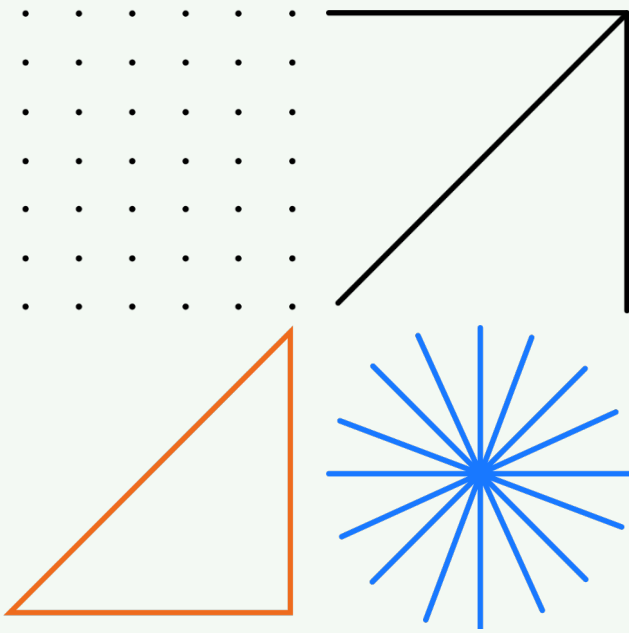


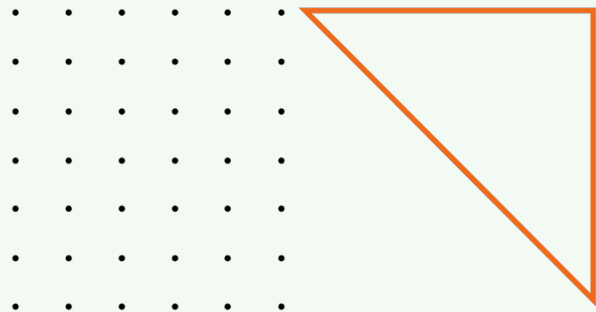
**PAQT**



# Safety & quality sheet

PAQT.com

SAQ-30-05-23-R1



# 1. Beveiliging en kwaliteitsborging

De hoge kwaliteit en betrouwbaarheid van de software die wij leveren, is een van de belangrijkste pijlers van PAQT.com. Hier lichten we toe hoe we deze zaken borgen. We hanteren het **BIV-model** dat staat voor: **B**eschikbaarheid, **I**ntegriteit en **V**ertrouwelijkheid. Dit model wordt ook gehanteerd binnen de ISO 27001, de internationale norm voor informatiebeveiliging. PAQT is ISO 27001 en NEN 7510 gecertificeerd en ontwerpt, ontwikkelt en beheert applicaties volgens deze norm.

## **BIV: Beschikbaarheid**

Een applicatie moet altijd beschikbaar zijn voor de gebruikers. Dit borgen we met de volgende maatregelen:

- **Hardware, server & applicatiemonitoring:** de toegang tot alle applicaties (access logs), de systeem- en applicatielogs worden 24/7 opgeslagen op onze ELK stack (Elasticsearch, Logstash, Kibana). Incidenten worden hierdoor direct gedetecteerd en genotificeerd. Onregelmatigheden kunnen achteraf snel worden opgespoord en opgelost. Dagelijks worden deze logs handmatig gecontroleerd door de applicatieverantwoordelijke Lead developer en de CISO.
- **Onverwachte fouten (real-time):** Als er zich een fout voordoet in de applicatie wordt het verantwoordelijke ontwikkelteam direct geïnformeerd via Sentry. Hiermee worden incidenten gerapporteerd zonder dat de gebruiker dit zelf hoeft te doen of zelfs nog voordat de gebruiker ervan op de hoogte is.
- **Bereikbaarheid (99.99% uptime):** Vanaf 217 locaties wereldwijd wordt met via Uptrends getest of de applicatie bereikbaar is. De beschikbaarheid van de servers is 99,99%, exclusief gepland onderhoud.
- **Configuratie webserver via versiebeheer:** Alle wijzigingen aan de servers worden gelogd in versiebeheersysteem Github. Zo borgen we dat er geen fouten kunnen ontstaan in de configuratie en dat een server snel opgezet kan worden. We hanteren het zes-ogen-principe.
- **OAP-straat:** Iedere applicatie wordt ontwikkeld in een OAP-straat (Ontwikkel, Acceptatie, Productie-omgeving) via Github workflows en actions. Binnen de OAP-straat wordt de applicatie zowel automatisch als functioneel getest voordat deze op een productieomgeving terecht komt. Pas na goedkeuring door de opdrachtgever komen de geteste nieuwe versie live.
- **Code-reviews:** Alle code die wordt geschreven wordt door minimaal twee andere developers gecontroleerd, getest, voorzien van eventuele bevindingen en verwerkt via Github. Alle handelingen worden geregistreerd en gelogd. De code reviews zijn vast onderdeel van de Software Development Lifecycle (SDL) en worden conform het Informatiebeveiligingshandboek ook actief gecheckt op voorwaarden voor security by design.
- **Automatische tests voor iedere oplevering:** Bij het releasen van een nieuwe versie worden onderdelen van de applicatie automatisch getest met PHPUnit en/of Jest, Dusk en andere technieken om het correct functioneren van de applicatie automatisch te controleren.
- **Back-ups:** Er worden kopieën gemaakt van de laatste 21 nachten en 1 per week van de laatste 6 weken. Deze worden opgeslagen in een ander datacentrum dan waar de applicatie gehost wordt. Wij bewaken het back-up proces en hebben een disaster recoveryplan om bij ernstige calamiteiten de applicatie zo snel mogelijk te herstellen. Het volledige back-up proces wordt periodiek getest door de CISO.

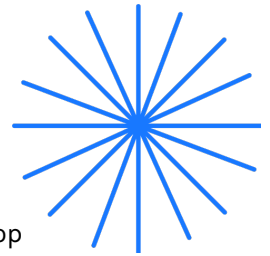


elastic

SENTRY

UPTRENDS





## BIV: Integriteit

Om de integriteit te bewaken moeten we de informatie op een platform kunnen valideren op correctheid. We hanteren hiervoor de volgende maatregelen:

- **Coding standaarden (onder andere PSR-12, PSR-4, eslint en stylelint):** Alle code wordt geschreven volgens de internationaal geldende “PSR-12”-norm. Hierdoor is code altijd leesbaar en daarmee overdraagbaar.
- **Static code analysis:** Alle code wordt automatisch geanalyseerd door de applicatie PHPStan. Hiermee worden eventuele bugs gedetecteerd zodat ze verholpen kunnen worden voordat een nieuwe versie van de applicatie naar productie gaat.
- **Automatisch patchen van kwetsbaarheden:** Alle gebruikte dependencies worden automatisch 24/7 gescand op kwetsbaarheden en wanneer dat nodig is gepatched via Dependabot. Het beleid is dat kritische kwetsbaarheden standaard binnen 24 uur worden gepatched, hier wordt actief op gemonitord.
- **End-to-End tests via team Tech:** Software development teams kunnen alleen na goedkeuring van team Tech aanpassingen doen aan de infrastructuur via IaS. Verder worden automatisch na iedere build de permissies binnen de software gecontroleerd en gerapporteerd aan team Tech. Dit is een losstaand team dat bestaat uit de CISO en twee senior specialisten.



## BIV: Vertrouwelijkheid

Om de vertrouwelijkheid te bewaken moeten we ervoor zorgen dat informatie van de applicatie niet in handen kan komen van derden. Hiervoor nemen we de volgende maatregelen:

- **Interne procedures/registratie en controle van toegang tot live data:** Alle procedures zijn beschreven en geformaliseerd volgens de ISO 27001 en NEN 7510 normen. Deze wordt jaarlijks door een externe partij geaudit. De toegang wordt actief gecontroleerd door de CISO.
- **Gegevensclassificatie door CISO:** Alle gegevens worden geclassificeerd door de CISO en zijn doorgaans minimaal klasse 3 (applicatie met gevoelige informatie). Vertrouwelijke informatie is alleen toegankelijk voor specifieke personen binnen onze organisatie. Ook dit is volgens de ISO 27001 en NEN 7510-normeringen.
- **Vulnerability scans (OWASP top-10):** Bij elke nieuwe versie van softwareoplossingen die wij implementeren worden er automatisch vulnerability scans uitgevoerd. Dit gebeurt met de online diensten Detectify en Holm Security. Ook wordt er getest op de wereldwijd meest voorkomende beveiligingslekken aan de hand van actuele informatie door de onafhankelijke beveiligingsorganisatie OWASP. Aanvullend kunnen er pentesten worden ingepland.
- **Toegang server via VPN:** Beheertoegang tot servers waar applicaties worden gehost verloopt altijd via het beveiligde VPN-protocol. Daarnaast wordt gebruik gemaakt van SSH (public/private key) en IP-whitelisting om toegang tot de infrastructuur te beveiligen.
- **SSL:** Er wordt standaard gebruik gemaakt van een 2.048-bits sterke SSL-verbinding.



## 2. Ontwikkelteam

### 2.1 Kwaliteit en bedrijfszekerheid

Onze opdrachtgevers vertrouwen PAQT hun bedrijfskritische software toe. Dat geeft ons de verplichting om alles uit de kast te halen en de beste oplossingen te realiseren. We leggen de lat dan ook hoog als het gaat om kwaliteit, betrouwbaarheid en veiligheid.

Onze ervaren ontwikkelteams werken met de modernste technieken, volgens internationale standaarden en we zijn **ISO 9001, ISO 27001 en NEN 7510 gecertificeerd**. Het spreekt voor zich dat we alle software zelf onderhouden en er dag en nacht bovenop zitten.

Daarnaast maken we ons sterk voor verdere professionalisering van de branche. We doen dat binnen Dutch Digital Agencies, de branchevereniging van de beste digitale bureaus in ons land. En we zijn medeoprichter van de Dutch Laravel Foundation.



### 2.2 Alleen samen lukt het

Succesvolle software kan alleen geïmplementeerd worden wanneer alle betrokken partijen optimaal samenwerken. Bij PAQT werk je samen met een vast ontwikkelteam, dat voor jou door het vuur gaat. Je eigen team kent jouw software door en door. Zij zijn betrokken tijdens het ontwerp en de implementatie, maar ook bij beheer, onderhoud en het verfijnen en verbeteren van je software. Hierdoor heb je aan een half woord genoeg.

Software implementeren is dus echt samenwerken - waarbij onze opdrachtgever altijd de regie behoudt. Dankzij het unieke PAQT.com samenwerkingsplatform is een project op ieder moment en voor alle stakeholders volkomen inzichtelijk en begrijpelijk. Zo houden we grip op scope, tijd en budget.

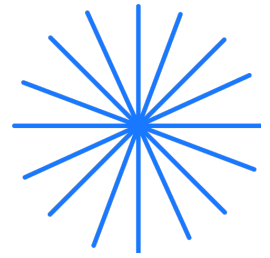
### 2.3 Agile Scrum

Voor het beheersen van haar projecten hanteert PAQT de ontwikkelmethode Agile Scrum. Dit is de meest efficiënte én effectieve methode om software te ontwikkelen. Bij Agile Scrum hebben opdrachtgevers en het ontwikkelteam nauw contact. Dit heeft een aantal grote voordelen:

- De opdrachtgever heeft gedurende het gehele proces invloed en kan dus snel bijsturen.
- Er zijn meerdere tussenoplevingen waarbij de applicatie getest kan worden op accurate werking.
- De opdrachtgever kan al tijdens het project de applicatie aanbieden aan testklanten. Dit zorgt ervoor dat er tijdens de ontwikkeling ruimte is om gebruik te maken van voortschrijdend inzicht.

### 2.4 De 5 zekerheden van PAQT

1. We begrijpen je
2. Je innovatie is snel operationeel
3. Jij bent altijd 'in control'
4. Je bent klaar voor de toekomst
5. Je eigen team gaat voor jou door het vuur!



## 3. Datacenter & hosting

### 3.1 Partners

Producten, diensten, applicaties en data van onze opdrachtgevers zijn ondergebracht op servers die aan de hoogste veiligheidsnormen voldoen. De hosting van de fysieke apparatuur en de faciliteiten van het datacenter zijn in handen van partners die uitblinken in hun vakgebied. Deze hebben wij geselecteerd op basis van uitstekende veiligheid, continuïteit, kennisniveau en apparatuur.

Voor managed hosting is onze partner:

#### **Cyso B.V. (KvK nr. 37133395)**

Wognumsebuurt 3  
1817 BH Alkmaar  
KVK: 37133395

Cyso beschikt over onderstaande certificeringen:

- ISO 27001, 20000
- NEN 7510

Voor het datacenter is dit:

#### **Global Switch B.V. (KVK nr. 27184200)**

Johan Huizingalaan 759  
1066 VH Amsterdam  
Netherlands

Global Switch beschikt over onderstaande certificeringen:

- ISO 9001, 14001, 27001, 45001, 50001
- ISAE 3402
- AMS-IX Conform PCI DSS

### 3.2 Kenmerken datacenter

Global Switch is toonaangevende eigenaar, exploitant en ontwikkelaar van grote, carrier- en cloudneutrale, multi-klienten datacenters voor IT-bedrijven in Europa en Azië-Pacific. Global Switch biedt klanten technische ruimte om hun computerservers, netwerkapparatuur en overige IT-infrastructuur te huisvesten. Daarbij verzekeren ze een 24x7x365 bedrijfszekere stroom en koeling, beveiliging en bewaking van de infrastructuur en de omgeving.

Dankzij de carrier- en cloudneutrale status van Global Switch, hebben ze een netwerkdichte omgeving opgebouwd met ongeveer honderd carriers, cloud- en andere netwerkserviceproviders. Het groeiende ecosysteem, de nabijheid van het centrale zakendistrict en de belangrijkste Nederlandse kabelinfrastructuur, maar ook de aanwezigheid van AMS-IX en NL-ix, maken de faciliteit een logische keuze voor elke onderneming of organisatie die op zoek is naar betrouwbare, snelle verbindingen binnen Nederland en over de hele wereld.

#### **Overzicht gebouw**

Global Switch heeft voor hun datacentrum van 32.000 m<sup>2</sup> een langdurige erfpachtovereenkomst met een automatisch recht van verlenging. Het heeft twee datavloeren met een vloerplafondhoogte van zes meter. Het pand is gebouwd om als datacenter te kunnen fungeren met operationele prestaties die Tier III overtreffen. Verdere eigenschappen van het datacenter zijn:

- Kooien voor flexibele en veilige IT-ruimten
- Structureel stalen frame met gewapend betonvloeren en metalen buitenbekleding
- Geen verhoogde vloer
- Minimum vanaf afwerking vloer: 3,9 m vrije hoogte tot onderzijde van de laagste balken
- Vloerbelasting van 15 kN/m<sup>2</sup>
- 2 goederenliften (4 ton)

### **Stroomvoorziening**

Het datacenter is rechtstreeks aangesloten op het landelijke stroomnetwerk en biedt gemiddeld een standaard dichtheid van 2000 W/m<sup>2</sup> met volledige ondersteuning voor hogere dichtheden. Daarnaast is Global Switch de enige provider in de stad met een eigen stroomvoorziening van 72MVA bij 50 kV.

Technische (IT) stroom in hal 1 via roterende UPS-systemen met dieselgeneratoren op locatie met N+1 redundantie en in de hallen 2, 3 en 4 via statische UPS in 2N-configuratie

- Mechanische systemen met een back-up van een stand-by generatorsysteem voor de hallen 2, 3 en 4 met N+1 redundantie
- Volledig gescheiden stroomverdeling naar technische ruimtes
- Brandstofopslag op locatie voor 48 uur werking op vollast met 24x7x365 brandstoflevering

### **Maatregelen tegen brand**

Global Switch heeft een volledig analoog adresseerbaar branddetectiesysteem in alle ruimtes. Er is een snel rookdetectiesysteem met aanzuiging (24x7x365 bewaakt) en er is een gasblussysteem (Inergen) in de technische ruimtes.

### **Beveiliging & toegangscontrole**

Het operationeel centrum is 24x7x365 bemand en er is altijd bewaking door professionele beveiligers. Zij worden in hun werk geholpen door constante camerabewaking (CCTV), zowel binnen als buiten, een uitgebreid inbraakdetectiesysteem met alarm naar alle ruimtes en een terrein-inbraakdetectiesysteem (PIDS). Voor optimale veiligheid worden camerabeelden 31 dagen bewaard.

Fysieke toegang tot het datacentrum is enkel mogelijk via een mantrap-deur, waarbij strikte toegangscontrole plaatsvindt volgens ISO 27001 norm, met behulp van keycards en biometrische systemen. Ook de laad- en losruimte van het datacentrum wordt 24x7x365 beveiligd.

### **Beheer van kritieke omgevingen**

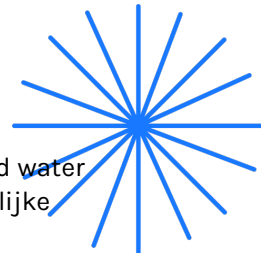
In het datacentrum is continue bewaking van de omgeving op het gebied van thermische condities. Een ervaren team biedt 24x7x365 facilitair management en ook alle gebouwbeheersystemen worden ieder uur van de dag bewaakt. Verder beschikt Global Switch over omvangrijke energiemeetsystemen en werken ze volgens een internationaal erkend programma voor kritieke omgevingen.

### **Werkprocessen**

De werkwijze van Global Switch voldoet aan ISO 27001. Deze internationale norm stelt de strengst mogelijke eisen aan informatiebeveiliging. Men gebruikt hierbij een robuust Critical Environments Programme (programma voor kritische omgevingen). Dit staat centraal bij het toepassen en handhaven van situaties uit de praktijk in alle datacenters.

### **Koeling**

In het datacentrum zorgt een 35 MW koelvoorziening met minimaal N+2 bedrijfszekerheid op alle systemen voor de juiste temperatuur. Wandventilatoren houden de temperatuur en luchtvochtigheid in de technische ruimte binnen het aanbevolen bereik van ASHRAE TC9.9. Er



liggen overal gescheiden leidingen en de koelinfrastructuur werkt door middel van gekoeld water (Chiller Assist) waardoor minder mechanische koeling nodig is en daarom minder schadelijke koudemiddelen en fossiele brandstoffen nodig zijn om systemen draaiende te houden.

### **Natuurverschijnselen**

Het datacenter bevindt zich in Amsterdam, in de wijk Slotervaart/Overtoomseveld, grenzend aan de belangrijkste Nederlandse glasvezelroutes in Amsterdam. Het pand is in 2014 opgeleverd en speciaal ontworpen en gebouwd om als datacenter te fungeren. De serverruimte bevindt zich boven NAP.

### **Milieu**

Via exploitatie en innovaties in ontwerp, verbetert Global Switch continu de energie-efficiëntie van onze datacenters. Zo zijn bijvoorbeeld onderstaande maatregelen genomen in het datacenter:

- Hoog efficiënte UPS met lithium batterijen met een lange levensduur
- Ventilatoren en pompen met variabel toerental, ledverlichting
- Gebruik van koelgassen met een laag broeikas-opwarmingsvermogen (GWP)
- Selectie van schakelapparatuur die SF6 vrij is
- Installatie van uitgebreide meet- en monitoringssystemen om de energieprestaties te optimaliseren en het energieverbruik te verminderen

### **Netwerk**

Het datacentrum is carriernutraal met toegang tot meerdere wereldwijde en regionale carriers en internet-serviceproviders met darkfiber, wavelength, ethernet, MPLS, VPLS, IP-transit, peering, CDN, opslag, virtuele diensten (SDN), spraak- en mobiele diensten. Er is toegang tot diverse clouddiensten via vooraanstaande aanbieders van openbare, privé en hybride clouddiensten:

- 3 verschillende MMR's en 3 verschillende Building Entry Points
- Gescheiden kabelrouteringen en leidingschachten
- Dakruimte beschikbaar voor satelliet- en antenne-apparatuur
- AMS-IX, NL-ix, GE-CIX, NetIX Communications en Speed-IX aanwezig

## **3.3 Kenmerken hosting**

Cyso is dé toonaangevende Nederlandse leverancier van managed internet services, platformen en infrastructuur voor de zakelijke markt. Ze leveren maatwerkoplossingen en beheer voor complexe, bedrijfskritische platformen en applicaties en sluiten daarmee perfect aan op de hoge eisen die PAQT stelt aan partners.

### **Platform**

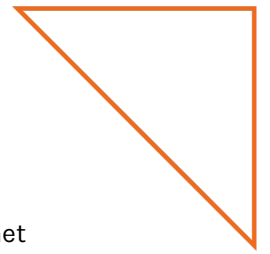
Het virtualisatieplatform is opgezet met vSphere, een door VMWare gestandaardiseerde en gevalideerde omgeving, waardoor alle onderdelen optimaal met elkaar samenwerken.

### **Servers**

De PowerEdge servers van Dell zijn voorzien van de laatste Intel Xeon processoren. De servers zijn redundant uitgevoerd, waardoor er bij problemen direct overgeschakeld kan worden op een andere server.

### **Opslagruimte**

De opslag wordt verzorgd door enterprise opslagsystemen van Pure en Tintri. Deze systemen maken gebruik van een grote hoeveelheid snelle SSD-schijven, een flash cache en intelligente RAID-levels. Alles is redundant uitgevoerd, zodat elk onderdeel van het systeem kan uitvallen zonder dat dit een onderbreking tot gevolg heeft.



### Firewall en toegang

De enterprise firewalls leveren hoogwaardige bescherming tegen netwerk-, content- en/of applicatie-level bedreigingen. Deze dienst grijpt in op de netwerklaag (OSI Layer 3/4) van het dataverkeer van en naar de infrastructuur. Hiermee wordt gecontroleerd welke applicaties en diensten op servers publiekelijk toegankelijk moeten zijn en welke geheel of gedeeltelijk afgeschermd dienen te worden op basis van geografische bron, netwerkpoort, IP-adres en protocol.

### Back-up

De back-up en recovery van de gegevens is als volgt geregeld.

- **Frequentie / RPO (recovery point in time):** Eénmaal per dag wordt een volledige back-up gemaakt. Dit betekent een maximaal dataverlies van 24 uur.
- **Medium:** Er wordt een back-up gemaakt op de harde schijven van een fysiek andere server, in een ander datacenter.
- **Bewaartermijn:** De back-up wordt gedurende drie weken bewaard. Dit betekent dat er 21 dagen teruggekeken kan worden.
- **Recoveryprocedure:** Gegevens uit de back-up worden op verzoek beschikbaar gemaakt. De recoveryprocedure valt binnen de Supporturen strippenkaart.
- **RTO (Recovery Time Objective)** Het uit de back-up halen van individuele bestanden (en databases) verloopt volgens het standaard incident management proces. Het compleet herstellen en weer in productie nemen van een server/platform in het geval van een disaster is afhankelijk van de grootte en complexiteit van het platform. Voor back-up en recovery van servers op apparatuur anders dan van Cyso, kan Cyso in samenwerking met PAQT.com advies geven en dit technisch inregelen volgens hetzelfde proces, binnen de mogelijkheden van de infrastructuur. Cyso en PAQT kunnen in zo'n geval wel het proces inrichten en bewaken, maar geen garanties geven over de kwaliteit en beschikbaarheid van de (data van de) back-ups.

### Support

De servers worden met monitoringsoftware continu in de gaten gehouden. Mochten er indicaties zijn van (toekomstige) problemen dan worden wij hiervan automatisch, per sms, op de hoogte gesteld zodat meteen kan worden ingegrepen. Ook is de storingsdienst 24 uur per dag en 7 dagen per week bereikbaar voor het geval zich calamiteiten voordoen. De gegarandeerde responstijd op een storing is 4 uur, maar in de praktijk wordt er direct actie ondernomen.

### VPN

De infrastructuur is alleen bereikbaar via versleutelde VPN-verbindingen. Een beperkt aantal medewerkers van PAQT heeft deze beheertoegang in verband met hun DevOps rol. Voor beheertoegang tot individuele servers is daarnaast een versleutelde SSH-verbinding nodig.

### Software-updates

Maandelijks worden updates van servers uitgevoerd binnen vooraf gedefinieerde onderhoudsvensters. Deze onderhoudsvensters zijn iedere werkdag van 00:00 - 04:00 uur. Zo blijven systemen veilig en stabiel. Zijn er lekken in software gevonden, dan worden deze snel en verantwoord geïnventariseerd en gepatcht via Trivy.