|  |
| --- |
| Template Architectuur[Ondertitel] |

|  |  |
| --- | --- |
| Auteur(s): |  |
| Versie: |  |
| Datum: | Kies of typ een datum |
| Kenmerk: |  |
|  |
|  |

**Documentinformatie**

Dit document maakt onderdeel uit van een complete set (piramide) met formeel vastgestelde documenten op strategisch, tactisch en operationeel niveau. Dit document heeft betrekking op de laag Beleid in de beleidspiramide.



**Versiebeheer**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur** | **Verwerking** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Distributielijst**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Ontvanger** | **Doel** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Vaststelling**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum** | **Vastgesteld door** | **Vastgesteld op** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Samenhang met andere documenten**

|  |  |  |  |
| --- | --- | --- | --- |
| **Naam** | **Bovenliggend** | **Gelijk niveau** | **Onderliggend** |
| [INFORMATIEBEVEILIGINGSBELEID] | x |  |  |
| [ARCHITECTUURDOCUMENTEN] |  |  | x |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | G04; |
| ISO27001 |  |

**Creative Commons**

Dit template is een product van het SURF Security Expertise Centrum en beschikbaar onder de licentie Creative Commons Naamsvermelding 4.0 Internationaal. <https://creativecommons.org/licenses/by/4.0/deed.nl>

Inhoudsopgave

|  |
| --- |
| [Samenvatting 4](#_Toc157689001)[1 Inleiding 5](#_Toc157689002)[2 Model 6](#_Toc157689003)[2.1 Enterprise Architectuur 6](#_Toc157689004)[2.2 Enterprise Information Architectuur 6](#_Toc157689005)[2.3 IT-architectuur 6](#_Toc157689006)[2.4 Informatiebeveiligingsarchitectuur 6](#_Toc157689007)[2.5 Netwerkarchitectuur 6](#_Toc157689008)[2.6 Groei naar doelarchitecturen 7](#_Toc157689009)[2.7 Separate goedkeuring 7](#_Toc157689010)[3 Principes 8](#_Toc157689011)[3.1 Security by Design 8](#_Toc157689012)[3.2 Security by Default 8](#_Toc157689013)[3.3 Zero Trust 8](#_Toc157689014)[3.4 [Principe] 8](#_Toc157689015)[4 Wijzigingen en afwijkingen 9](#_Toc157689016)[Vaststelling 10](#_Toc157689017) |

Samenvatting

Hier komt een samenvatting, op zichzelf leesbaar, van de inhoud van dit document in max. 1 A4.

# Inleiding

[INSTELLING] hanteert voor de vormgeving van haar IT-omgevingen een architectuur, waarin de samenhang van de IT- en andere componenten wordt geschetst, en keuzes worden aangegeven bepaalde componenten al of niet toe te laten in de (IT) omgeving en hoe dat dient te gebeuren. Opzet, beheer en handhaving van deze (IT-)architectuur is neergelegd bij de IT-afdeling.

De onderkende [INSTELLING]-brede risico’s, en architectuurkeuzes en -componenten hebben invloed op de gewenste en haalbare informatiebeveiliging, en op de ten behoeve van informatie­beveiliging in te zetten IT-beveiligingsarchitectuur en de componenten daarvan. Dit vindt weerslag in deze informatiebeveiligingsarchitectuur.

# Model

## Enterprise Architectuur

[INSTELLING] hanteert voor de organisatie -architectuur het [Invullen]-model. Dit wordt als volgt gehanteerd:

* [Keuzes uit/in het model hier opsommen]

De huidige de facto Enterprise Architectuur is weergegeven in het document [EAM Ist-document]

De doel- Enterprise Architectuur is weergegeven in het document [EAM Soll-document]

## Enterprise Information Architectuur

[INSTELLING] hanteert voor de organisatie-informatie-architectuur het [Invullen]-model. Dit wordt als volgt gehanteerd:

* [Keuzes uit/in het model hier opsommen]

De huidige de facto Enterprise Information Architecture is weergegeven in het document [EIAM Ist-document]

De doel- Enterprise Information Architecture is weergegeven in het document [EIAM Soll-document]

## IT-architectuur

[INSTELLING] hanteert voor de organisatiebrede IT-architectuur het [HOSA/MOSA/MORA/HORA/TOGAF/...]-model. Dit wordt als volgt gehanteerd:

* [Keuzes uit/in het model hier opsommen]

De huidige de facto IT-architectuur is weergegeven in het document [IT-Architectuur Ist-document]

De doel-IT-architectuur is weergegeven in het document [IT-Architectuur Soll-document]

## Informatiebeveiligingsarchitectuur

[INSTELLING] hanteert voor de organisatiebrede informatiebeveiligingsarchitectuur het [HORA/HOSA/TOGAF/SABSA/...]-model. Dit wordt als volgt gehanteerd:

* [Keuzes uit/in het model hier opsommen]

De huidige de facto informatiebeveiligingsarchitectuur is weergegeven in het document [IB-Architectuur Ist-document]

De doel-informatiebeveiligingsarchitectuur is weergegeven in het document [IB-Architectuur Soll-document]

## Netwerkarchitectuur

[INSTELLING] hanteert voor de organisatiebrede netwerkarchitectuur het {NETWERKARCHITECTUURMODEL] model. Dit wordt als volgt gehanteerd:

* [Invullen]

De huidige de facto netwerkarchitectuur is weergegeven in het document [Netwerk Ist-document]

De doel-netwerkarchitectuur is weergegeven in het document [Netwerk Soll-document]

## Groei naar doelarchitecturen

[INSTELLING] heeft de huidige, de facto architecturen en de doelarchitecturen gedocumenteerd en heeft inzicht in de verschillen daartussen.

[INSTELLING] streeft bij besluitvorming over veranderingen aan processen, systemen en netwerken naar verkleining van die verschillen.

## Separate goedkeuring

[SENIOR MANAGEMENT] van [INSTELLING] heeft bovenstaande de facto- en doelarchitecturen goedgekeurd.

# Principes

## Security by Design

[INSTELLING] hanteert in de informatiebeveiligingsarchitectuur het Security By Design principe. Hieronder wordt verstaan dat bij het ontwerp van systemen en wijzigingen aan systemen en processen, ervoor wordt zorggedragen dat informatiebeveiliging als een van de doelstellingen van het ontwerp wordt uitgevoerd en onlosmakelijk onderdeel is van de implementatie. Bij [implementatie/onderhoud/...] toetst de [verantwoordelijk functionaris] dat aan dit principe onverkort wordt voldaan.

## Security by Default

[INSTELLING] hanteert in de informatiebeveiligingsarchitectuur het Security By Default principe. Hieronder wordt verstaan dat systemen zodanig zijn geïmplementeerd dat als ze onverhoopt niet naar behoren (dus veilig) werken, de informatie die door de systemen wordt verwerkt, ten minste even veilig is als bij normaal functioneren. Bijvoorbeeld doordat bij storingen niet alleen toegang tot alle gegevens krijgen maar juist automatisch wordt teruggevallen op een zeer restrictief toegangsregime. Bij [implementatie/onderhoud/...] toetst de verantwoordelijk functionaris dat aan dit principe onverkort wordt voldaan.

## Zero Trust

[*Deze paragraaf is optioneel en geeft een, overigens wel geadviseerd, voorbeeld. Zie* [*https://sec.surf.nl/zero-trust-cyberweerbaarheid/*](https://sec.surf.nl/zero-trust-cyberweerbaarheid/) *voor een uitwerking hoe hiermee om te gaan.]*

[INSTELLING] hanteert in de Identity- en Access Management-architectuur het Zero Trust principe. Het zero trust-principe gaat er niet vanuit dat het IT-landschap vertrouwd kan worden en veilig is, maar neemt als uitgangspunt dat het niet veilig is. Het gaat uit van het principe ‘nooit vertrouwen, altijd verifiëren’: ieder toegangsverzoek wordt volledig geverifieerd, gemachtigd en versleuteld voordat toegang wordt verleend. Bij [implementatie/onderhoud/...] toetst de verantwoordelijk functionaris dat aan dit principe onverkort wordt voldaan.

## [Principe]

[INSTELLING] hanteert in de informatiebeveiligingsarchitectuur het [...] principe. Hieronder wordt verstaan [uitleg]. Bij [implementatie/onderhoud/...] toetst de [verantwoordelijk functionaris] dat aan dit principe onverkort wordt voldaan.

# Wijzigingen en afwijkingen

Voorafgaand aan keuzes voor voorgestelde veranderingen in de informatieverwerking en IT van [INSTELLING] wordt getoetst of zal worden voldaan aan de architectuurprincipes en of de veranderingen realisatie van de doelarchitectuur dichterbij brengen.

Indien naar mening van [INSTELLING] het eventueel niet voldoen te veel risico’s met zich meebrengt of die risico’s niet voldoende eenvoudig en efficiënt kunnen worden gemitigeerd, zal [INSTELLING] de voorgestelde veranderingen afwijzen of alternatieven eisen die wel binnen de principes passen.

Indien risico-mitigering redelijkerwijs mogelijk is, zullen de mitigerende acties onder budget van de veranderingen worden uitgevoerd voordat of uiterlijk gelijktijdig met de veranderingen als zodanig worden geïmplementeerd.

Voor zover zulke aanpassingen niet redelijkerwijs mogelijk blijken, zal [INSTELLING] per afwijking bepalen of dit additionele risico kan worden geaccepteerd en worden geadministreerd conform geïmplementeerde risicobehandelingsprocedures.

Voor zover de huidige informatiebeveiligingsarchitectuur niet voldoet aan de gekozen principes, wordt per geval en per principe bepaald welke risico’s hierdoor eventueel onvoldoende worden gemitigeerd. Per geval wordt bepaald of en hoe dit additionele risico zal worden behandeld conform geïmplementeerde risicobehandelingsprocedures.

# Vaststelling

Dit beleid is aldus vastgesteld.

[PLAATS], [DATUM].

[HET COLLEGE / DE RAAD VAN BESTUUR].

[Na (her)vaststelling, ook de tabel op p.2 bijwerken]