Vereisten Privacy & Security by Design IT-leveranciers/dienstverleners **VITO-703-WER-001-N**	Versie:1 Publicatiedatum:27/05/2025 Pagina 1 of 5

Autheurs huidige versie:	Charlotte Vanhoof; Kris Van de Water
Eigenaars:	Information Security Officer en DPO

1 DOEL

Met deze set van informatiebeveiligingsvereisten beoogt VITO dat Privacy en Security steeds geborgd worden doorheen de levensloop van een IT-oplossing.

VITO verwacht bij elke offerte en aanbod van een IT-oplossing dat een deskundige leverancier/opdrachtnemer spontaan de juiste maatregelen treft om veilige IT-diensten, software en IT-systemen op te leveren, te onderhouden en veilig uit dienst te nemen.

Het doel van dit document is om daarbij duidelijkheid te geven aan wat zowel VITO, als opdrachtgever, en de opdrachtnemer onder privacy en security by design verstaan. Door van bij de aanvang duidelijkheid te hebben over wie welke rol daarbij opneemt, wordt vermeden dat kwetsbare systemen worden opgeleverd en kunnen extra kosten doorheen de verdere levensloop vermeden worden.

2 TOEPASSINGSGEBIED EN DOELPUBLIEK

Vanuit VITO hechten we belang aan informatieveiligheid en hebben we vereisten gedefinieerd waaraan alle IT- diensten, software en IT-systemen (hierna IT-oplossing) die we vanuit VITO afnemen moeten voldoen.

Deze **vereisten zijn verplicht** voor nieuwe IT-oplossingen en bij wijzigingen aan een huidige implementatie van een reeds geleverde IT-oplossing.

3 WERKINSTRUCTIE STAPPEN

Binnen iedere inkoop/aanbesteding en contract mbt een IT-oplossing moet van bij de aanvang duidelijk zijn wie welke taken met betrekking tot informatiebeveiliging opneemt.

Waar relevant kunnen deze vereisten worden gehanteerd voor de beoordeling van de offerte of de uitvoering van de opdracht. Een IT-oplossing kan pas als opgeleverd worden beschouwd als aan deze 2 vereisten werd voldaan.

3.1 Privacy by Design

- Privacy By Design & Default: De leverancier/opdrachtnemer moet aandacht besteden aan privacy in elke fase van de ontwikkeling en het gebruik van een IT-oplossing.
- Gegevensbescherming: De leverancier/opdrachtnemer moet passende maatregelen nemen om persoonsgegevens adequaat te beschermen, in lijn met GDPR en andere relevante regelgeving.
- Minimale Gegevensverzameling: De leverancier/opdrachtnemer moet de IT-oplossing zo ontworpen hebben om alleen noodzakelijke gegevens te verzamelen, te gebruiken en te bewaren.
- Maximale gegevensbescherming: Standaard-instellingen moeten steeds uitgaan van de hoogste bescherming voor de betrokkenen.

3.2 Security by Design

- Security by design : De leverancier/opdrachtnemer zorgt ervoor dat de IT-oplossing is ontworpen met beveiliging als een kernaspect, van de architectuur tot de implementatie en gebruik. Het Open Web Application Security Project (OWASP) (open source-project rond computerbeveiliging) vertaalde deze pijlers in concrete security design principes.
- Risico gebaseerd: De leverancier/opdrachtnemer moet een gedocumenteerde risicoanalyse aanbieden die aangeeft hoe zij risico's hebben geïdentificeerd en beheersmaatregelen hebben genomen om deze te beperken.

Beide bovenstaande principes moeten bewaakt worden doorheen de volledige levenscyclus. **Daarbij moet er door de leverancier/opdrachtnemer in elke offerte en aanbod van IT-oplossing, minimaal beschreven** worden hoe onderstaande privacy en security aspecten worden ingeregeld. **Behoudens andersluidende of meer strikte bepalingen in het bestek, moet daarbij specifiek benoemd worden voor welke aspecten de leverancier/opdrachtnemer geen verantwoordelijkheid neemt en/of waar er extra kosten van toepassing kunnen zijn.**

1) Toegangsbeheer en Authenticatie

We waken over de identiteiten en autorisaties die toegang hebben tot onze omgeving.

- Authenticatie: De IT-oplossing is bij voorkeur integreerbaar met onze gecentraliseerde IT-oplossing voor identiteits-en toegangscontrole waarmee we inzetten op Single Sign-On (SSO).
- Sterke Authenticatie: De IT-oplossing moet multifactor-authenticatie ondersteunen, vooral voor gebruikers met beheerdersrechten.
- Rechtenbeheer: De IT-oplossing moet opgezet zijn conform de principes van 'least-privilege' en 'segregation of duty', waarbij er een autoriatiematrix aangeleverd wordt met welke rollen en rechten er zijn. Daarop moeten strikte procedures hanteerbaar zijn voor het verlenen, wijzigen en intrekken van specifieke rechten binnen de IT-oplossing.

2) Log-management en Auditeerbaarheid

Op basis van logging moeten de juiste events bewaard, gemonitord en gealarmeerd worden.

- Loggen van Toegang: De IT-oplossing moet alle toegangspogingen en acties (crud) van gebruikers en beheerders loggen en die logs bewaren voor auditing.
- Monitoring en alerting: Alle veiligheidsgerelateerde activiteiten (zoals toegangspogingen, wijzigingen en incidenten) moeten rapporteerbaar zijn, ook voor periodieke review.
- Zowel technische/systeemlogging, applicatieve logging en de logging van persoonsgegevens moeten worden bewaard conform de wettelijke vereisten.

3) Encryptie

We werken met moderne en veilige versleutelingsmechanismes en up-to-date encryptie-standaarden.

- Encryptie van Gegevens: Conform de dataclassificatie moeten zowel gegevens in rust (AES256) als gegevens in transit (Mozilla standard) versleuteld worden op basis van een recent protocol en algoritme.

4) Gegevensbeveiliging

We werken met systemen die onze gegevens veilig houden

- Back-up en Herstel: Er moet een back-up- en herstelbeleid zijn voor het geval van dataverlies of een incident.
- Segregatie: De IT-oplossing of services moeten veilig gesegmenteerd en logisch gescheiden zijn tov niet relevante assets of services.
- Remote Toegang: Toegang tot de VITO interne netwerk-omgeving verloopt enkel via de VITO VPN-toepassing waarmee interne bronnen die remote bereikt moeten worden, toegankelijk zijn in het kader van de opdracht of het ondersteunen van de IT-oplossing.

5) Vulnerability Management, Patching & Change Management

We werken met up to date besturingssystemen, software, services en firmware die ook gemonitord worden op kwetsbaarheden.

- Patch Management: De leverancier/opdrachtnemer moet de veilige werking van de IT-oplossing garanderen en eventuele afhankelijke componenten systematisch updaten en patchen om beveiligingsrisico's te minimaliseren.
- Vulnerability Management: De leverancier/opdrachtnemer moet procedures hebben voor het identificeren, evalueren en verhelpen van kwetsbaarheden in de IT-oplossing en hun systemen.
- Change Management : De leverancier/opdrachtnemer moet procedures hebben om de impact van wijzigingen onder controle te houden en een roll-back mogelijk te maken. Bij iedere grote update of nieuwe release moet de leverancier/opdrachtnemer testen uitvoeren die garanderen dat de wijzigingen de goede werking en veiligheid verzekeren.

6) Penetratietests en Compliance

We werken met systematisch geteste en performante systemen.

- Penetratietests: De leverancier/opdrachtnemer moet periodieke penetratietests uitvoeren om mogelijke beveiligingslekken in de IT-oplossing tijdig te identificeren. Minimaal moet de IT-oplossing daarbij de OWASP top 10 succesvol doorstaan. Daarbij gaan we uit van het principe dat 'critical' en 'high' kwetsbaarheden die naar boven komen doorheen de levensloop van een IT-oplossing, asap gemitigeerd worden. Voor 'medium' en 'low'-kwetsbaarheden volstaat een aanpak die het reguliere patch-management volgt.
- Externe Audits: De leverancier/opdrachtnemer moet regelmatig externe beveiligingsaudits uitvoeren en moet rapporten daarvan op verzoek kunnen delen.
- Compliance: De leverancier/opdrachtnemer moet rapportages kunnen verstrekken die aantonen dat de IT-oplossing voldoet aan GDPR- en NIS2-vereisten.
- Service-levels: De leverancier/opdrachtnemer zorgt voor periodieke (standaard maandelijks) rapportering van de afgesproken SLA's die betrekking hebben op VITO en specifiek de IT-oplossing waar de SLA betrekking op heeft. Laag scorende en niet-gehaalde SLA's worden voorzien van een actieplan ter verbetering en compensatie bij herhaling of ernstige onderbreking.

7) Continuïteit

We waken over de continuïteit van onze diensten en gegevens, ook bij afloop of vroegtijdige beëindiging van de opdracht.

- Continuïteit: De leverancier/opdrachtnemer moet borgen dat de continuïteit van de dienstverlening wordt gegarandeerd.
- Exit-plan: De leverancier/opdrachtnemer beschrijft hoe een exit of migratie naar een andere leverancier/opdrachtnemer zal verlopen, bv. Bij End of life van de IT-oplossing en/of bij afloop van de opdracht.
- Data-overdracht: De leverancier/opdrachtnemer beschrijft hoe data wordt overgedragen en hoe de data na overdracht wordt behandeld/vernietigd conform GDPR.
- Licentie-overdracht: De leverancier/opdrachtnemer beschrijft of en hoe licenties zullen worden behandeld bij wijziging of bij afloop van de opdracht.

4 COMMUNICATIE VEREISTEN

Publiek op vito.be beschikbaar als onderdeel van de inkoopvoorwaarden waarvan het integraal deel uitmaakt.

5 AANVERWANTE DOCUMENTEN EN REFERENTIES

Referentie	Titel/omschrijving
VITO-701-RIC-002-N	Inkoopvoorwaarden

6 HISTORIEK

Versie	Datum	Reden
1	27/5/2025	NIS2 en GDPR compliancy