Technische Gids

MISSION CRITICAL CLOUD

100% Nederlands, 100% betrouwbaar

INHOUDSOPGAVE

1. DIGITALE SOEVEREINITEIT

In een tijd waarin data dé kern is van elke organisatie, groeit ook het besef dat grip op die data essentieel is. Digitalisering heeft onze manier van werken en innoveren veranderd, maar maakt ons ook afhankelijk van technologieën en aanbieders buiten onze landsgrenzen. Denk aan Amerikaanse hyperscalers of clouddiensten die vallen onder buitenlandse wetgeving (U.S. CLOUD Act). Juist voor organisaties die met gevoelige of bedrijfskritische gegevens werken, roept dat vragen op: Waar staat mijn data? Wie heeft er toegang toe? En in hoeverre heb ik écht controle?

Digitale soevereiniteit gaat over het behouden van die controle – over data, infrastructuur en digitale processen. Het is geen luxe, maar een strategische noodzaak. Zeker in sectoren waar compliance, beschikbaarheid en veiligheid niet optioneel zijn.

1.1 Digitale soevereiniteit in de Mission Critical Cloud

Binnen onze Mission Critical Cloud staat digitale soevereiniteit centraal. De volledige cloudomgeving draait binnen datacenters op Nederlands grondgebied. Zo loop je geen risico dat de Amerikaanse overheid toegang tot jouw data krijgt (en mogelijk bedrijfs-/concurrentiegevoelige informatie.) én mitigeren we de afhankelijkheid van een datacenterpartij.

Voor organisaties die werken met vertrouwelijke of gereguleerde gegevens – zoals in de publieke sector, zorg of finance – is de onafhankelijkheid van Amerikaanse wetgeving cruciaal. Onze oplossing combineert de flexibiliteit en schaalbaarheid van een moderne cloudomgeving met keiharde garanties op het gebied van continuïteit, dataresidentie, compliance en security.

In public clouds valt jouw data, ook als de data op Nederlands grondgebied staat, onder buitenlande wetgeving. Met de Mission Critical Cloud blijft alle data binnen Nederlandse grenzen en onder Nederlandse wetgeving. Geen risico op buitenlandse toegang, wél juridische duidelijkheid en volledige grip op compliance.

2. TRIPLE DATACENTER INFRASTRUCTUUR

Beschikbaarheid en betrouwbaarheid vormen de "backbone" van de Mission Critical Cloud. Door te werken met een triple-datacenterarchitectuur elimineren we single points of failure en maximaliseren we de weerbaarheid van de infrastructuur. Onze cloudomgeving is verspreid over drie geografisch gescheiden datacenters binnen Nederland. Deze opzet garandeert dat bij uitval van één locatie – zelfs langdurig – alle cruciale workloads operationeel blijven. Dit maakt onze oplossing bij uitstek geschikt voor organisaties die afhankelijk zijn van een non-stop digitale beschikbaarheid en zich geen downtime kunnen veroorloven.

2.1 Onafhankelijke datacenters

De datacenters waar wij gebruik van maken bevinden zich op drie geografisch gescheiden locaties in Nederland:

- Delft (NorthC Datacenters)
- Amsterdam (Equinix AM5)
- Haarlem (Iron Mountain).

Deze strategische spreiding en het feit dat alle datacenters boven NAP staan, voorkomen uitval door regionale calamiteiten, zoals natuurrampen, stroomstoringen of cyberaanvallen.

Daarnaast zijn de datacenters drie onafhankelijke entiteiten, wat bijdraagt aan de structurele onafhankelijkheid van onze cloudoplossing.

2.2 Duurzaamheid van datacenters

We maken uitsluitend gebruik van datacenters die duurzaamheid hoog in het vaandel hebben staan en dit minimaal kunnen aantonen met een ISO 14000 certificering. De datacenters draaien op groene stroom en hebben een lage Power Usage Effectiveness (PUE), wat zorgt voor een minimale ecologische impact. Met een PUE tussen 1,16 en 1,25 komt de energie-efficiëntie uit op 80% tot 86%. Dankzij energiezuinige hardware en slimme koelingstechnieken zijn de datacenters niet alleen betrouwbaar, maar ook duurzaam in gebruik. Daarnaast werken we continu aan het verder reduceren van het energieverbruik.

Triple-datacenterarchitectuur van de Mission Critical Cloud

2.3 Geen invloed van Amerikaanse wetgeving

Dataopslag is niet alleen een technische keuze, maar ook een juridische. Veel internationale cloudproviders vallen onder Amerikaanse wetten zoals de Cloud Act en Patriot Act, die buitenlandse overheden het recht geven om toegang te eisen tot jouw data – zelfs als die fysiek in Nederland of Europa staat. Dit staat op gespannen voet met Europese wetgeving zoals de AVG.

Met onze Mission Critical Cloud garanderen we volledige digitale soevereiniteit. Onze cloud is 100%:

- Gebouwd in Nederland
- Gehost in Nederland
- Beheerd in Nederland

Jouw data valt dus uitsluitend onder Nederlands recht – zonder achterdeuren, zonder buitenlandse inmenging.

Voor organisaties die werken met gevoelige gegevens of bedrijfskritische software is dit geen luxe, maar noodzaak. Bij ons weet je zeker: wat van jou is, blijft van jou.

3. OPBOUW EN INRICHTING

Onze cloudomgeving is ontworpen zonder Single Point of Failure (SPOF). Dit betekent dat elk component redundant is uitgevoerd om een beschikbaarheid van nagenoeg 100% te garanderen. Door een gedistribueerde architectuur en sterke failover-mechanismen zorgen wij ervoor dat kritieke workloads ongestoord kunnen blijven draaien, zelfs bij onverwachte incidenten.

3.1 Onafhankelijk van datacenters

Onze cloudomgeving is verspreid over meerdere datacenters. Hierdoor leidt een storing op één locatie niet tot downtime. Zo blijft je IT-omgeving altijd beschikbaar, ook in onverwachte situaties.

3.2 Onafhankelijk van locatie en entiteit

De datacenters zijn geografisch gescheiden én in handen van verschillende partijen. Dat voorkomt afhankelijkheid van één eigenaar en verkleint het risico op grootschalige uitval door lokale storingen.

3.3 Onafhankelijk van stroomvoorziening

Kortstondige uitval wordt uiteraard opgevangen door UPS-systemen en generatoren. Om deze noodvoorzieningen zo min mogelijk in te hoeven zetten maken de datacenters gebruik van verschillende energie-infrastructuren én zijn ze aangesloten op onafhankelijke energieleveranciers.

3.4 Onafhankelijk van leveranciers

We kiezen bewust voor een multi-vendorstrategie. Dit geeft ons de vrijheid om altijd de beste technologieën toe te passen – zonder afhankelijk te zijn van één leverancier. Voor jou betekent dit maximale flexibiliteit en technologische voorsprong.

3.5 Onafhankelijk van Internet Service Providers

We maken gebruik van meerdere internetproviders. Hierdoor wordt automatisch de snelste en meest stabiele route naar jouw eindgebruikers gekozen. Dat zorgt voor betrouwbare connectiviteit en lage latency, ongeacht je locatie.

3.6 Onafhankelijk van beheer en onderhoud

Onze cloud draait volledig in eigen beheer. Wij voeren het beheer uit vanuit een zelfstandig opererende beheeromgeving. Dit betekent dat wij 24/7 zelf het onderhoud uitvoeren en incidenten oplossen, zonder afhankelijk te zijn van de cloudinfrastructuur waar onze klanten op draaien. En daarom zijn wij in staat keiharde SLA-garanties af te geven.”

3.7 Onafhankelijk van klantomgevingen

Elke klantomgeving is logisch en fysiek gescheiden. Data en applicaties zijn volledig afgeschermd. Klanten kunnen specifieke hard- en software integreren, van legacy-systemen tot de nieuwste AI-technologie.

4. SECURITY

De Mission Critical Cloud is opgebouwd volgens het Security by design principe. Met een gelaagde aanpak gebaseerd op zeven security-pijlers bieden we een toekomstbestendige beveiliging die opgewassen is tegen de dreigingen van vandaag én morgen.

4.1 Well Architected Framework

Onze Mission Critical Cloud is ontworpen conform de best practices van Well-Architected Frameworks, met specifieke aandacht voor de eisen die aan bedrijfskritische applicaties gesteld worden.

Dit houdt onder andere in dat wij gebruik maken van het zero-trust-principe. Toegangen staat dus altijd dicht en (onderdelen van) software zijn niet vanaf internet benaderbaar, tenzij hiervoor een functionele toepassing is.

Een bezoek aan de datacenters en werkzaamheden aan de Mission Critical Cloud worden nauwkeurig gelogd zodat deze terug te herleiden zijn naar een natuurlijke personen.

Daarnaast wordt het gehele platform periodiek getoetst aan de aanbevelingen van het Open Web Application Security Project (OWASP) en de Center for Internet Security (CIS) benchmarks. Het optimaliseren van de veiligheid van de cloudinfrastructuur is bij ons een continu proces.

4.2 Bescherming tegen DDoS-aanvallen

Om de beschikbaarheid van bedrijfskritische applicaties te garanderen, maken we gebruik van geavanceerde DDoS-bescherming via onder andere NaWas (Nationale Wasstraat) en Cloudflare. Deze oplossingen detecteren en mitigeren volumetrische en gerichte aanvallen in real time, nog vóórdat ze impact hebben op jouw workload.

NaWas biedt een krachtige buffer tegen grote netwerkgerichte aanvallen vanuit een Nederlands samenwerkingsverband van internetproviders en hostingpartijen.

Cloudflare voegt daar wereldwijde dekking en intelligente filtering aan toe, inclusief bescherming op het niveau van applicaties en API's. Door deze combinatie voorkomen we dat kwaadaardig verkeer je omgeving bereikt, terwijl legitiem verkeer ongemoeid doorgang vindt.

Zelfs bij grootschalige DDoS-campagnes blijft je cloudomgeving responsief en bereikbaar – essentieel voor organisaties die 24/7 online beschikbaar moeten zijn. Deze bescherming is standaard onderdeel van onze Mission Critical Cloud en vormt een belangrijke bouwsteen in onze security-aanpak.

4.3 Web Application Firewall

Onze Mission Critical Cloud is standaard uitgerust met een geavanceerde Web Application Firewall (WAF) die bescherming biedt tegen veelvoorkomende en geavanceerde aanvallen op het applicatieniveau. Denk aan bedreigingen zoals SQL-injecties, cross-site scripting (XSS), remote file inclusion en zero-day exploits.

De WAF analyseert al het HTTP- en HTTPS-verkeer in real-time en past intelligente detectie- en blokkeringstechnieken toe, zonder de performance of beschikbaarheid van je applicatie negatief te beïnvloeden. Door gebruik te maken van signature-based en anomaly-based detection kunnen we ook nieuwe of afwijkende aanvalspatronen vroegtijdig herkennen.

Daarnaast maken we gebruik van automatische updates van threat intelligence-feeds, waardoor de WAF voortdurend leert van nieuwe dreigingen wereldwijd. Hiermee wordt niet alleen de reactietijd bij incidenten verkort, maar wordt ook preventief opgetreden tegen opkomende risico’s.

De WAF kan flexibel worden geconfigureerd per applicatie of tenant, zodat maatwerkbeveiliging mogelijk is op basis van de gevoeligheid en het risicoprofiel van de applicatie. Zo bieden we maximale bescherming, zonder concessies te doen aan snelheid, gebruikerservaring of ontwikkelvrijheid.

4.4 Monitoring & Threat Hunting

In de Mission Critical Cloud ben je verzekerd van een proactieve beveiligingslaag die 24/7 waakt over jouw cloudomgeving. Door gedragsanalyse en patroonherkenning worden afwijkingen razendsnel gedetecteerd, nog voordat ze uitgroeien tot serieuze incidenten.

Onze aanpak bestaat uit twee complementaire pijlers:

1 Realtime monitoring

We monitoren netwerkverkeer, systeemlogs, en gebruikersgedrag met behulp van geavanceerde tooling en gedragsmodellen. Wij signaleren afwijkingen van de norm, zoals ongebruikelijke inlogpogingen, dataverkeer buiten kantooruren of verdachte resource-activiteit. Dit stelt ons in staat om bedreigingen vroegtijdig te herkennen en direct passende maatregelen te treffen.

2 Proactieve threat hunting

Ons security team voert gericht onderzoek uit naar subtiele signalen van potentiële aanvallen – zelfs als deze nog geen directe impact hebben. Denk aan het opsporen van 'living off the land'-technieken, laterale bewegingen binnen het netwerk of voorbereidingen voor datadiefstal. Door dreigingen in een vroeg stadium te identificeren, minimaliseren we risico's en beperken we de kans op schade of verstoring van kritieke processen.

Door monitoring en threat hunting te combineren, creëren we een gesloten feedbackloop: detectie, analyse en respons versterken elkaar continu. Deze aanpak vormt een essentieel onderdeel van de bredere beveiligingsstrategie van onze Mission Critical Cloud en stelt organisaties in staat om cyberdreigingen altijd één stap voor te blijven.

4.5 Vulnerability Scanning

We houden grip op de beveiligingsstatus van jouw cloudomgeving. Onze gestructureerde aanpak helpt je om kwetsbaarheden niet alleen te identificeren, maar ook effectief te prioriteren en te verhelpen – zonder dat je het overzicht verliest.

Onze aanpak bestaat uit vier pijlers:

1 Realtime CVE-monitoring

We houden wereldwijd bekende kwetsbaarheden (Common Vulnerabilities and Exposures) continu in de gaten. Zodra een nieuwe CVE impact kan hebben op jouw omgeving, analyseren we de relevantie en stellen we – indien nodig – direct mitigerende maatregelen voor.

2 Proactief patchbeheer

Op basis van scanresultaten en CVE-informatie zorgen wij voor een planmatig patchbeleid. Dit verkleint het aanvalsoppervlak en voorkomt dat bekende lekken open blijven staan. Voor kritieke kwetsbaarheden hanteren we een versnelde responstijd.

3 Maandelijkse securityscans

We voeren periodiek uitgebreide scans uit op systeemniveau, netwerkcomponenten en applicaties. Hiermee brengen we bekende kwetsbaarheden (zoals OWASP en CVE's)in kaart. Deze scans wordenafgestemd op jouw specifieke cloudomgeving en risicoprofiel.

4 Praktisch actieplan met prioritering

Je ontvangt heldere rapportages met aanbevelingen en prioriteiten. In overleg bepalen we welke maatregelen doorgevoerd worden, zodat de balans tussen veiligheid, stabiliteit en beschikbaarheid gewaarborgd blijft.

4.6 Security logging and alerting

Je beschikt over een krachtige beveiligingslaag die verdachte activiteiten binnen jouw cloudomgeving direct zichtbaar maakt. Door centraal logging en intelligente alerting te combineren, bieden we niet alleen inzicht, maar ook direct handelingsperspectief bij potentiële bedreigingen. Zo behoud je de controle over je security – op elk moment, vanuit één overzicht. De beveiligingslaag omvat:

Realtime alerts op maat

We configureren meldingen op basis van jouw risicoprofiel, compliance-eisen en applicatielogica. Denk aan alerts bij ongeautoriseerde toegangspogingen, policy-overtredingen of afwijkend gedrag van gebruikers of systemen. Zo krijg je alleen signalen die er écht toe doen.

Flexibele opvolging

Afhankelijk van je interne processen kunnen meldingen automatisch worden opgevolgd door ons securityteam, jouw eigen IT-afdeling of een combinatie van beide. Dit zorgt voor maximale flexibiliteit en duidelijke verantwoordelijkheden bij incidentafhandeling.

Volledige logging en compliance audit trail

We voeren periodiek validaties uit op back-ups om zeker te stellen dat data volledig en correct is opgeslagen. Daarnaast testen we het herstelproces regelmatig, zodat je verzekerd bent van een snelle en effectieve recovery wanneer het erop aankomt.

Continue monitoring en optimalisatie

Onze specialisten evalueren de effectiviteit van logging- en alertregels periodiek. Zo zorgen we dat het systeem meebeweegt met jouw infrastructuur en dreigingslandschap, zonder overspoeld te raken door irrelevante meldingen.

4.7 Lifecycle management (LCM)

Cloudcomponenten worden continu onderhouden en geüpdatet. Denk aan security patches, software-updates, major upgrades en hardware vervangingen, - essentieel om beschikbaarheid, veiligheid en compliance te waarborgen.

Binnen de Mission Critical Cloud doen we aan lifecycle management. Door structurele updates te combineren met continue optimalisatie, zorgen wij dat je cloudinfrastructuur altijd aansluit op de laatste standaarden, zonder dat jij of je team belast wordt met complex onderhoud of risicovolle migraties. Onze aanpak omvat:

Regelmatige (ad hoc) updates van images en runtime-stacks

We zorgen ervoor dat je workloads draaien op ondersteunde en actuele versies van besturingssystemen, libraries en containers. Hetzelfde geldt uiteraard voor de onderdelen van de cloudomgeving. Dit verkleint het risico op kwetsbaarheden, voorkomt technische schuld en zorgt voor maximale compatibiliteit met moderne cloudplatformen.

Continu versiebeheer en compatibiliteitsanalyse

We volgen actief de roadmap van gebruikte platformen en diensten. Wanneer nieuwe versies of functionaliteiten beschikbaar komen die relevant zijn voor jouw omgeving, adviseren wij gericht over performance- of securityverbeteringen. Zo profiteer je tijdig van innovaties, zonder zelf te hoeven bijhouden wat er verandert.

Risicobeheersing bij upgrades

Voordat we updates implementeren, testen we deze op impact en stabiliteit. Voor kritieke systemen hanteren we gefaseerde uitrolstrategieën en rollback-opties. Zo blijven updates beheersbaar en voorspelbaar, met minimale impact op je operatie.

4.8 Data integriteit en vertrouwelijkheid

Binnen de Mission Critical Cloud van ACC ICT staat de bescherming van data centraal. Of het nu gaat om klantgegevens, intellectueel eigendom of bedrijfskritische applicatiedata – je kunt rekenen op een cloudomgeving die ontworpen is voor vertrouwelijkheid, integriteit en herstelbaarheid. Onze aanpak omvat:

Encryptie by default

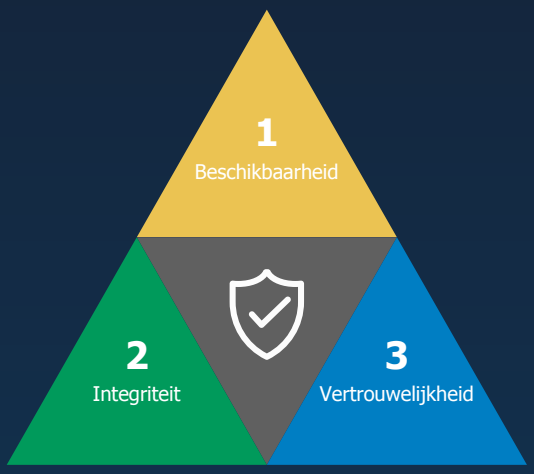
Alle data wordt standaard versleuteld met sterke cryptografische standaarden (AES-256 en TLS 1.2+). Daarmee borgen we de vertrouwelijkheid en beschermen we gevoelige informatie tegen ongeautoriseerde toegang, zowel intern als extern.

Geografisch gespreide back-ups

Back-ups worden redundant opgeslagen op minimaal twee fysiek gescheiden locaties binnen Nederland. Dit garandeert dat gegevens altijd beschikbaar blijven, zelfs bij regionale verstoringen of calamiteiten. Hierdoor wordt er altijd een set van de back-updata bewaard buiten de productielocaties.

Immutable back-ups

Om je te beschermen tegen ransomware en opzettelijke dataverwijdering, bieden we immutable back-ups aan. Deze zijn niet te wijzigen of te verwijderen gedurende een vooraf gedefinieerde retentieperiode. Dit maakt herstel na een aanval snel, betrouwbaar en controleerbaar.



Integriteitsvalidatie en hersteltesten

We voeren periodiek validaties uit op back-ups om zeker te stellen dat data volledig en correct is opgeslagen. Daarnaast testen we het herstelproces periodiek, zodat je verzekerd bent van een snelle en effectieve recovery wanneer het erop aankomt.

Compliancy en auditing

Onze opslag- en back-upoplossingen voldoen aan strenge normen zoals ISO 27001, NEN 7510 en ISAE 3402 type II, wat essentieel is voor organisaties die onder toezicht staan of werken met gevoelige persoonsgegevens.

5. ONZE CONTINUÏTEITSREGELINGEN

Een verstoring of faillissement heeft impact op je dienstverlening, reputatie en bedrijfsvoering. Juist daarom moet de beschikbaarheid van bedrijfskritische applicaties – zoals SaaS-diensten – altijd gegarandeerd zijn. Niet alleen de werking, maar ook de borging van code, (klant)data, technische kennis én bescherming tegen datalekken moet strak geregeld zijn.

Met onze continuïteitsregelingen – inclusief technische en juridische garanties – blijft je omgeving beschikbaar, ook in crisissituaties. Zo houd je controle over je operatie, wat er ook gebeurt.

In samenwerking met de Universiteit Utrecht ontwikkelden we twee innovatieve regelingen die risico's wegnemen en zekerheid bieden, afgestemd op jouw situatie:
– Business Edition
– Developers Edition

5.1 Business Edition

Deze regeling beschermt jouw IT-omgeving. In geval van faillissement van ACC ICT blijft onze dienstverlening beschikbaar, zodat jouw kritische applicaties gewoon blijven draaien. Geen datalekken, geen stilstand – wél continuïteit en controle.

- ✓ Jouw online IT-omgeving, apps en applicaties (SaaS-oplossingen) blijven tenminste drie maanden functioneren
- ✓ Alle functionaliteiten, inclusief uitwijk, back-up en beschikbaarheidsgaranties blijven gehandhaafd
- ✓ Onze IT-specialisten blijven het dagelijkse beheerwerk uitvoeren
- ✓ Hardware, data en persoonsgegevens vallen niet in handen van schuldeisers
- ✓ Er gaat geen data verloren
- ✓ De online IT-omgeving, apps en applicaties (SaaS-oplossingen) worden overgedragen aan de rechtsopvolger van onze organisatie
- ✓ Onze IT-specialisten facliiteren een eventuele migratie naar een nieuw cloudplatform

5.1 Developers Edition

Speciaal voor softwarebedrijven die hoge eisen stellen aan hun dienstverlening. Deze regeling waarborgt de werking van je SaaS-platform, ook in het geval van een faillissement van jouw organisatie of ACC ICT. Daarmee voldoe je aan de strengste continuïteitsnormen én versterk je het vertrouwen bij klanten.

- ✓ Jouw online IT-omgeving, apps en applicaties (SaaS-oplossingen) blijven tenminste drie maanden functioneren
- ✓ Alle functionaliteiten, inclusief uitwijk, back-up en beschikbaarheidsgaranties blijven gehandhaafd
- ✓ Onze IT-specialisten blijven het dagelijkse beheerwerk uitvoeren
- ✓ Hardware, data en persoonsgegevens vallen niet in handen van schuldeisers
- ✓ Er gaat geen data verloren
- ✓ Jouw klantdata wordt overdragen aan de rechtmatige eigenaren, ter voorkoming van dataverlies en/of datalekken
- ✓ De online IT-omgeving, apps en applicaties (SaaS-oplossingen) worden overgedragen aan de rechtsopvolger van jouw organisatie
- ✓ Onze IT-specialisten faciliteren een eventuele migratie naar een nieuw cloudplatform
- ✓ Jouw eindklanten worden tenminste drie maanden rechtstreeks ondersteund

"Wij garanderen dat jouw digitale informatie veilig beschikbaar is, onafhankelijk van derden, altijd en overal."
- Paul Bijleveld, Managing director - ACC ICT"

6. KEY PERFORMANCE INDICATORS (SLA)

Onze cloudprestaties worden gemeten aan de hand van duidelijke KPI's, waarmee we onze garanties kunnen onderbouwen.

6.1 Beschikbaarheid

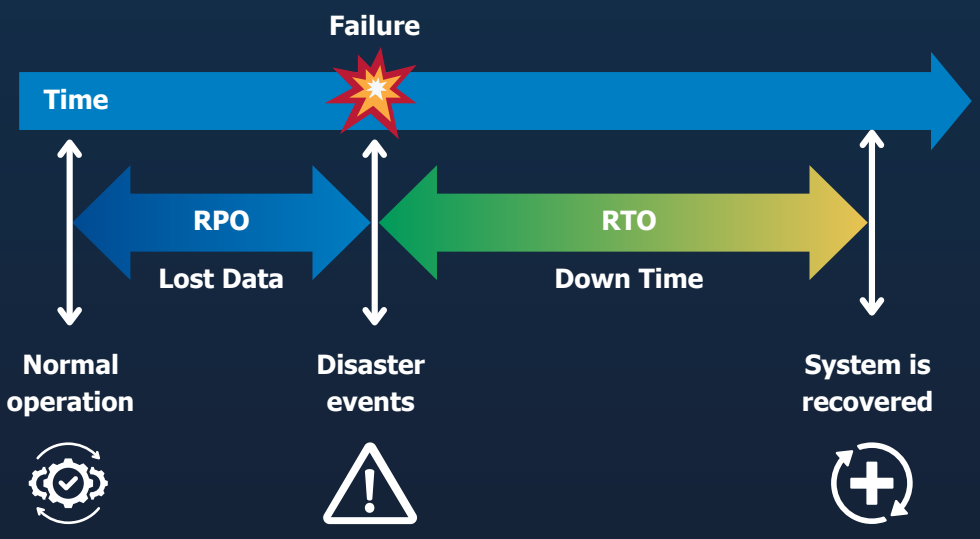
Met een minimale beschikbaarheid van 99,99% op onze cloudomgeving – en een gerealiseerde uptime van 99,9995% in de afgelopen 10 jaar– ben je verzekerd van een stabiele cloudomgeving. Dankzij de redundante infrastructuur en 24/7 monitoring blijft je omgeving continu beschikbaar.

6.2 RTO en RPO

Onze Recovery Time Objective (RTO) bedraagt maximaal 4 uur, tailormade is deze zelfs tot bijna nul te reduceren. De Recovery Point Objective (RPO) wordt klantspecifiek afgestemd, zodat jij precies de balans bepaalt tussen het risico op dataverlies en de investeringen om dergelijke risico's te mitigeren. Zo sluiten continuïteit en investeringen altijd aan op je bedrijfsrisico's.

6.3 Voorspelbare kosten

Met een transparante kostenstructuur weet je precies waar je aan toe bent. Geen verrassingen achteraf, maar helder inzicht in wat je cloudomgeving kost – en waarom. Dat maakt budgetteren eenvoudig en betrouwbaar. Dit is ideaal voor SaaS-bedrijven omdat deze transparantie het mogelijk maakt de clouddiensten te verwerken in de tarieven richting eindklanten, zonder dat jouw marge onder druk komt te staan.



7. COMPLIANCE EN WETGEVING

Voor organisaties die werken met gevoelige of gereguleerde data is compliance geen bijzaak, maar een vereiste.

De Mission Critical Cloud van ACC ICT is ontworpen om te voldoen aan de hoogste standaarden op het gebied van informatiebeveiliging, privacy en risicobeheersing. Dankzij onze Nederlandse cloudomgeving en strakke beveiligingsmaatregelen bieden we een solide basis voor sectoren waar continuïteit, integriteit en wet- en regelgeving centraal staan.

Overzicht van de normen en kaders waaraan onze cloudomgeving voldoet.

Norm / Richtlijn	Toelichting
AVG / GDPR	Dataopslag en -verwerking vinden uitsluitend plaats binnen Nederland, onder EU-jurisdictie. Geen risico op conflicterende wetgeving zoals de Amerikaanse CLOUD Act.
NIS2-richtlijn	Onze beveiligingsarchitectuur en incidentresponsprocedures zijn afgestemd op de nieuwe Europese verplichtingen voor vitale en digitale sectoren.
BIO (Baseline Informatiebeveiliging Overheid)	Cloudomgeving is compatibel met overheidsnormen voor informatiebeveiliging, inclusief logging, toegang en dataminimalisatie.
DORA (Digital Operational Resilience Act)	Onze inrichting sluit aan bij de eisen voor operationele weerbaarheid zoals deze vanaf 2025 gelden voor de financiële sector.
ISO 27001	Onze informatiebeveiliging is ingericht volgens internationaal erkende standaarden voor risicomanagement, toegang, logging en procesbeheersing.
NEN 7510	Specifieke ondersteuning voor zorgorganisaties. Wij voldoen aan alle eisen voor vertrouwelijkheid en beschikbaarheid van patiëntdata.
ISAE 3402 Type II	Onafhankelijke audit die bevestigt dat onze interne processen aantoonbaar gecontroleerd en effectief zijn ingericht. Belangrijk voor organisaties met uitbestedingsverantwoordelijkheid.
DNB – Toetsingskader uitbesteding en IT-beheer	Onze cloudomgeving sluit aan op de toezichtvereisten van De Nederlandsche Bank, inclusief dataminimalisatie, uitbestedingsrisico's en contractuele waarborgen voor beschikbaarheid, integriteit en vertrouwelijkheid.

8. TOEKOMSTVISIE

ACC ICT is sinds 2002 actief als Managed Service Provider (MSP). Na een periode van 10 jaar hebben wij in 2012 gekozen om van scratch af aan een compleet nieuwe cloudinfrastructuur te ontwerpen. De ervaring leerde ons dat onafhankelijk van derden opereren één van de belangrijkste uitgangspunten is om de eindverantwoordelijkheid over alle klantafspraken te kunnen garanderen. Dit ontwerp heeft geresulteerd in de bouw van onze Mission Critical Cloud waarbij volledige autonomie, beschikbaarheid en veiligheid hand in hand gaan.

Door onze cloudomgeving volledig in Nederland te bouwen en beheren, bieden we maximale controle over data – zonder afhankelijkheid van buitenlandse partijen of wetgeving. Sterker nog, wij hebben onze cloud zo opgebouwd dat we afhankelijkheden volledig uitsluiten. Dat is wat wij verstaan onder digitale soevereiniteit.

Onze Mission Critical Cloud is een strategisch fundament dat is ontworpen voor organisaties die geen concessies willen doen op het gebied van betrouwbaarheid, veiligheid, beschikbaarheid of compliance.

En we kijken vooruit! Technologie staat nooit stil – en wij dus ook niet. Zo hebben wij in 2020 de Mission Critical Cloud geoptimaliseerd voor Kubernetes platformen, waarbij Kubernetes-features als; op- en afschalen, redundantie, rolling updates, etc. volledig worden gesupport. Daarnaast blijven wij continu doorinvesteren in automatisering, security, cloud native toepassingen, compliance-vraagstukken én de integratie van AI.

Want toekomstbestendig zijn betekent: continu innoveren, zonder je basis uit het oog te verliezen. Of het nu gaat om nieuwe wetgeving zoals DORA en NIS2, of om de steeds hogere eisen van jouw eindklanten – niet voor niets luidt onze missie;

Wij garanderen dat jouw digitale informatie veilig beschikbaar is, onafhankelijk van derden, altijd en overal.

Ik ben ervan overtuigd dat het onze rol en verantwoordelijkheid is om organisaties uit te dagen na te denken over de keuzes die ze maken. De uitkomst is altijd goed, mits deze op basis van de juiste en volledige informatie gemaakt wordt. Want tenslotte wordt het succes van morgen bepaald door de keuzes die we vandaag maken

Met onze Mission Critical Cloud bieden wij naast een technische oplossing, de zekerheid van een strategische IT-partner die jouw business begrijpt en met je meedenkt, meegroeit en meewerkt aan jouw digitale succes.

Paul Bijleveld

Managing Director - ACC ICT