkomsten begrijpen en kunnen vertrouwen. Gerbuik maximaal bronvermeldingen, dit verhoogt de betrouwbaarheid.
Klakkeloos gebruik van AI output kan ernstige en ongewenste gevolgen hebben.
Bij gebruik van AI moet de eindverantwoordelijkheid voor een besluit altijd bij de medewerker liggen; dit vereist duidelijke afspraken over welke verantwoordelijkheid bij welke partij ligt en welke processtappen bij een fout genomen worden.

Gebruik AI conform (inter)nationale wet- en regelgeving

DRAFT

Principe: Gebruik AI conform (inter)nationale wet- en regelgeving

Nummer: AI04

Gebruik AI en door AI gegenereerde output conform de (inter)nationale wetgeving en regelgeving.

Rationale

Gebruik AI altijd in overeenstemming met geldende wet- en regelgeving.
Denk hierbij aan o.a. :

- AVG: Algemene Verordening Gegevensbescherming;
- MDR: Medical Device Regulation;
- EHDS: European Health Data Space;
- EU AI Act: European Artificial Intelligence Act.

Bijv. de MDR stelt dat software, en dus ook AI, in de zorg alleen gebruikt mag worden nadat de veiligheid en effectiviteit van de toepassing ervan uitgebreid is getest en bewezen.
Dit geldt ook als AI alleen gebruikt wordt als hulpmiddel voor jezelf bij je werk als zorgverlener.

Implicaties

Let op eventueel vereiste certificeringen van toegepaste AI-diensten en zgn. AI-clients (chatbot apps).
Houdt de actuele wet- en regelgeving voor AI bij. AI, en dan met name AI-LLM, is een vakgebied dat sterk in ontwikkeling is. (inter)nationale wet- en regelgeving zal meer dan gemiddeld onderhevig zijn aan wijzigingen en aanpassingen.
Gebruik van AI vraagt een minimale geletterdheid in AI van alle gebruikers, bijvoorbeeld door training en/of een toets.

AI-oplossingen zijn modulair en flexibel

Principe: AI-oplossingen zijn modulair en flexibel

Nummer: AI05

AI-oplossingen moeten modulair en flexibel zijn om te kunnen functioneren in een omgeving met meerdere, onafhankelijke AI-toepassingen.

Rationale

Gezien de huidige beperkingen in ICT-koppelingen en API-standaarden, is het onwaarschijnlijk dat een enkele, geïntegreerde AI-toepassing toegang heeft tot verschillende gegevensbronnen zonder complexe en foutgevoelige authenticatie- en autorisatieprocessen. Door AI-oplossingen modulair en flexibel te ontwerpen en in te richten kan Kentalis specifieke AI-oplossingen inzetten voor verschillende toepassingen zonder afhankelijk te zijn van een enkele en allesomvattende AI-oplossing: inzet (en ontwikkeling) van AI-oplossingen specifiek voor bepaalde applicaties en/of gegevensbronnen. In feite zorgt dit architectuur principe er voor dat wij flexibel kunnen zijn met AI-inzet.
Een voorbeeld: de AI-bot van Copilot kan niet worden ingezet in de Zenya-omgeving. Er zijn momenteel (nog) geen standaarden waarbij de ene AI-tool ingezet kan worden in een andere omgeving (waarin je alleen geauthentiseerd in kunt komen); vgl. met een API; er zijn geen AI-API's-standaarden.

Biedt de mogelijkheid om snel te reageren op veranderingen en nieuwe eisen door de modulaire opzet.
Biedt vermindering van complexiteit, beheer en onderhoud(kosten) door het vermijden van ingewikkelde authenticatie- en autorisatie processen over omgevingen en systemen heen.

Implicaties

Risico's omtrent information disclosure nemen toe.
Voor een ' groeps-AI agent " die andere AI agents bevraagt gelden dezelfde regels als voor AI-agents.

Kentalis EA: IT Infrastructuur & Cloud Architectuurprincipes

- INFRA01: SaaS boven PaaS boven IaaS
- INFRA02: Flexibiliteit en schaalbaarheid
- INFRA03: Mobiel tenzij

SaaS boven PaaS boven IaaS

Principe: SaaS boven PaaS boven IaaS

Nummer: INFRA01

Alle ICT services gaan naar de cloud, waarbij SaaS het uitgangspunt is.

Rationale

Kentalis wil toekomstige ICT-oplossingen afnemen als diensten uit de cloud. Bij selectie daarvan heeft SaaS de sterke voorkeur: de oplossing kan daadwerkelijk in zijn geheel als dienst worden afgenomen. Eerst als SaaS niet mogelijk blijkt, bijvoorbeeld niet wordt aangeboden, worden PaaS respectievelijk IaaS overwogen.

Implicaties

Toekomstige ICT-oplossingen worden geselecteerd op basis van het beschikbaar zijn als SaaS, eventueel PaaS of IaaS.
Daarnaast moet de ICT-oplossing passen binnen de Kentalis *policies* voor authenticatie, autorisatie, dataopslag.
Migratie van bestaande Kentalis on-premise oplossingen geschiedt met ditzelfde uitgangspunt.

Bron:
ICT Strategie | Uitgangspunten | Uitbesteden doen we waar dit verantwoordelijk kan en vanuit een beheersbare situatie.
Principes | "Alleen Cloud"

Flexibiliteit en schaalbaarheid

Principe: Flexibiliteit en schaalbaarheid

Nummer: INFRA02

ICT infrastructuur oplossingen zijn flexibel en schaalbaar.

Rationale

Flexibiliteit: het snel kunnen inspelen op verzoeken vanuit onderwijs, zorg en/of de academie.
ICT infrastructuur oplossingen zijn gemakkelijk aan te passen aan veranderende vraag en aan een (al dan niet frequent) wisselende vraag door:

- verzoeken vanuit de academie, onderwijs en/of zorg om nieuwe diensten *(bijv. digitaal onderwijs, wonen);*
- toepassing van nieuwe technologie voor bestaande diensten *(bijv. opslag en beheer van documenten);*
- toepassing van nieuwe technologie voor nieuwe diensten *(bijv. domotica).*

Schaalbaar: het snel kunnen aanpassen van geboden ICT infrastructuur capaciteit aan een veranderende vraag, opdat maximale kostenefficiëntie wordt bereikt.

Implicaties

Het flexibel en schaalbaar maken en houden van de ICT-infrastructuur stelt eisen aan inrichting en beheer, bijv.

- het verregaand standaardiseren van ICT-oplossingen, met standaard koppelvlakken *("industry best practises")*
- het continue actief monitoren van huidig gebruik en anticiperen op verwacht gebruik

Bron:
ICT Strategie | Doelstelling | Informatietechnologie is doelmatig Producten en diensten leveren toegevoegde waarde, schaalbaarheid en flexibiliteit worden vergroot, tegen optimale kosten en in relatie tot verbruik en eenduidige toepassing

Mobiel tenzij

Principe: Mobiel tenzij

Nummer: INFRA03

Applicatiefunctionaliteit aanbieden aan eindgebruikers op “plaats-, tijd- en apparaat-onafhankelijk.”

Rationale

De eindgebruiker in elke situatie de op dat moment gewenste applicatie functionaliteit aanbieden, *“any place, any time, any device*”.

Eindgebruikers krijgen de dienstverlening die ze nodig hebben voor het uitoefenen van hun rol, toegang tot de juiste applicatiefunctionaliteit en de juiste data *(“Need to Know”)*

Implicaties

Applicaties functionaliteit van aanbieders kunnen afnemen op verschillende manieren (verschillende apparaten) en toegespitst op Kentalis business rollen (Persona’s).

Bron:
ICT Strategie | Principe | Mobiel, tenzij.

Kentalis EA: Security Architectuurprincipes

- SEC01: Veilig omgaan met gegevens
- SEC02: Toegang tot gegevens op basis van rol
- SEC03: Security by design
- SEC04: Beveiligingsmaatregelen in verhouding tot risico's
- SEC05: De eigenaar van data bepaalt het beveiligingsniveau
- SEC06: Toegang en gebruik van data is auditable
- SEC07: Toegang tot elke applicatie verleend door SSO

Veilig omgaan met gegevens

Principe: Veilig omgaan met gegevens

Nummer: SEC01

De Kentalis medewerker gaat veilig om met gegevens (je kunt veilig werken of je werkt niet).

Voorwaardenscheppend voor veilig werken is rol-gebaseerde omgang met data en toepassingen.

Rationale

Kentalis wil veilig omgaan met gegevens van haar cliënten, leerlingen en medewerkers.

Kentalis moet zich daarnaast houden aan de wet- en regelgeving t.a.v. het gebruik en verwerken van deze gegevens.

Need to know, Least privilege, zero trust en audittrail zijn uitgangspunten: Gegevens zijn toegankelijk enkel voor zover verifieerbaar nodig voor de uitoefening van een rol.

Implicaties

De Kentalis dagelijkse wijze van werken vraagt kennis en discipline voor wat betreft het omgaan met gegevens.

Het veilig werken met data moet geborgd zijn in rolbeschrijvingen en procesbeschrijvingen. Toegang tot informatie is gebaseerd op rollen *("role-based access control", RBAC*).

Een vorm van dataclassificatie en *tooling* faciliteren het veilig omgaan met gegevens.

Bron:
ICT Strategie | Principes | Veilig is dé norm.

Toegang tot gegevens op basis van rol

Principe: Toegang tot gegevens op basis van rol

Nummer: SEC02

Toegang tot gegevens wordt verleend op basis van rol.

Rationale

De ICT strategie stelt: de Kentalis medewerker gaat veilig om met gegevens (‘ Veilig is de norm’: je kunt veilig werken of je werkt niet). Voorwaardenscheppend voor veilig werken is rol-gebaseerde omgang met data en toepassingen.

Gegevens zijn toegankelijk enkel voor zover nodig voor de uitoefening van een rol (“need to know”/”least privilege” en “zero trust”).

Implicaties

De Kentalis dagelijkse wijze van werken vraagt kennis en discipline voor wat betreft het omgaan met gegevens.

Het veilig werken met data moet geborgd zijn in rolbeschrijvingen en procesbeschrijvingen. Toegang tot informatie is gebaseerd op rollen *(“role-based access control”, RBAC*). De organisatie bepaalt welke rollen welke rechten heeft, ICT implementeert de instrumenten om dit te faciliteren.

Een vorm van dataclassificatie en *tooling* faciliteren het veilig omgaan met gegevens.

Bron:
ICT Strategie | Principes | Veilig is dé norm.

Security by design

Principe: *Security by design*

Nummer: SEC03

Bij elke architectuur en design overweging en besluit wordt het informatiebeveiligingsaspect meegenomen.

Beveiliging is een integraal onderdeel van de bedrijfsvoering en de organisatie.

Rationale

Informatiebeveiliging wordt integraal benaderd: vanuit organisatie, informatie, gegevens, infrastructuur en beheeroptiek. Op deze aspecten en op de verschillende abstractieniveaus is beveiliging afgewogen en doordacht, zowel op het conceptuele (principes, standaarden), logische (ontwerp, richtlijnen, richtlijnen voor wachtwoorden, gebruikersaccounts etc.) en fysieke (concrete maatregelen) niveau.

Bij elk architectuur en design besluit wordt de informatiebeveiliging meegenomen: getoetst aan het Kentalis beveiligings- en privacy beleid en aan wet- en regelgeving.

"privacy by design": privacy wordt gezien als een expliciet onderdeel van informatiebeveiliging en wordt in alle architectuur- en designoverwegingen meegenomen.

Beveiliging wordt niet gezien als een punt dat achteraf nog even gerealiseerd moet worden. Security wordt tijdens veranderingen in bedrijfsvoering en/of organisatie meegenomen.

Implicaties

Bij elk architectuur en design besluit moet het security-aspect expliciet meegenomen worden en gedocumenteerd.

Referentie naar "7 foundational principles" voor *security by design*.

Bron:
ICT Strategie | Principes | Veilig is dé norm.

Beveiligingsmaatregelen in verhouding tot risico's

Principe: Beveiligingsmaatregelen in verhouding tot risico"s

Nummer: SEC04

De beveiligingsmaatregelen *("security controls")* staan in verhouding tot de risico's.

Ze voldoen aan de eisen gesteld door wet & regelgeving.

Rationale

De beveiligingsmaatregelen worden genomen naar ratio van het bedrijfsrisico dat Kentalis loopt bij falen van de beveiliging.

Bij een lager risico passen lichte maatregelen, bij een groter risico passen zwaardere maatregelen.

Waarde toekennen aan de informatie helpt in het bepalen van risico's en het vaststellen van beveiligingsmaatregelen om deze risico's te mitigeren. De informatie wordt niet zwaarder beveiligd dan nodig voor Kentalis en gesteld door wet en regelgeving.

Implicaties

De informatiebeveiliging wordt volgens naleving van de wet toegepast. Beveiliging moet voldoen aan de NEN7510 (voor zorg), ISO27001 en de AVG.

Eventuele restrisico's moeten expliciet door de applicatie-eigenaar geaccepteerd worden en vastgelegd in een risicoregister.

Vraagt om actief risicobeheer: continue monitorren, beoordelen en anticiperen op, wijzigende, bedreigingen.

Te nemen maatregelen zijn onderhevig aan PDCA (Plan-Do-Check-Act).

Bron ICT Strategie | Doelstellingen | Informatietechnologie is compliant. Voldoet aan wet- en regelgeving en "best practices" data is veilig, integer en betrouwbaar.

De eigenaar van data bepaalt het beveiligingsniveau

Principe: De eigenaar van data bepaalt het beveiligingsniveau

Nummer: SEC05

Elk data object heeft een eigenaar ("*Business Owner*"). De eigenaar bepaalt het vereiste niveau van beveiliging voor het betreffende informatie object.

Rationale

De eigenaar bepaalt het beveiligingsniveau van data (waarbij de wet- en regelgeving het minimumniveau dicteert!) en stelt vast wie, wanneer, waar, wat/welke informatie mag inzien of wijzigen en controleert dit periodiek. De eigenaar heeft inzicht in de aard van de informatie en het gewenste beveiligingsniveau.

De eigenaar accordeert de vereiste informatieveiligheid maatregelen (de *"security controls")*.

Implicaties

Elk informatieobject moet toegewezen zijn aan een eigenaar binnen Kentalis. "*Business Owner*".

Elk informatieobject moet een dataclassificatie hebben (Kentalis onderscheidt vier dataclassificaties: Openbaar, Intern, Vertrouwelijk, Zeer vertrouwelijk).

De beveiligingsmaatregelen moeten evenredig zijn met hetgeen beveiligd wordt.

Toegang en gebruik van data is *auditable*

Principe: Toegang en gebruik van data is *auditable*

Nummer: SEC06

De toegang tot en het gebruik van data en applicaties is *auditable*,.

Rationale

Het is mogelijk om de datum, tijd en verantwoordelijkheid op het niveau van een individu vast te leggen voor alle belangrijke gebeurtenissen (modificaties, kopieën, verwijderingen). Nen 7513 schrijft dit voor.

Het is ook een voorwaarde voor voeren van data management.

Implicaties

De applicaties moeten inzicht kunnen geven in toegang en gebruik van data. Op elk moment moet een overzicht gegeven kunnen worden wie toegang heeft gehad tot specifieke data of een applicatie heeft gebruikt. Security-monitoring en -logging zijn belangrijke instrumenten daarvoor.

Reconstructie van gebeurtenissen in de tijd moet mogelijk zijn.

Toegang tot elke applicatie verleend door SSO

Principe: Toegang tot elke applicatie verleend door SSO tenzij

Nummer: SEC07

De toegang tot alle applicaties wordt verleend door Single Sign On (SSO).

Rationale

SSO is het uitgangspunt waaraan elke applicatie moet voldoen. Indien Kentalis de mogelijkheid biedt tot SSO op een applicatie is direct inloggen niet meer toegestaan. De zekerheden die SSO biedt zouden anders omzeild kunnen worden waardoor een kwetsbaarheid ontstaat en het biedt een mogelijkheid om buiten Identity en Access management (IAM) rechten toe te kennen waardoor er onvoldoende controle kan worden uitgevoerd.

Implicaties

Uitzonderingen:

Beheeraccounts van leveranciers op applicaties. Deze worden via een aparte registratie in IAM bewaakt.

- Voor admin account kunnen afwijkende regels gelden.
- In uitzonderlijke gevallen krijgen externe medewerkers toegangsrechten zonder in AFAS geregistreerd te zijn en dus zonder over een Microsoft account bij Kentalis te beschikken. Ook deze worden in IAM geregistreerd. Als toegang tot niet openbare gegevens geboden wordt:
  - Is MFA verplicht
  - Moeten de rechten aangevraagd worden via IAM, in IAM worden geregistreerd en periodiek gecontroleerd worden op consistentie met de rechten in de applicatie.

Als toegang tot niet openbare gegevens geboden wordt:

- Applicaties die laagdrempelig toegankelijk dienen te zijn voor personen die niet aan Kentalis gelieerd zijn mogen voor dergelijke toegang een lager authenticatieniveau instellen, mits in de applicatie geregeld is dat dergelijke accounts nimmer toegang tot de infrastructuur of data van Kentalis verkrijgen. Die laatste is bijvoorbeeld voor sollicitantentoegang op Emply of cursisten in LMS. Deze worden niet in IAM geregistreerd.
- Applicaties die uitsluitend publieke informatie bevatten.

Kentalis EA: Beheer Architectuurprincipes

- BEH01: Minimale beheerslast
- BEH02: Geautomatiseerd updaten tenzij
- BEH03: Beheer browser plug-in/extensie als separate applicatie
- BEH04: Actief beheer van ICT-diensten en ICT-componenten

Minimale beheerlast

Principe: Systemen en diensten worden gekozen en ingericht op minimale beheerlast

Nummer: BEH01

De Kentalis en ICT-systemen worden gekozen en ingericht opdat het dagelijks beheer minimaal is.
Standaard beheertaken, actief en bewakend, zijn zoveel mogelijk geautomatiseerd.

Rationale

Dit geldt voor ICT-systemen en diensten, dit geldt ook voor de procesinrichting en bewaken van proces flows.
Pas 'automatiseer de automatisering toe'.

Implicaties

Beslissers moeten bij keuze van procesinrichting en ICT-systemen en diensten onderscheid kunnen maken in gevraagde beheerlast per oplossingsscenario.
Elke applicatie, ongeacht wel/geen SaaS, heeft een DAB en SLA om de beheerslast en de KPIs te expliciteren. Periodiek overleg met de leverancier vindt plaats waar Service Level Management aspecten als service level afspraken en rapportages, geplande en ongeplande verstoringen en de roadmap op de agenda staan.

Geautomatiseerd updaten tenzij

Principe: ICT-systemen worden geautomatiseerd bijgewerkt tenzij

Nummer: BEH02

De Kentalis ICT-systemen worden geautomatiseerd bijgewerkt (geupdate) tenzij het om een majeure wijziging gaat met te verwachten grote impact op systemen of op eindgebruikers.

Rationale

Leveranciers brengen frequent updates uit voor systeemsoftware en applicaties, bij Kentalis in gebruik. Hetzelfde geldt, zelfs in verhoogde mate, voor afgenomen SaaS-diensten. De leveranciers kondigen de updates vooraf aan.

Onderscheid moet gemaakt worden in kleine, standaard, updates (bijv. v1.01 naar v1.02) en updates die wijzigingen inhouden met grote impact voor eindgebruikers en/of substantieel risico voor continuiteit en beveiligingsniveau (bijv. v1.04 naar v2.0).

Kleine, standaard, updates (patches) worden geautomatiseerd uitgevoerd. Vanwege de aard en met name ook de hoge frequentie van updates checkt de beheerder niet vooraf aard en impact van wijziging.

Grote updates worden vooraf handmatig beoordeeld, eerst uitgevoerd in een testomgeving, en daarna ingebracht in het change-proces en gepland voor uitvoering.

Uitvoering in de productie-omgeving moet, waar wenselijk, in twee etappes kunnen geschieden: uitvoering eerst voor een pilot groep waarna algehele uitvoering.

Implicaties

De beheerders moeten inzicht kunnen hebben in aard en impact van een update, zowel van geplande als van uitgevoerde updates. Daarnaast moeten beheerders , bijv. in geval van een verstoring, toegang hebben tot een centrale logging faciliteit opdat een reconstructie van gebeurtenissen in de tijd mogelijk is.

Beheer browser plug-in/extensie als separate applicatie

Principe: Beheer een browser plug-in als een separate applicatie

Nummer: BEH03

Beschouw een plug-in cq. extensie als een aparte applicatie. De plug-in moet een nuttige functie vervullen (in meer formele termen: een positieve business case hebben) en mag geen onaanvaardbare risico's of andere neveneffecten met zich meebrengen

Rationale

Elke plug-in separaat registreren in de KAL/KAAL lijst als plug-in voor herkenbaarheid.
Dat een plug-in geïntegreerd is met een ander product (bijvoorbeeld van Microsoft maar er zijn er meer) is voor het besluit om het op de KAL of KAAL te zetten irrelevant.
Daarmee wordt een mogelijke wildgroei aan plug-in's voorkomen en security-aspecten van elke plug-in bewaakt.

Maak onderscheid in procedures voor plug-ins en SaaS-applicaties
Maak voor plug-ins, onder voorwaarde dat ze gratis zijn en Kentalis geen beheer doet of andere vormen van ondersteuning biedt, een eenvoudigere intake/change procedure.

Implicaties

De beheerders moeten inzicht kunnen hebben in aard en impact van een plug-in update. Frequentie en aard van plug-in updates in combinatie met vaak zeer beperkte impact en risico vraagt om een vereenvoudigde intake/change procedure vergeleken met (SaaS)-applicatie versiebeheer.

Actief beheer van ICT-diensten en ICT-componenten

Principe: Actief beheer van ICT diensten en componenten

Nummer: BEH04

Elke afgenomen ICT-dienst en elk ICT-component wordt actief beheerd. of

Elke afgenomen ICT-dienst en elk ICT-component wordt actief beheer opgevolgd, afhankelijk van aard en belang van de dienst of component voor de primaire dienstverlening

Rationale

Van elk ICT component en elke ICT dienst wordt bij de intake de wijze van beheer vastgesteld en vastgelegd, afhankelijk van het belang van de dienst voor de Kentalis bedrijfsvoering.
Actief beheer betekent dat bepaald is:

- Welke rol neemt het operationeel beheer op zich
- Welke rol neemt het service management-deel op zich
- Welke rol verzorgt de rapportages van de dienstverlening, waarover wordt met welke frequentie gerapporteerd
- SLA opgesteld
- KPI's vastgesteld
- Waarover te rapporteren
- Frequentie waarmee tactisch & operationeel overleg met de leverancier

Implicaties

Actief beheer

Kentalis EA: Bijlagen