|  |
| --- |
| Template LeveranciersmanagementOndertitel |

|  |  |
| --- | --- |
| 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 Thema-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 |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Verwijzingen naar SURFaudit Toetsingskader en ISO27001**

|  |  |
| --- | --- |
| **Kader** | **Verwijzing (tags)** |
| SURFaudit Toetsingskader | SC.01; SC.02; SC.03; SC.04 |
| ISO27001 | A.5.19; A.5.20; A.5.21; A.5.22; A.5.23 |

**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](#_Toc161840113)[1 Inleiding 5](#_Toc161840114)[2 Contracten 6](#_Toc161840115)[3 Aanbestedingseisen 7](#_Toc161840116)[4 Rapportages 8](#_Toc161840117)[5 Interne beheersing bij derden 9](#_Toc161840118)[Cloudgebruik 10](#_Toc161840119)[6 Data-afscherming 11](#_Toc161840120)[Vaststelling 12](#_Toc161840121)[Bijlage 1 Voorbeeld Inkoop eisen beveiliging PvE 13](#_Toc161840122)[1.1 Autorisatie 14](#_Toc161840123) |

Samenvatting

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

# Inleiding

[INSTELLING] heeft in het informatiebeveiligingsbeleid opgenomen dat het beleid ook betrekking heeft op externe relaties. Van deze externe relaties zijn leveranciers een belangrijke groep. Dit betreft niet alleen leveranciers van IT-diensten op onze systemen, maar ook leveranciers van IT-diensten op hun eigen systemen of in de cloud. En er zijn leveranciers van diensten die niet-IT-diensten leveren, maar wel informatie van ons verwerken. Op al deze leveranciers zijn alle regels die we hanteren voor informatiebeveiliging onverkort van toepassing, en bij het aangaan, beheren, gebruiken en ontkoppelen van deze relaties zijn behalve onze algemene regels, ook specifieke regels van toepassing.

Mede door middel van Leveranciersmanagement zoals weergegeven in dit document, geeft [INSTELLING] hier invulling aan.

[*Onderstaande zal door een aparte SURF-werkgroep nadere uitwerking krijgen. Vooralsnog staan hieronder alleen enkele algemene regels en de regels opgesteld die conform het SURFaudit Toetsingskader nodig zijn.]*

# Contracten

*[Vul hier in hoe wordt omgegaan met ‘het’ contractenregister, en met het register met IT-leveranciers in het bijzonder.]*

Het contractenregister (incl. het register met IT-leveranciers) spelen een essentiële rol in het effectieve beheer van leveranciersrelaties en het waarborgen van naleving van contractuele verplichtingen. Aangezien de inrichting en mate van volwassenheid van contract- en leveranciersmanagement kunnen variëren per instelling, wordt hieronder een overzicht gegeven van enkele richtlijnen en aanbevelingen hoe dit te beschrijven.

Contractenregister

* Definitie: Het contractenregister omvat alle contracten die de organisatie heeft afgesloten met interne en externe partijen.
* Beheer: Het register moet centraal worden beheerd en regelmatig worden bijgewerkt om de meest actuele informatie weer te geven.
* Inhoud: Elk contract moet duidelijk worden geïdentificeerd met relevante details, waaronder contractnaam, partijen, contactgegevens, start- en einddatum, contractvoorwaarden, verantwoordelijke functionarissen, geleverde producten/diensten, contractuele verplichtingen en service level agreements (SLA's).
* Risicobeoordeling: Voer regelmatig een risicobeoordeling uit van IT-leveranciers om potentiële risico's te identificeren en passende beheersmaatregelen te implementeren.
* Prestatiebeoordeling: Evalueer periodiek de prestaties van IT-leveranciers aan de hand van overeengekomen SLA's en KPI's om de kwaliteit van de geleverde producten/diensten te waarborgen.
* Toegang: Zorg ervoor dat het register toegankelijk is voor relevante belanghebbenden binnen de organisatie, zoals juridische, financiële en operationele teams.

Door een gestructureerd contractenregister te onderhouden en te beheren, borgt [INSTELLING] beter grip op haar leveranciersrelaties, het verminderen van risico's en naleving van contractuele verplichtingen.

# Aanbestedingseisen

[INSTELLING] hanteert bij voorgenomen aanschaf van IT-diensten de processen en procedures die voor heel [INSTELLING] gelden, te weten:

*[Vul hier de aanbestedingsregels in, of verwijs naar (het document met) de aanbestedingsregels of het Inkoopbeleid die bijvoorbeeld een afdeling Inkoop bijhoudt.]*

Voor de aanschaf of inhuur van IT-diensten en/of IT-middelen gelden bovendien de volgende eisen:

* [De aan te schaffen c.q. te huren dienst of het IT-middel past binnen de vastgestelde (doel)architectuur.]
* [Het contract voor de aan te schaffen c.q. te huren dienst of het IT-middel wordt eerst toegekend, goedgekeurd en ondertekend als ... <vul hier de eisen in zoals een volledig uitgewerkte SLA *op basis van business requirements;* niet een voornemen er ooit een op te stellen, etc.>]
* [Verwijs hier naar SURF Security Baseline[[1]](#footnote-2) en benoem wat daaruit voor de specifieke casus van toepassing is].
* [In Bijlage 1 van deze template is een voorbeeld gegeven van hoe eisen verwerkt kunnen worden in een pakket van eisen. Let op hier aan te geven wat knock-outcriteria zijn, zoals het voldoen aan het informatiebeveiligingsbeleid van je instelling, welke bandbreedtes (voor ondersteuning bijvoorbeeld) acceptabel zijn enz. Hierbij kan ook worden aangegeven dat voordat het contract wordt getekend, vaststaat dat de leverancier voldoet aan alle wettelijke en contractverplichtingen zoals het op peil hebben van de interne beheersing als hieronder aangegeven.]

# Rapportages

De SLA bevat clausules die de leverancier verplichten periodiek, ten minste per kwartaal, te rapporteren over de geleverde diensten c.q. productprestaties, afwijkingen daarvan en opgetreden incidenten.

[*Per kwartaal is een redelijke termijn. Als de leverancier (gegeven de risico’s) minder belangrijk is in het grotere geheel, kan eventueel met een halfjaarlijkse of jaarlijkse rapportage worden volstaan*.]

Deze rapportages en de relationele en contractuele aspecten die de afgelopen periode zijn voorgevallen, worden besproken met de feitelijke dienst- c.q. [PRODUCTONTVANGER / PRODUCTMANAGER / IT-MANAGER] en de betreffende proces- of systeemeigenaar van [INSTELLING].

[*Overweeg hier meer specifieke regels op te nemen over de rapportage.*]

[*Neem hier ook (verwijzingen naar) de regels op rond rapportage over incidenten, zeker als er privacy-aspecten aan de orde zijn.]*

# Interne beheersing bij derden

*[Neem hier de regels op die worden opgelegd aan de leveranciers, en wat te doen bij afwijkingen of tekortkomingen. Minimaal moeten hier regels staan over:*

*Dat de leverancier zelf de interne beheersing op orde heeft (opzet, bestaan en werking), ten minste op hetzelfde niveau als je instelling;*

*Dat de status van de interne beheersing bij de leverancier periodiek wordt beoordeeld (bijvoorbeeld door jaarlijkse audit(s) of door andere rapportages);*

*Dat er procedures zijn afgesproken hoe de leverancier gaat aantonen dat die zich aan alle contractbepalingen houdt.]*

Binnen [INSTELLING] wordt in het risicomanagement aparte aandacht gegeven aan de risico’s rond doorlopende dienstverlening van voldoende kwaliteit door respectievelijke leverancier(s). Hierbij wordt rekening gehouden met eventuele geheimhoudingsovereenkomsten, escrow-overeenkomsten, doorlopende (financiële) levensvatbaarheid van leveranciers, het voldoen aan onze beveiligingseisen, verwerkersovereenkomsten ingeval de leverancier namens ons persoonsgegevens verwerkt, eventuele beschikbare alternatieve leveranciers voor bepaalde diensten en producten, bonus/malusregelingen in contracten etc.

Indien in dit specifieke risicomanagement zaken opduiken die nader onderzoek of besluiten vergen, zoals ongemitigeerde, onmitigeerbare of nog niet geaccepteerde risico’s, dan worden deze met het [COLLEGE VAN BESTUUR / CONTRACTEIGENAAR] besproken en het [COLLEGE VAN BESTUUR / CONTRACTEIGENAAR] beslist over eventueel te nemen maatregelen.

# Cloudgebruik

*[Als je instelling aparte regels heeft over leveranciers met software in de cloud (Software-as-a-Service), en/of over cloud-leveranciers, neem die dan hier op.]*

*[Als je instelling gebruik maakt van de cloud, neem hier dan de regels en procedures op over wat je zelf nog aan (beveiligings)instellingen moet hebben geregeld ... “Het staat in de cloud en die is wel veilig, toch?” is zeker onvoldoende!]*

# Data-afscherming

*[Neem hier de regels op die zijn afgesproken over de bescherming van de gegevens die door derden worden verwerkt. Denk hierbij aan het verschil tussen gegevensgebruik door interne afdelingen (HR- en Financiën-gegevens apart), ingehuurde derden, SaaS-leveranciers en anderen, cloudleveranciers, etc. Let hierbij op wat er in het kader van de Avg is afgesproken, en wat al of niet in Verwerkersovereenkomsten is verwerkt – zowel de dingen die wel standaard zijn, als de afwijkingen (opsommen).]*

# Vaststelling

Dit beleid is aldus vastgesteld.

[PLAATS], [DATUM].

[CISO / DIR IT / CIO].

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

1. Voorbeeld Inkoop eisen beveiliging PvE

Onderstaand een voorbeeld van inkoop eisen die in een PvE gesteld kunnen worden bij de uitvoer van een aanbesteding.

|  |  |  |
| --- | --- | --- |
| **Nr.**  | **Eis**  | **Beantwoording**  |
| 0 | De leverancier kan aantonen door middel van certificeringen dat de beveiliging van de omgeving van de leverancier voldoet aan geldende beveiligingsnormen (ISO27001, ISAE3402 type 2, SOC compliance rapport) |  |
| 1  | Het gegevenstransport is beveiligd door middel van het TLS 1.2 protocol.  |   |
| 2  | Webbased single sign on (SSO) is mogelijk via het SAML v2 protocol voor elke vorm van gebruikers authenticatie.   |   |
| 3  | Het systeem ondersteunt SSO/  federatieve authenticatie via SURFconext  |   |
| 4  | Systeemwachtwoorden (bijvoorbeeld service accounts) voldoen aan het Opdrachtgever wachtwoordbeleid (zie document ‘Toegangsbeleid 2.0’) en kunnen bijvoorbeeld periodiek zonder impact veranderd worden.  |   |
| 5  | In de applicatie kan het autorisatiemodel op verschillende niveaus worden ingesteld, zoals: 1. op systeemniveau;
2. op het niveau van gegevensmanipulatie (CRUD);
3. op het niveau van gegevensgroepen en verzamelingen;
4. op het niveau van functies (lookup/report);
5. op het niveau van schermen;
6. op het niveau van workflow.
 |   |
| 7  | De applicatie implementeert security by design en volgt best-practices zoals OWASP (Open Web Application Security Project). Dit zal gecontroleerd worden door de Opdrachtgever met behulp van een penetratietest of gelijkwaardige onderbouwing bij oplevering.  |   |
| 8  | Alle mutaties in de applicatie kunnen worden gelogd, waaronder in ieder geval vastlegging van mutatiedatum/tijd en gebruikers-id.   |   |
| 9  | Op basis van het ISMS met bijbehorende risico inventarisatie heeft de Opdrachtnemer alle benodigde technische en operationele controlemaatregelen geïmplementeerd. Opmerking: onder ISMS wordt verstaan een verzameling beleidsregels en procedures voor systematisch management van gevoelige data van een organisatie, in dit geval die van de Opdrachtgever. Het ISMS minimaliseert risico’s en verzekert bedrijfscontinuïteit door pro-actief de impact te beperken bij een security breach.  |   |
| 10  | De Inschrijver gaat er mee akkoord dat Opdrachtgever zelf, dan wel derden in opdracht van Opdrachtgever, audits mag uitvoeren om te valideren dat (a) het ISMS voldoet en (b) de naleving van de adequate en tijdige implementatie van controlemaatregelen te toetsen.  |   |
| 11  | De Inschrijver maakt geen gebruik van derde partijen en locaties voor de hosting van de applicatie of indien dit wel het geval is dan dienen alle partijen vooraf bekend gemaakt te worden en ook te voldoen aan de eerder gestelde eisen en randvoorwaarden.  |   |
| 12  | Verwerking en opslag van informatie vindt alleen plaats in landen van EER of landen met een passend beschermingsniveau.  |   |
| 13  | Instelling mag een algehele of gedeeltelijke technische audit (laten) uitvoeren bij de Opdrachtnemer ingeval er geen ISA3402 type 2 verklaring of iets vergelijkbaars aanwezig is.  |   |
| 14  | Voor vertrouwelijke informatie wordt gebruik gemaakt van sterke authenticatie gebaseerd op minimaal twee factoren.  |   |
| 15  | Voor als vertrouwelijk of geheim geclassificeerde informatie dient het systeem alle verbindingen zowel intern als extern te versleutelen en voor als intern geclassificeerde informatie alleen de externe verbindingen. Het De applicatie maakt gebruik van veilige en actuele communicatie en versleutelingsstandaarden (zoals TLS, FTPS; Zie ook “ICT beveiligingsrichtlijnen voor Transport Layer Security (TLS) van het NCSC)[[2]](#footnote-3) |   |

* 1. Autorisatie

|  |  |  |
| --- | --- | --- |
| **Nr.**  | **Eis**  | **Beantwoording**  |
| 1  | De applicatie biedt de mogelijkheid tot het definiëren van gebruikersrollen. Autorisaties zijn gekoppeld aan een rol en een gebruiker kan 1 of meerdere rollen hebben. De gebruikersrollen kunnen door de beheerorganisatie worden gedefinieerd.  |   |
| 2  | De applicatie biedt de mogelijkheid om autorisaties op verschillende niveaus vast te leggen, maar met een zelfde functie. Voorbeeld cijferinvoer: * Een examinator (gebruikersrol) mag alleen cijfers invoeren voor een specifiek vak.

Het secretariaat (gebruikersrol) mag cijfers invoeren voor alle vakken die horen bij die specifieke leerstoelgroep.   |   |
| 3  | Het systeem biedt de mogelijkheid om via autorisatie te regelen of gebruikers alleen data mogen raadplegen, of ook mogen invoeren, wijzigen of verwijderen.  |   |
| 4  | Het systeem biedt de mogelijkheid om de beschikbare functionaliteiten en menu-items door autorisatie in te richten (welke profielen kunnen welke onderdelen in de applicatie raadplegen / wijzigen).  |   |
| 5  | Bij het definiëren van gebruikersrollen is het mogelijk om de toegang en het recht op muteren te beperken tot gegevens van bijvoorbeeld een bepaalde opleiding, leerstoelgroep en/of vakken.  |   |
| 6  | Het systeem biedt de mogelijkheid om een overzicht te maken van toegewezen autorisaties.  |   |

1. https://sec.surf.nl/controls/ [↑](#footnote-ref-2)
2. Zie <https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1> [↑](#footnote-ref-3)