

Principes

Inhoudsopgave

Principes	1
Principes Bedrijfsarchitectuur	1
Kandidaat principes Bedrijfsarchitectuur	2
Vervallen principes Bedrijfsarchitectuur	2
Principes Informatiesysteem architectuur	2
Principes Data architectuur	2
Principes Applicatie architectuur	2
Kandidaat principes Informatiesysteemarchitectuur	2
Vervallen principes Informatiesysteemarchitectuur	2
Principes Technologie architectuur	2
Kandidaat principes Technologie architectuur	3
Vervallen principes Technologie architectuur	3
Principes Security architectuur	3
Generieke principes	3
Privacy principes	3
Security principes technisch (SCIRT-STITCH1.0)	3
Security-by-design principes software ontwikkeling	3
Security principes business	4
Security van gegevens	4
Principes Sourcing	4
Principes achtergrondinformatie	4
Doel	4
Eigenaarschap	4
Reikwijdte	5
Toepasbaarheid (a.k.a. Primacy of Principles)	5
Historie en context	5
Eigenschappen	5
Principes en abstractie	5
Handige Links	6
Kandidaat principes	6

Principes

Voor vragen of opmerkingen over principes kun je terecht bij: architectuur@fontys.nl

Principes Bedrijfsarchitectuur

Bedrijfsprincipes zijn richtinggevende uitspraken op het gebied van de organisatie, producten & diensten, processen en middelen.

- BP1 - Alle vormen van onderwijs worden ondersteund door de IV
- BP2 - De individuele student staat centraal bij de inrichting van IV
- BP3 - Flexibel aanpasbaar onderwijsaanbod
- BP4 - Integrale sturing op de kernactiviteiten Onderwijs, Onderzoek en Valorisatie staan centraal.
- BP5 - Nauwe samenwerking met het werkveld
- BP6 - Processen worden integraal beschouwd en aangestuurd

Informatieprincipes zijn richtinggevende uitspraken op het terrein van applicaties, gegevens en gegevensuitwisseling.

- IP1 - Eigenaarschap wordt belegd
- IP2 - Reductie van complexiteit en standaardisatie²
- IP3 - De kwaliteit van gegevens sluit optimaal aan bij het gebruik
- IP4 - De informatie voorziening wordt geïntegreerd aangeboden
- IP5 - De informatie voorziening wordt duurzaam ingericht
- IP6 - Er wordt op een vertrouwelijke manier met gegevens omgegaan
- IP7 - Archiefwaardige informatie wordt in aangewezen applicaties gearhiveerd

Kandidaat principes Bedrijfsarchitectuur

- verdere verdieping van BP2 - De leervraag van de deelnemer staat centraal bij de inrichting van IV

Vervallen principes Bedrijfsarchitectuur

- BP 4
- IP8 - Gegevens die worden uitgewisseld worden geconformeerd aan het gegevensmodel (FBD)

Principes Informatiesysteem architectuur

Principes Data architectuur

- DP1 - Digitaliseer data
- DP2 - Data heeft één systeem als bron
- DP3 - Raadpleeg data bij de bron
- DP4 - Gegevens blijven eigendom van Fontys (was PP13)

Principes Applicatie architectuur

- AP1 - Applicaties worden altijd gekoppeld via de Fontys integratie laag
- AP2 - Applicaties en leveranciers worden beschouwd en behandeld als services
- AP3 - Buy before build
- AP4 - Vermijdt maatwerk
- AP5 - Applicaties functioneren logisch maar in één laag
- AP6 - Er is sprake van modulaire toepassing van laag-overschrijdende applicaties
- AP7 - Een gegevenselement heeft één systeem als bron
- AP8 - Applicaties binnen Fontys worden zoveel mogelijk hergebruikt
- AP9 - Applicaties moeten zijn ingericht met rol gebaseerde toegang
- AP10 - Digitalisering van de input
- AP12 - Minimaliseer gebruik van Microsoft Office producten (zoals Word/Excel-PowerPoint-Visio) als productiesystemen
- AP13 - Management Informatie is rechtstreeks gebaseerd op de feitelijke transactiedetails
- AP14 - Granulariteit van gegevens zijn op transactie-niveau
- AP15 - Interoperabiliteit van applicaties is niet beperkt tot Fontys

Kandidaat principes Informatiesysteemarchitectuur

Vervallen principes Informatiesysteemarchitectuur

- AP4
- AP11

Principes Technologie architectuur

Technische principes zijn richtinggevende uitspraken op het terrein van technische componenten, gegevensopslag en netwerken.

- TP1 - Benut de Cloud
- TP2 - Gebruik Microsoft
- TP3 – Onafhankelijkheid tijd, apparaat en plaats
- TP4 – Veilige authenticatie
- TP5 – Gebruik versleuteld netwerkverkeer
- TP6 – Uitzonderingen zijn tijdelijk
- TP7 - Vooruitstrevende technologie gebruiken
- TP8 – Technische kaders gelden

NOTE! Technologie principes zijn ook opgenomen in de Technische Kaders.

Kandidaat principes Technologie architectuur

Vervallen principes Technologie architectuur

TP9 - Eindgebruikersfunctionaliteit kan tijd- en plaats onafhankelijk worden gebruikt

Principes Security architectuur

De kaders vanuit wetgeving (AVG) en SURF zijn hiervoor leidend.

Randvoorwaardelijk architectuurprincipe: Het succes van het toepassen van ISP-principes is evenredig met het eenduidig belegd zijn van verantwoordelijkheid van data, proces en systeem.

De Twijnstra-Gudde Rapportage evaluatie Interventieagenda Fontysberaad van 2019 laat zien dat aan deze randvoorwaarde nog niet wordt voldaan.

Generieke principes

- ISP-G.01 - Informatieveiligheid is een verantwoordelijkheid van iedereen en we communiceren open over risico's
- ISP-G.02 - Informatieveiligheid is risico gebaseerd
- ISP-G.03 - Informatieveiligheid is een continu kwaliteitsproces
- ISP-G.04 - Integrale aanpak informatiebeveiliging door Security by Design
- ISP-G.05 - Standaard beperkte toegang en veilige instellingen door Security by Default
- ISP-G.06 - Mitigerende maatregelen tegen informatierisico's is een (eerste) lijnverantwoordelijkheid
- ISP-G.07 - Mitigerende maatregelen zijn in balans met het risico (proportionaliteit)
- ISP-G.08 - Zorg voor eenvoud. Complexiteit is de vijand van beveiliging
- ISP-G.09 - Wees terughoudend met vertrouwen, controleer altijd
- ISP-G.10 - Verzeker dat veiligheid een motor is voor innovatie

Privacy principes

LET OP! Bij Fontys geldt het adagium *Privacy by Design*, waarbij de privacy principes op **WETTEN** zijn gebaseerd.

- **WET** ISP-P.01 - Data moet alleen voor welbepaalde doelen worden verzameld en alleen voor die doelen worden gebruikt. (Doelspecificatie)
- **WET** ISP-P.02 - Er mag niet meer verzameld worden dan noodzakelijk voor het doel. (Dataminimalisatie)
- **WET** ISP-P.03 - Gegevens moeten voldoende accuraat en actueel zijn. (Juistheid)
- **WET** ISP-P.04 - Persoonsgegevens zijn opgeslagen in lijn met de AVG. (Opslag)
- **WET** ISP-P.05 - Verwerking moet transparant zijn.
- **WET** ISP-P.06 - Individuen moeten inzage hebben in hun gegevens en waar nodig om correctie of verwijdering kunnen vragen.
- **WET** ISP-P.07 - Privacy gegevens moeten afdoende worden beveiligd.
- **WET** ISP-P.08 - Bij de start van het ontwerpen van een informatiesysteem of dienst wordt de bescherming van persoonsgegevens meegenomen (privacy by design)
- **WET** ISP-P.09 - Standaardinstellingen van een programma, app, website, dienst of apparaat worden altijd zo privacy-vriendelijk mogelijk ingesteld (privacy by default)
- **WET** ISP-P.10 - Accountability

Security principes technisch (SCIRT-STITCH1.0)

- ISP-T.01 - Alle gegevens worden versleuteld getransporteerd, inclusief alle opslag op mobiele apparaten
- ISP-T.02 - De identiteit van gebruikers is gecontroleerd en federatief beheerd
- ISP-T.03 - Autorisatie vindt plaats op basis van functiescheiding en least privilege (need-to-know)
- ISP-T.04 - Veilig sessiemanagement wordt toegepast
- ISP-T.05 - Alle in- en uitvoer van data wordt genormaliseerd, gevalideerd en ingeperkt
- ISP-T.06 - Configuratie-lekken worden voorkomen
- ISP-T.07 - Systemen bieden voldoende mogelijkheden voor auditing en logging
- ISP-T.08 - Er vindt continu onderhoud en patchmanagement plaats
- ISP-T.09 - Aanvullend on-premise: perimeter security, segmentering, hardening, fysieke beveiliging

Security-by-design principes software ontwikkeling

- ISP-O.01 - Secure software life cycle
- ISP-O.02 - Ontwerp vereist security controls door gebruik te maken van threat modeling (STRIDE)
- ISP-O.03 - Webapplicaties worden informatieveilig ontwikkeld en bevatten geen kwetsbaarheden uit de OWASP Top-10
- ISP-O.04 - Formeel testtraject voor promotie van O(ntwikkeling) T(est) A(ccceptatie) P(roductie)

Security principles business

- ISP-B.01 - Informatiebeveiligings- en privacy incidenten worden altijd (veilig) gemeld, geregistreerd, geprioriteerd en opgevolgd
- ISP-B.02 - De data- en procesverantwoordelijke beschikt over een release kalender en voorkomt legacy (versie beheer)
- ISP-B.03 - Interne- en externe (IaaS, PaaS of SaaS) systemen worden getoetst op kwetsbaarheden (e.g. vulnerability scanning, pentesten)
- ISP-B.04 - Er worden periodiek audits uitgevoerd
- ISP-B.05 - Organiseer gebruikersopleidingen en bewustmakingsinitiatieven

Security van gegevens

Datamanagement is nog onvolwassen binnen Fontys

- ISP-D.01 - Gegevens zijn en blijven eigendom van Fontys (ook na contract-einde)
- ISP-D.02 - Er is duidelijk gedefinieerd datamanagementplan in lijn met het bedrijfsmodel
- ISP-D.03 - Implementatie van data lifecycle control
- ISP-D.04 - Identificatie van data-eigenaarschap en -beheer
- ISP-D.05 - Gegevens (analoog en digitaal) zijn beveiligd op basis van hun risicoclassificatie

(BIVCP: Beschikbaarheid, Integriteit, Vertrouwelijkheid, Controleerbaarheid, Privacy)

- ISP-D.06 - Het maximaliseren van het nut van gegevens om herverzameling of verwerking van gegevens te voorkomen

(Eenmalige vastlegging (data bij de bron) en (via API) meervoudig gebruik)

- ISP-D.07 - Opzetten van gegevenskwaliteitsnormen (datakwaliteit)
- ISP-D.08 - Zorgen voor goede documentatie en tracking van gegevens
- ISP-D.09 - Bedrijfscontinuïteit, incl. back-up & restore en disaster recovery (Azure)?

Principes Sourcing

- Sourcing 1 - Een goede Fontys onderwijs (ondersteunende) oplossing stelt de student en het onderwijs & onderzoek centraal door functionaliteit te beoordelen vanuit hun perspectief. Dit wordt gedaan door middel van customer journey en persona's student, werkveld, docent & lector en medewerker.
- Sourcing 2 - De markt voor digitaal onderwijs en onderwijs ondersteuning is beter in staat dan Fontys om passende IV oplossingen aan te bieden.
- Sourcing 3 - Fontys kiest voor volwassen IV oplossingen.
- Sourcing 4 - Fontys kiest voor IV oplossingen die voldoen aan haar kaders.
- Sourcing 5 - Voor onderwijs specifieke IV oplossingen (Digitale onderwijs vernieuwing en ICT in Onderwijs) bestaat de mogelijkheid tot experimenteren onder voorwaarden.

Principes achtergrondinformatie

Doel

Het doel van principes is om concrete richtlijnen te hebben die sturing geven aan gezamenlijke ontwikkelingen. De principes zijn in feite de afspraken die gemaakt worden en die worden toegepast bij de besluitvorming over vernieuwing. Het geeft de kaders waaraan nieuwe ontwikkelingen geacht worden te voldoen.

Eigenaarschap

Eindverantwoordelijk	Concern Informatie Manager => John Kropman
Verantwoordelijk	Architectuur Team
Geconsulteerd	ISP, Infra consultants en andere consultants binnen Dienst IT
Geïnformeerd	Alle Fontys medewerkers kunnen bij deze principes.

Reikwijdte

De principes gelden voor iedereen die betrokken is bij de informatievoorziening van Fontys.

Ze gelden dus voor iedereen!

De principes worden met name veel gebruikt door:

- Architectuur Team en specifieke Solution Architecten die betrokken zijn bij de projecten
- Architectuur Board
- Informatie Managers
- Projectleden
- Projectstuurgroep

Toepasbaarheid (a.k.a. Primacy of Principles)

Principes zijn ontstaan vanuit twee redenen:

1. onze regel om voor Fontys een beheerbare informatievoorziening te realiseren
2. opgelegd vanuit wetgeving.

Voor 1 geldt: **”Pas toe of leg uit!”**. We verzoeken dringend om de principes toe te passen, maar er is ruimte om in overleg af te wijken van een principe, waarbij de argumenten om af te wijken vastgelegd worden in de PSA en het centrale Afwijkingenregister

Voor 2 geldt: van een **WET** kan niet worden afgeweken en het principe dient toegepast te worden. Bij afwijken worden de gevolgen van het overtreden van de wet aanvaard. Neem bij twijfel contact op met je leidinggevende, juridische zaken, het ISP office of het AT.

Historie en context

Alles verandert in het leven en in de wereld, zo ook Principes. Om toch te zorgen dat de principes enigszins stabiel zijn en er ook historische context wordt behouden, passen we op de Principes het principe toe van ”Append Only”. Dit houdt in dat principes wel kunnen vervallen, maar dat er geen nieuwe voor in de plaats komt. Nieuwe principes komen altijd met een nieuwe code, zodat verwijzingen naar de principes stabiel blijven.

Link naamswijzigingen zullen ook stabiel blijven, waarbij oude namen naar de meest recente linknaam zullen redirecten.

Eigenschappen

Ieder principe heeft dezelfde eigenschappen:

1. **Unieke naam** - De naamgeving van het principe is kort, bondig en makkelijk te onthouden.
2. **Beschrijving** - Kort en bondig beschrijving van het principe
3. **Rationale** - Beschrijft de voordelen en de relaties met andere principes, als het kan met een verhelderend voorbeeld.
4. **Implicaties** - Geeft aan wat de gevolgen zijn voor mij, het product, de dienst of project?
5. **Grafisch element**- Verwijzing naar entiteiten in de Fontys Enterprise Architectuur waar dit principe gevolgen heeft. (De eigenschappen worden automatisch gegenereerd vanuit de applicatie Sparx Enterprise Architect)
6. Metadata: **Startdatum** en evt ”Einddatum”
7. Contactgegevens

Voor uitgebreide uitleg zie TOGAF Components of Architecture Principles

Principes en abstractie

”The devil is in the details”

We willen just-enough principes. Te weinig levert geen resultaat en kwaliteit. Te veel maakt het proces stroperig en nodigt uit tot omzeilingen via olifantenpaadjes. Het balanceren van het juiste aantal principes blijft een continu proces.

Naast principes zijn er meerdere vormen van sturing. Hieronder van algemeen naar concreet (As van concretisering):

- principes
- richtlijnen
- kaders

- business rules
- werkinstructies

TODO: uitwerken welke we gebruiken binnen Fontys en hoe deze vormen zich tot elkaar verhouden.

Handige Links

- Principe volgens Wikipedia
 - Principes architectuur volgens TOGAF
 - Principes informatievoorziening volgens HORA
 - Fontys Motivatie View met principes
 - ArchiXL voorbeeldprincipes
-
- Agile Manifesto Principles
 - Johan Cruijff principes

Kandidaat principes

- 2021-03-02 Johan Theunissen: Data provenance should be transparent.
- Make IT Small! (2019-10-04 - Johan Theunissen: zie Thema - Wendbare & flexibele organisatie)
- Gegevens zijn beveiligd op basis van hun risicoclassificatie
- Beveilig de zwakste schakel
- Defence in depth, beveiliging op elke laag
- Faal veilig
- Gebruik open standaarden
- Least privilege, alleen toegang tot voor het werk noodzakelijke informatie
- Zorg voor functiescheiding
- Zorg voor eenvoud. Complexiteit is de vijand van beveiliging.
- Wees terughoudend met vertrouwen
- Neem aan dat je geheimen niet zeker zijn. (Security through obscurity)
- Houd beveiliging bruikbaar
- Beveiliging kan niet achteraf als extraatje worden aangebracht
- Laat de moeilijke dingen aan de experts over
- Security en privacy zijn niet uitwisselbaar
- Law of Demeter (principle of least knowledge)
 - Toepassen op AT: Positiespel!!!
 - Business Architect hoeft niet te praten met Technology Architect.(wel met de tussen in gepositioneerd Informatie Systemen Architect)
- Think BIG, start small, Learn Fast
- The higher the uncertainty, the faster the feedback loop
- Unsure? Test it with a customer!

LEAN Principles Deze LEAN Principles zijn optioneel en ter inspiratie.

- Define Value
- Map the Value Stream
- Create Flow
- Establish Pull
- Pursue Perfection

Seven deadly wastes in Lean = TIMWOOD

1. Transportation: moving things around;
 2. Inventory
 3. Motion: people moving;
 4. Waiting: people waiting;
 5. Over-processing: producing more quality or functionality than the customer wants;
 6. Over-production: producing a higher quantity than the customer needs;
 7. Defects: Failures in processes and products, leading to rework and waste.
-
- LEAN - Principe S1 - Sorteren - Sort (EN) - Seiri (JP)
 - LEAN - Principe S2 - Schoonmaken - Shine (EN) - Seiso (JP)

- LEAN - Principe S3 - Schikken - Straighten (EN) - Seiton (JP)
 - LEAN - Principe S4 - Standaardiseren - Standardize (EN) - Seiketsu (JP)
 - LEAN - Principe S5 - Standhouden - Sustain (EN) - Shitsuke (JP)
-