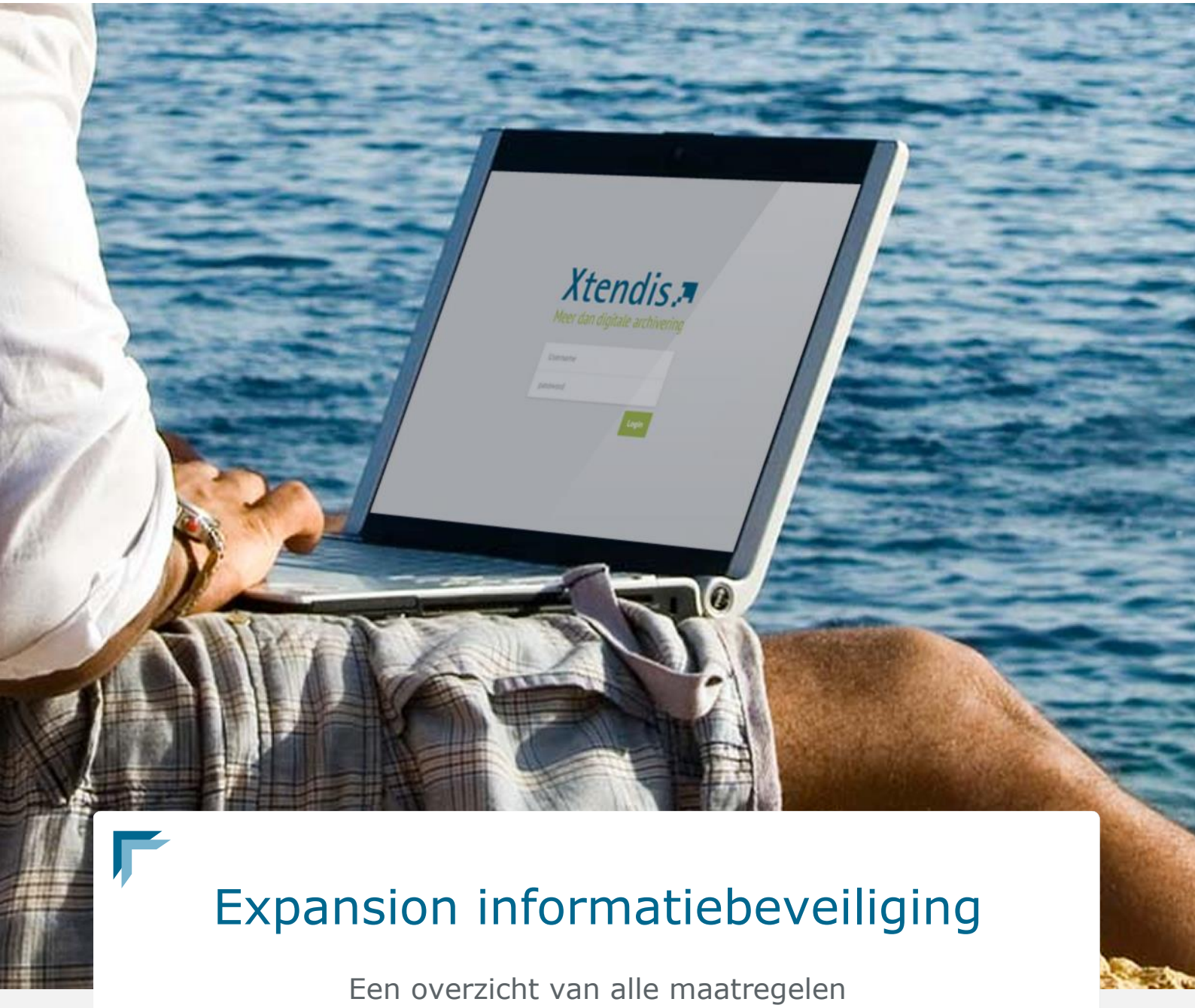


Expansion informatiebeveiliging

Een overzicht van alle maatregelen

Opgesteld door: Wim Vis

Rotterdam, 21 november 2018

Inhoud

1. Inleiding

Informatiebeveiliging staat centraal in de dienstverlening van Expansion. Onze klanten kunnen erop vertrouwen dat hun documenten en gegevens altijd veilig zijn, ongeacht of gebruik wordt gemaakt van een on-premises- of cloudoplossing.

"Informatie-beveiliging staat centraal"

In dit document wordt beschreven op welke wijze Expansion invulling geeft aan informatiebeveiliging. De maatregelen bevinden zich op verschillende niveaus:

- Organisatie
- Product (Xtendis)
- Infrastructuur (Cloud/datacenter)
- Zekerstelling en garanties

2. Organisatie

Expansion B.V. wenst een beeld uit te stralen en te handelen als een organisatie die te allen tijde streeft naar continuïteit en het vertrouwelijk en integer omgaan met klantinformatie. Expansion B.V. voldoet daarbij aan de geldende wet- en regelgeving. Om dit te kunnen realiseren heeft Expansion B.V. een managementsysteem opgezet, waarin alle kritische momenten op het gebied van informatiebeveiliging zijn geborgd. De werking van het informatiebeveiligingsmanagementsysteem kan door onafhankelijke partijen worden geverifieerd en bevestigd.

2.1. NEN-ISO 27001:2013

Expansion is NEN-ISO 27001:2013 gecertificeerd. Een belangrijk onderdeel van de certificering dat onlosmakelijk verbonden is met het ISO-certificaat zelf is de Verklaring van Toepasselijkheid (VvT). Dit is een document met daarin opgenomen voor elk van de ongeveer 160 beheersmaatregelen of deze maatregel van toepassing is voor Expansion of niet. Omdat Expansion ervoor heeft gekozen haar gehele organisatie en dienstverlening te certificeren en niet alleen delen van de organisatie, zijn bijna alle maatregelen van toepassing. Naast dit overzicht is ook vermeld met welke procedures (vastgelegd in het Blue Book, het Expansion ISO Handboek) dit bereikt wordt en er is ook een overzicht welke maatregelen te maken hebben met welke eisen uit de ISO27001:2013.

2.2. ISAE 3402-Type II

Met het verkrijgen van de ISAE 3402 Type II verklaring wil Expansion nog een stap verder gaan. Deze verklaring toont aan dat Expansion in controle is over de maatregelen die zij neemt in het kader van de informatiebeveiliging. Expansion maakt hiervoor aantoonbaar op welke wijze de maatregelen worden ingevuld.

3. Product

Alle oplossingen van Expansion zijn gebaseerd op het systeem Xtendis.

Vanzelfsprekend staat ook binnen Xtendis alles in het teken van informatiebeveiliging. De kernfunctie van Xtendis is het bewaken van de digitale duurzaamheid van documenten. Digitale duurzaamheid houdt in dat de integriteit en authenticiteit van de documenten gewaarborgd is. Ook stelt het eisen aan de toekomstvastheid van de archiveringsoplossing. In de volgende subparagrafen wordt dieper ingegaan op deze begrippen en worden andere Xtendiskenmerken beschreven op het gebied van informatiebeveiliging.

3.1. Integriteit

De integriteit van een document heeft betrekking op de beveiliging van de inhoud. Xtendis geeft hier als volgt invulling aan:

- Alle documenten worden in Xtendis vastgelegd in een niet-manipuleerbaar bestandsformaat. Binnen Xtendis zijn geen functies beschikbaar om deze bestanden te wijzigen.
- Documenten worden nooit overschreven. Ieder document dat aan Xtendis wordt aangeboden, wordt als een unieke entiteit beschouwd.
- Documenten worden door Xtendis afgeschermd van directe toegang door gebruikers. Het toevoegen en raadplegen van documenten verloopt altijd via Xtendis-componenten. Het is dus niet mogelijk om op het niveau van het besturingssysteem (buiten Xtendis om) bestanden te wisselen. Indien mutaties plaatsvinden, zullen deze altijd vanuit Xtendis aangestuurd worden. Deze mutaties zijn binnen Xtendis traceerbaar.

De mate waarin aan deze integriteit wordt voldaan kan in Xtendis worden gecontroleerd (zie paragraaf Integriteitscontrole).

3.2. Authenticiteit

Met authenticiteit wordt de betrouwbaarheid van de originaliteit en de herkomst van een document bedoeld.

Xtendis wijst aan ieder document dat wordt vastgelegd de volgende onwijzigbare eigenschappen toe: aanmaakdatum, indexeerdatum, mutatiedatum, eigenaar, bron, batch_id, document_id, document_guid. Deze eigenschappen stellen de gebruikersorganisatie in staat om op ieder willekeurig document controles uit te voeren op de authenticiteit.

3.3. Autorisaties

Binnen Xtendis kunnen op geavanceerde wijze rechten worden toebedeeld aan gebruikers en systemen. Rechten kunnen zich op de volgende niveaus bevinden:

- Systeem
- Archieven
- Functies
- Zones

Zones zijn onderdelen van archieven die door klanten kunnen worden gedefinieerd. Door een document in een zone te plaatsen wordt automatisch bepaald welke gebruikersgroepen rechten hebben (raadplegen, muteren, verwijderen). Ook kan op deze manier worden bepaald welke systemen documenten uit Xtendis kunnen ophalen. In de praktijk wordt deze functionaliteit vaak toegepast om te bepalen welke documenten uit Xtendis op portalen mogen worden getoond en welke juist niet.

Binnen Xtendis wordt door middel van rechten bepaald welke medewerkers documenten mogen invoeren en/of verwijderen (deels of volledig).

Xtendis kan ten onrechte uitgevoerde verwijderacties binnen 14 dagen herstellen.

3.4. Identity Management

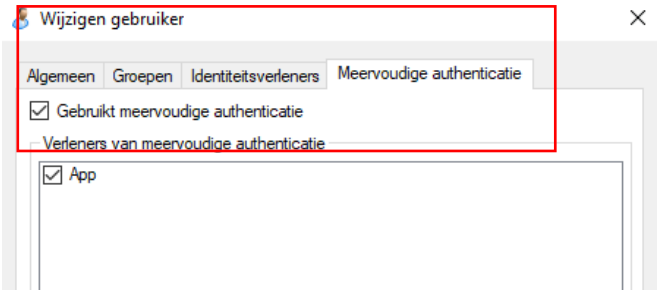
Het gebruikersbeheer in Xtendis voldoet aan de hoogste veiligheidseisen. Zo kan de sterkte van het wachtwoord dat een gebruiker toepast worden afgedwongen. Het systeem heeft een wachtwoord-vergeten procedure waarmee gebruikers op een veilige manier een nieuw wachtwoord kunnen kiezen.

Het rechtenbeheer in Xtendis kan worden gekoppeld aan generieke Identity Management (IdM) oplossingen die binnen organisaties worden gebruikt. Dit kunnen zowel On-Premises (Active Directory (AD))- als Cloud (Office 365, Google, iWelcome, ADFS)-oplossingen zijn.

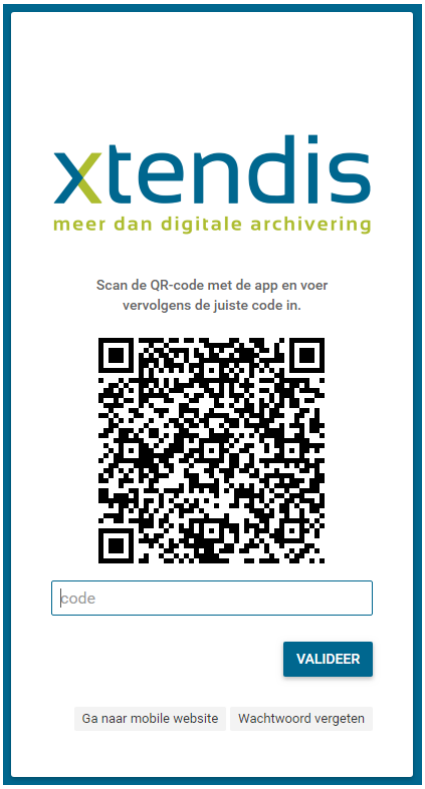
Gebruikers worden vanuit IdM omgevingen automatisch in Xtendis aangemaakt en mutaties worden automatisch verwerkt. Zo kan centraal beheerd worden welke medewerkers toegang tot Xtendis krijgen. Indien een medewerker uit dienst gaat, hoeft dit alleen binnen IdM te worden bijgewerkt, waarna Xtendis voor de betreffende gebruiker automatisch niet meer toegankelijk zal zijn.

3.5. 2-factor authenticatie

Ondanks dat Xtendis veelal gekoppeld wordt aan *Identity-Management-systemen* ondersteunt Xtendis ook 2-factor authenticatie.



De vereiste voor meervoudige authenticatie kan per gebruiker ingesteld worden. Hiervoor is in de cockpit een extra tab toegevoegd bij de Gebruikersinstelling waar deze functie aangezet kan worden.



Bij het eerste bezoek aan Xtendis krijgt de gebruiker een QR-code in de Xtendis-Web-Interface te zien. De gebruiker dient deze QR-code eenmalig met een Authenticator app te scannen (bijvoorbeeld Google Authenticator).
Deze app genereert periodiek een code die de gebruiker bij het inloggen dient in te geven als de sessie is verlopen.

De app onthoudt de link met Xtendis, dus het scannen van de QR-code is alleen de eerste keer nodig.

3.6. Audit Trail

Met behulp van de Xtendis Audit Trail kunnen alle handelingen binnen het systeem worden geregistreerd. Zo kan altijd de bron van iedere gegevensmutatie binnen het systeem achterhaald worden. Op de registraties kunnen rapportages worden gedraaid, waarbij handelingen op basis van uiteenlopende entiteiten kunnen worden gepresenteerd. Daarnaast kan bij ieder document een overzicht van geregistreerde handelingen worden opgevraagd: welke gebruiker heeft welke handeling op welk moment uitgevoerd?

3.7. Toekomstvastheid

Om de toekomstvastheid van de documenten te waarborgen wordt binnen Xtendis zoveel mogelijk gebruik gemaakt van industriestandaarden. Zowel de documenten als de metagegevens worden vastgelegd in bestandsformaten die wereldwijd worden toegepast. Dit betekent dat organisaties die Xtendis gebruiken onafhankelijk zijn van de leverancier om op lange termijn documenten te kunnen raadplegen en reproduceren. Een ander voordeel is dat relatief eenvoudig conversies kunnen worden uitgevoerd naar nieuwe standaarden.
De architectuur van Xtendis zorgt verder voor een onafhankelijkheid van specifieke opslagmedia. Dit geeft organisaties de garantie dat de documenten ook met toekomstige opslagtechnieken vastgelegd kunnen worden.

3.8. OWASP

Expansion houdt de belangrijkste security risico's zoals gepubliceerd door het Open Web Application Security Project (OWASP Top 10 Application Security Risks) nauwlettend in de gaten en past indien nodig Xtendis hierop aan.

3.9. Hashing, encryptie en andere toegepaste technieken

In Xtendis worden onderstaande technieken ingezet voor beveiliging. Per techniek wordt de Xtendis taak genoemd waarin deze wordt toegepast:

- Symmetrische encryptie: voor veilige opslag van gegevens in het Xtendis Beheer, zoals servernamen, gebruikersnamen en wachtwoorden.
- Asymmetrische encryptie:
    - met authenticatie voor:
        - Connection strings
        - Procesconfiguraties
        - Externe lookup configuraties
        - AD logon configuraties
        - Wachtwoord wijzigen
        - Wachtwoord resetten
    - met authenticatie met beperkte geldigheid voor:
        - Aanmelden, door geauthentiseerd onderdeel
        - Licentie
        - Wachtwoord vergeten proces
- Hashing, wordt toegepast voor wachtwoorden met SALT. Daarnaast worden Controle Hashes toegepast op de documentbestanden.
- Vertragingen: bij meerdere inlogpogingen wordt een vertraging toegepast wat de kans op hacks verlaagt.

In aanvulling op de encryptie binnen Xtendis, kan ook nog generieke encryptie worden toegepast. De volumes waarop de documenten worden opgeslagen kunnen worden gecodeerd door bijvoorbeeld Windows Encrypting File System (EFS). Voor de metadata (die in een SQL Server database worden vastgelegd) kan SQL Server Total Database Encryption (TDE) worden toegepast. Beide vormen van encryptie zijn transparant voor Xtendis.

3.10. Integriteitscontrole

Met behulp van de toegepaste Controle Hashes op de documentbestanden, kan in Xtendis pro-actief de integriteit van documenten worden gecontroleerd. Door te kiezen voor de beheerfuntie Herberekenen Hashes zal Xtendis een overzicht verstrekken van documenten waarvan de hash niet meer klopt. Voor deze documenten geldt dus dat hun inhoud op ongeautoriseerde wijze gewijzigd en kunnen vervolgens geanalyseerd worden.

4. Infrastructuur

Bij gebruik van de Xtendis Cloud oplossing wordt het systeem vanuit het Expansion datacenter aangeboden.

Ook hierin worden maximale veiligheidsmaatregelen getroffen.

Expansion heeft een virtueel datacenter binnen twee duurzame, carrier-neutrale datacenters van de organisatie Previder. Beide datacenters hebben een aantal unieke eigenschappen, die voor extreme bedrijfszekerheid zorgen. De stroomvoorziening, koeling en connectivity zijn volledig redundant uitgevoerd. De beveiliging staat op het hoogste niveau. Previder is ISO 27001, ISO 14001 en ISO 9001 gecertificeerd. De opzet van de Previder datacenters stelt Expansion in staat om Xtendis met de hoogst mogelijke redundancy aan te bieden.

De locatie van beide fysieke datacenters bevindt zich binnen Nederland.

Back-ups worden ingevuld middels snapshots die iedere dag worden gemaakt en standaard zeven dagen beschikbaar blijven. De back-ups worden net als de productieomgevingen verspreid over twee fysiek gescheiden locaties opgeslagen.

Communicatie van en naar de online Xtendis omgeving vindt plaats via beveiligde protocollen.

Optioneel kan gebruik worden gemaakt van IP Whitelisting, waarbij de klantomgevingen alleen benaderd kunnen worden vanaf adressen die door de klant zelf als vertrouwd worden beschouwd.

Het datacenter van Expansion voldoet zowel fysiek als digitaal aan zeer zware eisen. Dit blijkt onder andere uit de volgende zaken:

Algemeen

Datacenter algemeen	PDC1	PDC2
		
Adres	Expolaan 50 7556 BE Hengelo (Ov.) Nederland	Barnsteenstraat 15 7554 TC Hengelo (Ov.) Nederland
Algemeen	Box-in-box datacenter	Volledig nieuw gebouwd data-center. Betonnen/stalen draag constructies met aluminium gevelbeplating en betonnen binnenschil.
TIER classificatie	TIER 3+	TIER 3+
Certificering	ISO27001, ISO14001, ISO9001	ISO27001, ISO14001, ISO9001
Duurzaamheid	100% groene stroom BREEAM-Excellent PUE 1,16	100% groene stroom PUE 1,25
Hoogte ligging	14,5 meter boven NAP	19,2 meter boven NAP
Oppervlakte	11.000 m²	2.500 m²
Oppervlakte datavloer	4.500 m²	1.600 m²
Aggregaatruimte	Naast datacenter, containers	Apart gebouw
Aantal zalen	8+ private suites	4
Ruimte per zaal	540 m², 316 racks	400 m², 216 racks
Overige faciliteiten	Lounge Boardroom Meeting Rooms Werkruimtes Kantine WiFi	Lounge 2 x Boardrooms 2 x Meeting Rooms 4 x Werkruimtes Kantine WiFi
Parkeerplaatsen	80	32
Toegankelijkheid	24 x 7 toegang direct aan de A1 10 minuten v/d Duitse grens 30 minuten van Apeldoorn 85 minuten van Amsterdam	24 x 7 toegang 5 minuten van de A1, aan de A35 15 minuten v/d Duitse grens 35 minuten van Apeldoorn 90 minuten van Amsterdam
Laden en lossen	3 Beveiligde laad/losruimtes	Beveiligde laad/losruimte
Maximale vloerbelasting	18 kN/m²	18 kN/m²
Vrije hoogte vanaf datavloer	3 meter	5,5 meter
Hoogte datavloer	210 cm, alle bekabeling onder de vloer	100 cm, alle bekabeling onder de vloer
Type datavloer	Antistatisch	Antistatisch
Maximale dakbelasting	Nvt, box-in-box	100 kg/m²
Racks	19" racks met geper-foreerde deur (afmeting 600 x 1000 x 46HE)	19" racks met geper-foreerde deur (afmeting 600 x 1000 x 47HE)
Flexibele co-locatie (op aanvraag)	Footprint / Private corridor / Private Cage / Private Suite	Footprint / Private corridor / Private Cage op aanvraag

Connectiviteit

Connectiviteit	PDC1	PDC2
Fysieke toevoer	Drie geografisch gescheiden toevoerpunten (manholes)	Drie geografisch gescheiden toevoerpunten (manholes)
Meet-me rooms	2, geografisch gescheiden	3
Externe connectivity (Previder netwerk)	Geografisch gescheiden fibers naar Amsterdam (Nikhef), Equinix EN1 en PDC2	Geografisch gescheiden fibers naar Amsterdam (Telecity2) en PDC1
Carriers	PDC1 is carrier neutraal Aanwezige carriers • Tele2 • TrenT • Relined • Eurofiber • Ziggo • KPN • Cogas • Unet • UPC • Atrato • Breedband Nederland	PDC2 is carrier neutraal Aanwezige carriers • Tele2 • TrenT • Relined • Eurofiber • Ziggo • KPN • Unet • UPC • Atrato • Breedband Nederland • BT
Internet Exchanges	• AMS-IX • NDIX • NLIX • DE-CIX	• AMS-IX • NDIX • NLIX • DE-CIX
Interne aansluitingen	Beheerd door Previder en gemanaged in een geautomatiseerd systeem	

Stroomvoorziening

Stroomvoorziening	PDC1	PDC2
Stroomtoevoer	10 Megawatt	6 Megawatt
Transformatoren	2 x 1.000 kVA per zaal	2 x 2.500 kVA
Redundancy	2N	2N
Stroomtoevoer naar de racks	230V, via 2 onafhankelijke paden (2N)	230V, via 2 onafhankelijke paden (2N)
Distributie naar zalen	10kV ringsystemen (middenspanning)	Busductsysteem (laagspanning)
Krachtstroom	3 Fasen / 420V op aanvraag leverbaar	3 Fasen / 420V op aanvraag leverbaar
Standaard levering	2 * 32 Ampère per rack	4 * 16 Ampère per rack (zaal 1) 2 * 32 Ampère (zaal 2)
High Density	Op aanvraag leverbaar	Op aanvraag leverbaar
UPS	2 x 2 x 320 kVA (2N) per zaal	2 x 2 x 550 kVA (2N) per zaal
Dieselgeneratoren	8 * 2100 kVA (N+1)	4 * 2100 kVA (N+1)
Dieseltanks	24 uur werkvoorraad Contract voor 24/7 brandstoflevering	48 uur werkvoorraad Contract voor 24/7 brandstoflevering

Koeling

Klimaatbeheersing	PDC1	PDC2
Koelprincipe	Milieuvriendelijk free-to-air koelsysteem met closed-cold corridors op de datavloer. Hergebruik van warmte voor verwarming kantoorpand.	Milieuvriendelijk free-to-air koelsysteem met closed-cold corridors op de datavloer.
Capaciteit	Gemiddeld 1,2 kW/m² Maximaal 24 kW/m²	Gemiddeld 2 kW/m² Maximaal 24 kW/m²
Leidingen	Voorzien van lekdetectie, geplaatst onder de datavloer	Voorzien van lekdetectie, geplaatst onder de datavloer
Koeling	N+1 ACU's per zaal (N+2 optioneel)	N+2 ACU's per zaal
Hitteafvoer	N+1 chillers	N+1 chillers
Inregel temperatuur	22° Celsius uitblaas-temperatuur gemeten bij koelmachines	22° Celsius uitblaas-temperatuur gemeten bij koelmachines
Absolute vochtigheid	40% +/- 15%	40% +/- 15%
High Density	tot 24 kW per rack op aanvraag	tot 24 kW per rack op aanvraag

Beveiliging

Beveiliging	PDC1	PDC2
Bewaking datacenter	24*7*365	24*7*365
Fysieke beveiliging	• Verhoogd stalen hekwerk rond het terrein • Elektrische schuifhekken voor in- en uitgaande voertuigen • Beveiligde los- en laadruimten	• Verhoogd stalen hekwerk rond het terrein • Elektrische schuifhekken voor in- en uitgaande voertuigen • Beveiligde los- en laadruimten
Alarmsysteem	• Gecertificeerd borgklasse 3, bouwtechnisch borgklasse 4 • Gesloten videocircuit (CCTV) binnen en buiten	• Gecertificeerd borgklasse 4 • Gesloten videocircuit (CCTV) binnen en buiten
Toegangscontrole	• Secure Access List (SAL) • Elektronische pas i.c.m. geldig identiteitsbewijs	• Secure Access List (SAL) • Elektronische pas i.c.m. geldig identiteitsbewijs
Brandbeveiliging	**PDC1**	**PDC2**
Brandpreventie	Speciale staalconstructie en zalen gescheiden door brand-vertragende wanden met een vertraging van 60 minuten	Speciale staalconstructie en zalen gescheiden door brand-vertragende wanden met een vertraging van 60 minuten
Branddetectie	Aspiratiesysteem met rookdetectie	Aspiratiesysteem als voor alarm met losse rookdetectie
Blusinstallaties	• Milieuvriendelijk Argonite systeem in de zalen • Brandslanghaspels in de gangen	• Milieuvriendelijk Argonite systeem in de zalen • Watermist blussysteem in de noodstroom generatorruimte • Brandslanghaspels in de gangen

Gebouwmanagement	PDC1	PDC2
Geavanceerd gebouw-beheersysteem (GBS)	• Stabiliteit van de omgeving • Belangrijke elektrische en mechanische systemen • Onderlinge samenwerking tussen diverse systemen • Kritieke parameters, rapportage van systeemprestaties • Koppeling van veiligheidssystemen in geval van activering van het brandalarm • Stroomverbruikmeters • Waterverbruikmeters • Koel/warmte transportmeters	• Stabiliteit van de omgeving • Belangrijke elektrische en mechanische systemen • Onderlinge samenwerking tussen diverse systemen • Kritieke parameters, rapportage van systeemprestaties • Koppeling van veiligheidssystemen in geval van activering van het brandalarm • Stroomverbruikmeters

Twin-datacenter

Twin-datacenterconcept	
Afstand tussen PDC1 en PDC2	ca. 5 km hemelsbreed
Inter-datacenter connectivity	• redundante darkfibers • WDM • Ethernet VLAN's

5. Zekerstelling en garanties

De veiligheid van de informatie wordt ook bepaald door de mate van de continuïteit. Hierbij is van belang dat klanten geen afhankelijkheid van Expansion mogen hebben. Expansion biedt haar klanten hier verschillende voorzieningen voor aan.

5.1. Escrow

Klanten die Xtendis binnen hun eigen infrastructuur draaien kunnen een escrow overeenkomst afsluiten. Deze overeenkomst regelt dat een klant automatisch eigenaar wordt van de broncodes en technische documentatie in het geval Expansion ophoudt te bestaan. Met deze codes en documentatie kan het beheer en de verdere ontwikkeling van Xtendis door de klant zelf of door een door de klant aan te wijzen dienstverlener worden voortgezet.

5.2. Cloudsecure

Voor afnemers van clouddiensten (Xtendis Online) biedt een escrow overeenkomst onvoldoende zekerheid omdat het systeem niet beschikbaar is binnen de eigen infrastructuur.

Om die reden heeft Expansion met een onafhankelijke derde partij (Softcrow) een bredere regeling opgezet in de vorm van CloudSecure. Deze constructie zorgt er voor dat indien Expansion BV ophoudt te bestaan, alle benodigde rechten en overeenkomsten overgaan naar een onafhankelijke stichting (Stichting Xtendis Secure). Het betreft hier dus niet alleen de rechten op Xtendis, maar bijvoorbeeld ook de overeenkomsten met het datacenter. Afnemers van Xtendis Online kunnen zich bij deze stichting aansluiten. De stichting zorgt allereerst voor continuering van de dienstverlening in al haar facetten. Vervolgens kunnen de leden van de stichting in alle rust een structurele oplossing kiezen. Dit kan bijvoorbeeld de overdracht zijn van alle data naar aan andere leverancier of de voortzetting van de dienst waarbij een nieuwe leverancier de ondersteuning en verdere ontwikkeling verzorgt.

5.3. Dataportabiliteit

Afnemers van de clouddiensten kunnen te allen tijde exports ontvangen van de documenten en data die zij met Xtendis Online laten beheren. Het is mogelijk op voorhand afspraken te maken over het exportformaat en de tariefstelling.

5.4. Verwerkersovereenkomst

Bij gebruik van Xtendis Online is Expansion verwerker in de zin van de Toepasselijke Data Protectie Wetgeving (Wet bescherming persoonsgegevens, die per 25 mei 2018 zal worden vervangen door de Algemene Verordening Gegevensbescherming).

De verantwoordelijkheden van Expansion en haar klanten (de Verantwoordelijke) worden vastgelegd in een Verwerkersovereenkomst. Expansion heeft hiervoor een standaard opzet.