

Basisvereisten ICT voor leveranciers

Inhoud

1.	Doelstelling.....	3
2.	Definities.....	3
3.	Beheersprincipes.....	3
	Authenticatie & autorisatie	3
	Gebruikersbeheer.....	3
	Acceptatietesting.....	4
4.	Connected Device	4
5.	Servers.....	4
	Operating System.....	4
	Windows Server	5
	GNU/Linux based.....	5
	Virtuele servers.....	5
	Hypervisor en resources	5
	Back-up	6
	Operating System	6
	Fysieke servers	6
	Hardware.....	6
	Back-up	7
	Operating System	7
6.	Server software.....	7
	Databases	7
	Microsoft SQL Server – Shared Server	8
	Microsoft SQL Server – Dedicated Server.....	8
7.	Clients	9
	Back-up	9
	Client Hardware.....	9
	Network Access.....	9
	Microsoft Windows Operating System.....	9

Client Software	9
Webapplicatie.....	9
Thick Client.....	9
Mobiele App.....	10
Cloudapplicaties.....	10
8. Integraties met andere componenten	12
9. Beleid voor het melden van kwetsbaarheden	12
Verplichtingen van leveranciers	12
Reactie en samenwerking.....	12
Contractuele verankering	13
Controle en evaluatie.....	13

Versiebeheer

Versie	Datum	Auteur	Opmerking
1.0	08/11/2023	Koenraad Nobels	Opmaak 1 ^{ste} versie
2.0	31/03/2025	Annelore Van Eeghem	Kwetsbaarheden melden
3.0	03/03/2026	Annelore Van Eeghem	Cloudapplicaties en exit strategie
4.0	29/05/2026	Annelore Van Eeghem	Toevoeging Operating System: De implementator gebruikt steeds een door de vendor actief onderhouden besturingssysteem, gedurende de hele levensduur van de server.

1. Doelstelling

Dit document beschrijft eisen aan nieuwe componenten die potentieel aan onze ICT-omgeving toegevoegd worden en heeft als doel om leveranciers contractueel te verplichten om beveiligingskwetsbaarheden in hun producten en diensten tijdig te melden. Hierdoor kan de organisatie proactief handelen om risico's te beperken en de continuïteit en veiligheid van de ICT-omgeving te waarborgen. Deze bepalingen stellen ons in staat onze zeer diverse omgeving gestructureerd te beheren en beveiligen.

Dit document is van toepassing op alle leveranciers die software, hardware, of ICT-diensten leveren aan en maakt integraal deel uit van de contractuele afspraken met deze partijen.

2. Definities

ICT Component: groep van clients/client software en/of servers/server software die samen een applicatie of service aanbieden aan de eindgebruiker.

Connected device: host gekoppeld aan een netwerk beheerd door ICT. Overkoepelend voor clients en servers.

Client: host binnen het client netwerk, doorgaans fysiek en met rechtstreekse interactie door de eindgebruiker.

Voorbeelden: Echotoestel, RF-scanner, thermostaat, badgelezer, ...

Server: host binnen het server netwerk, doorgaans enkel rechtstreeks benaderd door leverancier en ICT.

Voorbeelden: applicatieserver voor 3D-reconstructie van beelden, webserver voor interne webapplicatie, ...

3. Beheersprincipes

Authenticatie & autorisatie

Binnen de organisatie gebruiken we Microsoft Active Directory voor authentication en authorization van gebruikers. Hierbij werken we steeds met recursief geneste group memberships.

Binnen Microsoft Azure werken we met Azure Active Directory waarmee we onze interne manier van werken verderzetten naar de Microsoft cloud applicaties.

Gebruikersbeheer

Gebruikers aanmaken en verwijderen gebeurt geautomatiseerd vanuit onze IAM-oplossing. Doorgaans verloopt dit d.m.v. Active Directory group memberships.

Indien de applicatie daar geen ondersteuning voor biedt, verwachten we een alternatieve, gedocumenteerde API om dit te kunnen automatiseren.

Acceptatietesting

Voor componenten met grote afhankelijkheid bij de eindgebruikers, werken we steeds met een acceptatie omgeving naast de productieomgeving voor het valideren van updates en belangrijke wijzigingen.

4. Connected Device

Deze rubriek is van toepassing op alle delen van de component die verbonden zijn met een door ICT beheerd netwerk.

Onze omgeving hanteert een strikte scheiding tussen clients en servers, met verdere segmentatie tussen verschillende groepen clients en servers onderling.

De standaard policy voor een component staat volgende zaken toe:

- Verbindingen tussen servers, deel van dezelfde component, zonder beperkingen.
- Verbindingen tussen clients en servers van dezelfde component zonder beperking.
- Uitgaande verbindingen met interne, basis netwerkservices (DHCP, DNS, NTP).
- Uitgaande verbindingen met externe hosts op basis van een aangeleverde lijst met koppels van URL met protocol.

Optioneel kunnen volgende zaken toegevoegd worden:

- Verbindingen tussen clients binnen hetzelfde segment zonder beperkingen.
- Toegang tot eigen component d.m.v. VPN, beheerd door ICT.
- Verbindingen met componenten van andere partijen op basis van een aangeleverde lijst met koppels van host met protocol.

Opzetten van een eigen LAN/WLAN naast de door ICT beheerde netwerkinfrastructuur is niet toegestaan.

Permanente tunnels voor ongecontroleerde toegang van buitenaf tot de component, hetzij voor support door de implementator, hetzij voor gebruik door de eindgebruiker, zijn niet toegestaan.

Bij gebruik van internal networking (bijvoorbeeld d.m.v. Docker of een tweede netwerk), gebeurt dit binnen subnet 10.255.0.0/16. Andere subnetten zijn voorbehouden aan de organisatie.

5. Servers

Deze rubriek is van toepassing op alle delen van de component die verbonden zijn met het datacenter netwerk.

Operating System

De implementator gebruikt steeds een door de vendor actief onderhouden besturingssysteem, gedurende de hele levensduur van de server.

Windows Server

Windows Server machines worden opgenomen in ons Active Directory domain.

Windows Server machines krijgen steeds een set basisinstellingen d.m.v. Group Policy.

Windows Server machines zijn voorzien van een EDR agent voor bescherming tegen malware.

Windows Updates worden structureel toegepast door ICT.

De implementator krijgt een eigen domain account met local administrator rechten op de relevantie machines.

Alle processen/services draaien onder het domain account van de implementator.

Het local administrator account is voorbehouden aan ICT.

Onze standaard disk layout wordt gerespecteerd:

- C disk: voorbehouden aan het besturingssysteem. Bijkomende software op deze disk is niet toegestaan.
- D disk: te gebruiken voor installatiebestanden van de implementator.
- Optioneel kunnen bijkomende disken voorzien worden naargelang gebruiksdoel en applicatiearchitectuur.

GNU/Linux based

ICT verwacht toegang tot een account met admin rechten voor gerichte troubleshooting en het voorzien van gepaste monitoring. Dit mag 'root' zelf zijn of een account dat root toegang kan verkrijgen d.m.v. permission escalation.

Onze standaard disk layout wordt gerespecteerd:

- /boot physical disk met 1 primaire partitie
- / physical volume (zonder partities) met 1 logical volume
- swap physical volume (zonder partities) met 1 logical volume
- Optioneel kan een bijkomend physical volume voorzien worden dat verder opgedeeld wordt in logical volumes naargelang gebruiksdoel en applicatiearchitectuur.

Updates voor het besturingssysteem en packages worden structureel toegepast door ICT of de implementator.

Virtuele servers

Dit is de standaard manier waarop we servers voorzien binnen onze omgeving.

Hypervisor en resources

Virtuele servers draaien we op een intern VMware vSphere platform. Dit platform zorgt voor een basisbescherming tegen hardware falen.

De specificaties van de virtuele machine dienen in lijn te liggen met de workload die de machine zal verrichten.

Resource reservation is niet toegestaan. Wij schalen het platform zodat er steeds voldoende resources ter beschikking zijn bij normale werking.

Live vMotion voor verdeling van de workload of het uitvoeren van onderhoud aan de onderliggende hardware nodes kan te allen tijde gebeuren.

Binnen elke virtuele server verwachten we de aanwezigheid van VMware Tools voor een ondersteund besturingssysteem.

Opslag van grote hoeveelheden ongestructureerde data gebeurt op een SMB/NFS share rechtstreeks op de centrale storage.

De werking van een virtuele server mag niet afhankelijk zijn van een hardware license key.

Back-up

Virtuele machines krijgen automatisch een dagelijkse snapshot back-up op niveau van de hypervisor.

Optioneel zijn er script triggers beschikbaar op volgende stappen in het back-up proces d.m.v. een agent voor ondersteunde besturingssystemen:

- Pre snapshot
- Post snapshot
- Post back-up (na datatransfer van snapshot inhoud)

Operating System

Windows Server

Vanuit ICT voorzien we virtuele machines standaard met de actuele versie van Microsoft Windows Server. Optioneel kunnen we werken op basis van de voorgaande indien deze nog minstens 3 jaar ondersteuning geniet.

GNU/Linux based

Andere operating systems zijn mogelijk indien aangeleverd, inclusief licenties.

Fysieke servers

In specifieke gevallen kan een fysieke server in onze omgeving opgenomen worden. De meest gebruikelijke redenen zijn:

- Extreem resource gebruik
- Gebruik van speciale hardware

Hardware

Fysieke hardware voldoet aan volgende specificaties:

- 19inch rack form factor
- Ingebouwde koeling volgt de flow van de racks: front to back.
- Elke component is voorzien van bijpassende rails
- Elke component is voorzien van een redundante PSU met C14 connector

- Elke component is voorzien van redundante aansluitingen voor het data netwerk d.m.v. RJ45/SFP+ connectors

Support gerelateerd aan de hardware verloopt via de implementator, niet rechtstreeks met de hardware vendor.

Optioneel kunnen meerdere redundante hardware componenten verdeeld worden over 2 of 3 fysiek gescheiden locaties, afhankelijk van de architectuur.

ICT verwacht toegang tot de ingebouwde management software van de hardware voor monitoring, power management en consoletoegang.

Onze datacenters zijn enkel toegankelijk onder begeleiding van ICT.

Back-up

Optioneel kan een selectie aan data op de fysieke server opgenomen worden in onze standaard back-up mits ondersteuning voor de back-up agent door het besturingssysteem. Dit onder voorbehoud dat de grootte van de dataset aanvaardbaar blijft.

Operating System

Te bepalen door leverancier, eigen licenties te voorzien.

6. Server software

Software draait steeds onder het aangeleverde service account.

Software draait steeds non-interactive. Er mag geen aangelogde Windows sessie nodig zijn voor normale werking.

Het geheel van processen op servers komt vanzelf in een correct werkende staat na een reboot, uitgevoerd op het niveau van het besturingssysteem.

Log files zijn beperkt in grootte, roteren automatisch en worden slechts bijgehouden gedurende een beperkte termijn naargelang hun nut.

Tijdelijke werkbestanden worden automatisch opgekuist.

Databases

Binnen de omgeving standaardiseren we onze databases op Microsoft SQL Server en PostgreSQL (voor specifieke doeleinden).

Oracle Database is enkel aanvaardbaar indien vanuit de implementator voorzien van een ASFU licentie, gezien de hosting op onze VMware infrastructuur.

Databases worden niet als fileserver gebruikt. Grote hoeveelheden ongestructureerde data hoort thuis op een filesystem.

Microsoft SQL Server – Shared Server

Doorgaans plaatsen we databases bij op één van onze bestaande consolidatie servers naargelang het gebruikspatroon.

Binnen databases voorzien we het relevante service account standaard van de rechten 'db_datareader', 'db_datawriter' en 'db_ddladmin'.

Optioneel kan dit uitgebreid worden naar 'db_owner' indien bepaalde instellingen op niveau van de database gerespecteerd worden.

Bijkomende rechten op niveau van de SQL Server instance (zoals 'sysadmin') zijn niet mogelijk.

De database naam is vrij te kiezen door ICT of ten minste te voorzien van een prefix.

Back-up

ICT voorziet standaard in dagelijkse back-ups van de database.

ICT voorziet standaard in periodieke back-ups van transaction logs.

Index maintenance

ICT voorziet standaard in dagelijks onderhoud van de database met:

- Index rebuilds (offline)
- Statistics updates
- Page checksum validation

Database creatie

De creatie van de databases verloopt volgens één van deze opties:

- Database wordt manueel aangemaakt door ICT
- Gebruikersaccount van implementator krijgt op niveau van de SQL Server instance de rechten 'db_creator' voor geautomatiseerde creatie van de database

Microsoft SQL Server – Dedicated Server

In uitzonderlijke gevallen kan ICT voorzien in een dedicated SQL Server instance voor de nieuwe component. Meestal gebeurt dit om volgende redenen:

- De workload van de server is dusdanig hoog dat andere databases gestoord worden in hun werking.
- Ongebruikelijke software componenten of integraties zijn nodig op de machine zelf.
- Specifieke rechten op SQL Server instance niveau zijn vereist.

Back-up

ICT voorziet standaard dezelfde zaken als voor onze shared server, tenzij anders overeengekomen.

Index maintenance

ICT voorziet standaard dezelfde zaken als voor onze shared server, tenzij anders overeengekomen.

7. Clients

Deze rubriek is van toepassing op alle delen van de component die verbonden zijn met het client netwerk.

Back-up

ICT voorziet GEEN back-ups van clients. Voor de organisatie belangrijke data hoort thuis op een server.

Client Hardware

Het client toestel gebruiken DHCP voor het ontvangen van een IP-adres, alsook de te gebruiken DNS en NTP servers.

Indien nodig kan d.m.v. een DHCP reservatie een vast IP-adres ingesteld worden.

Het client toestel beschikt over een RJ45-connector voor de verbinding.

Het client bepaalt d.m.v. autonegotiation een de gewenste instellingen voor snelheid en duplex.

Network Access

Gebruik van DHCP is belangrijk voor de correcte werking van de netwerkauthenticatie.

Clients verbinden met het draadloos netwerk d.m.v. IEEE802.1x EAP-TLS authenticatie op basis van een door ICT aangeleverd certificaat. De huidige versie van IEEE802.1x. is deel van de Wi-Fi standaard sinds 2004.

Clients verbinden met het bekabeld netwerk d.m.v. IEEE802.1x EAP-TLS authenticatie op basis van een door ICT aangeleverd certificaat.

Per uitzondering kan die gebeuren op basis van het MAC-adres.

Microsoft Windows Operating System

Clients met een door Microsoft ondersteund Windows besturingssysteem kunnen optioneel opgenomen worden in ons Active Directory domein.

Standaard bij gebruik van domain authentication met andere componenten.

Client Software

Webapplicatie

De applicatie is compatibel met Microsoft Edge (Stable/Extended Stable release channel).

De applicatie vereist geen specifieke Group Policy settings voor Microsoft Edge.

De applicatie vereist geen plug-ins of registratie van custom content handlers.

Thick Client

De software is compatibel met de door Microsoft ondersteunde Windows versies. Dit gedurende de hele duur van het contract.

De software is compatibel met de door Microsoft ondersteunde Windows Server versies in combinatie met meerdere, gelijktijdige gebruikerssessies op hetzelfde systeem. Dit gedurende

de hele duur van het contract.

Enkel van toepassing op software aangeboden via de Citrix-omgeving.

De software kan zonder menselijke interactie verdeeld worden d.m.v. Microsoft System Center Configuration Manager (SCCM) of Microsoft Application Virtualisation (App-V).

Standaard is een XDR-oplossing actief op elk werkstation. Indien de software voor de XDR agent risicovolle acties uitvoert, dient deze met een identificeerbaar certificaat gesigned te zijn voor whitelisting.

De software werkt correct bij gebruik zonder administrator rechten binnen het besturingssysteem.

De software stelt geen eisen aan de taal- en regio-instellingen van het besturingssysteem.

De software handelt authenticatie af op basis van Active Directory, los van de gebruikerssessie binnen het besturingssysteem.

De software handelt autorisatie af op basis van Active Directory group memberships, en biedt daarbij ondersteuning voor meermaals geneste groepen.

De software is compatibel met de door Microsoft ondersteunde versies van Office en Office 365.

Mobiele App

De applicatie is compatibel met alle, door Google ondersteunde Android versies. Dit gedurende de hele duur van het contract.

De applicatie kan verdeeld worden als APK via onze Mobile Device Management (MDM) tool.

Cloudapplicaties

Beschikbaarheid en continuïteit (Uptime en SLA)

De leverancier moet aantoonbare garanties bieden inzake beschikbaarheid en continuïteit:

- duidelijk gedefinieerde SLA met minimale uptimepercentages
- transparante afspraken rond onderhoudsvensters en geplande downtime
- escalatieprocedures en responstijden bij incidenten
- afspraken rond business continuity en disaster recovery (RTO/RPO)

Deze vereisten zijn noodzakelijk gezien Vitaz geen directe controle heeft over de onderliggende infrastructuur van de clouddienst.

Back up en herstel van gegevens

Voor elke cloudapplicatie moeten expliciete afspraken bestaan over gegevensbescherming:

- wie is verantwoordelijk voor back ups (leverancier, Vitaz of gedeeld)
- frequentie van back ups en bewaartermijnen ervan
- testbaarheid en aantoonbaarheid van restore procedures
- beschikbaarheid van back ups bij contractbeëindiging of incidenten.

Louter vertrouwen op interne back upmechanismen van de leverancier is onvoldoende zonder contractuele borging.

Databeheer en gegevenslocatie

De clouddienst moet voldoen aan expliciete vereisten inzake databeheer:

- duidelijkheid over gegevenslocatie (EU / EER / derde landen)
- toepassing van GDPR conforme waarborgen bij eventuele doorgifte buiten de EU
- eigenaarschap van data blijft te allen tijde bij Vitaz
- afspraken rond dataclasses (gevoelige, medische of persoonsgegevens)

Deze elementen moeten afgestemd worden met juridische dienst en DPO vóór aankoop.

Informatieveiligheid en toegangsbeheer

De leverancier moet aantonen dat de clouddienst voldoet aan gangbare beveiligingsprincipes:

- ondersteuning van sterke authenticatie (bij voorkeur MFA)
- rol- en toegangsbeheer afgestemd op het least privilege principe
- logging en auditmogelijkheden
- meldingsplicht en procedures bij beveiligingsincidenten.

Deze vereisten zijn essentieel in het kader van informatieveiligheid en NIS2 verplichtingen.

Supply chain en afhankelijkheden

Bij cloudoplossingen moet expliciet inzicht bestaan in afhankelijkheden:

- gebruik van subverwerkers of derde cloudplatformen
- transparantie over wijzigingen in de supply chain
- recht op kennisname en bezwaar bij wijzigende subverwerkers
- inschatting van risico's bij vendor lock in.

Dit is noodzakelijk om zowel operationele als juridische risico's te beheersen.

Lifecycle, wijzigingsbeheer en roadmaps

De leverancier dient duidelijke afspraken te maken over:

- wijzigingsbeheer en communicatie bij functionele of technische wijzigingen
- end of life en end of support termijnen
- inzage in productroadmap indien beschikbaar.

Onverwachte wijzigingen kunnen immers een directe impact hebben op processen en integraties binnen Vitaz.

Exitstrategie

Bij elke aankoop van een cloudapplicatie dient een exitstrategie te worden voorzien en beoordeeld. Deze exitstrategie moet minimaal volgende elementen bevatten:

- De wijze waarop data van de organisatie kan geëxporteerd worden bij het beëindigen van de overeenkomst.

- De formaten waarin data beschikbaar wordt gesteld en de compatibiliteit met andere systemen.
- De termijn en voorwaarden waaronder data beschikbaar blijft na beëindiging van de dienst.
- Afspraken rond de definitieve verwijdering van data na overdracht.
- Eventuele bijkomende kosten verbonden aan datamigratie of -verwijdering.
- Impact op integraties en afhankelijkheden met andere systemen.

Contractuele borging

Alle bovenstaande vereisten moeten:

- Opgenomen zijn in het contract en/of SLA
- Verifieerbaar zijn vóór finale goedkeuring
- Gekoppeld worden aan de exitstrategie

8. Integraties met andere componenten

De component maakt gebruik van standaard protocollen binnen de industrie of API's voor uitwisseling van informatie met andere componenten.

Protocollen maken steeds gebruik van de door IANA gestandaardiseerde poorten.

Fileshares worden enkel opgezet in samenspraak met ICT. ICT zorgt dan voor een overeenkomstige security group binnen Active Directory met de relevante gebruikers als lid. Shares met rechten voor iedereen zijn niet toegestaan.

9. Beleid voor het melden van kwetsbaarheden

Verplichtingen van leveranciers

- Leveranciers zijn verplicht om beveiligingskwetsbaarheden in hun producten of diensten die in gebruik zijn te melden.
- De melding moet ten minste de volgende informatie bevatten:
 - Een beschrijving van de kwetsbaarheid
 - De potentiële impact op de systemen
 - Tijdslijn en plan voor mitigatie of oplossing
 - Eventuele tijdelijke maatregelen om de risico's te beperken.

Reactie en samenwerking

- Na melding van een kwetsbaarheid wordt een impactanalyse uitgevoerd door het ICT-team.
- Leveranciers dienen proactief samen te werken om de kwetsbaarheid zo snel mogelijk te verhelpen.

- In geval van ernstige kwetsbaarheden met significante impact kunnen we besluiten om tijdelijke aanvullende beveiligingsmaatregelen te eisen of de samenwerking op te schorten.

Contractuele verankering

Dit document wordt opgenomen in de contracten met leveranciers als een bindende verplichting.

Niet-naleving kan leiden tot contractuele sancties, waaronder boetes, aansprakelijkheid voor schade, en in ernstige gevallen de beëindiging van de samenwerking.

Controle en evaluatie

We behouden het recht voor om periodieke audits uit te voeren om naleving van dit beleid te controleren.

Dit beleid wordt jaarlijks geëvalueerd en indien nodig aangepast aan nieuwe dreigingen en regelgeving.