CONTINUÏTEITS- EN BEVEILIGINGSPLAN

T&T COMPET&T B.V.
Versie 15.01

Niets uit deze publicatie mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm, geluidsband, elektronisch of op welke andere wijze dan ook en evenmin in een retrieval systeem worden opgeslagen, zonder voorafgaande schriftelijke toestemming van T&T

T&T levert digitale diensten voor de uitwisseling van persoonlijke gegevens

INHOUDSOPGAVE **PAGINA**

1 DOELSTELLING EN OPBOUW

1.1 Inleiding

Dit rapport beschrijft de maatregelen die T&T heeft getroffen om de veiligheid en beschikbaarheid (continuïteit) van haar SaaS-diensten te waarborgen.

De toereikendheid van de maatregelen wordt jaarlijks getoetst in een overleg tussen Directie en de ICT-manager. Indien gewenst en/of nodig zal het rapport worden aangepast, en door de directie gefiatteerd, waarna het wordt gepubliceerd op het intranet van T&T.

1.2 Opbouw rapport

In hoofdstuk 2, worden achtereenvolgens de bedreigingen op de volgende gebieden geïnventariseerd.

- Algemene risico's
- Fysieke bedreigingen
- Infrastructurele bedreigingen
- Data in handen van onbevoegden

Voor ieder van deze risico's worden de maatregelen genoemd die daar betrekking op hebben. De meeste van deze maatregelen zijn nader omschreven in hoofdstuk 3. Voor sommige wordt verwezen naar andere interne of externe informatiebronnen.

2 BEDREIGINGEN, RISICO'S EN DE MAATREGELEN DIE DAAR BETREKKING OP HEBBEN

2.1 Algemene risico's

Bedreiging	Maatregel	Zie
Insolventie	Solvabiliteit > 40%	KVK, gedeponeerde jaarstukken
	Escrow overeenkomst	3.1 Escrow overeenkomst
	Continuïteitsregeling	3.2 Continuïteitsregeling Sentia
Staking	Goede arbeidsomstandigheden	T&T intranet: Arbeidsvoorwaarden
	Continuïteitsregeling	3.2 Continuïteitsregeling Sentia
Slijtage	Onderhoudscontracten	3.7 Afgesloten onderhoudscontracten

2.2 Fysieke bedreigingen

Bedreiging	Maatregel	Zie
Natuurramp	Verzekeringen	3.3 Afgesloten verzekeringen
	Uitwijkfaciliteit	3.4 Uitwijk procedure
	Recovery	3.9 Backup en recovery
Brand	Verzekeringen	3.3 Afgesloten verzekeringen
	Uitwijkfaciliteit	3.4 Uitwijk procedure
	Brandslangen in beide vleugels	
	Recovery	3.9 Backup en recovery
	Brandwerende serverruimte	3.5 Uitrusting serverruimte
	Brandmeldsysteem serverruimte	3.5 Uitrusting serverruimte
	Brandblusinstallatie serverruimte	3.5 Uitrusting serverruimte
Waterschade	Verzekeringen	3.3 Afgesloten verzekeringen
	Uitwijkfaciliteit	3.4 Uitwijkprocedure
	Verhoogde vloer serverruimte	3.5 Uitrusting serverruimte
	Recovery	3.9 Backup en recovery
	Watersensoren serverruimte	3.5 Uitrusting serverruimte
Inbraak/diefstal	Verzekeringen	3.3 Afgesloten verzekeringen
	Uitwijkfaciliteit	3.4 Uitwijkprocedure
	Toegangsbeveiliging pand	3.6 Fysieke Toegangsbeveiliging
	Recovery	3.9 Backup en recovery

2.3 Infrastructurele bedreigingen

Bedreiging	Maatregel	Zie
Storing Electra	Dubbele verdeelinrichting	3.5 Uitrusting serverruimte
	UPS	3.5 Uitrusting serverruimte
	Uitwijkfaciliteit	3.4 Uitwijk procedure
	Recovery	3.9 Backup en recovery
Storing (computer) Systemen	Alle kritische componenten dubbel uitgevoerd	3.5 Uitrusting serverruimte
	Onderhoudscontracten	3.7 Afgesloten Onderhoudscontracten
	Uitwijkfaciliteit	3.4 Uitwijkprocedure
	Recovery	3.9 Backup en recovery
Storing koeling	Dubbel uitgevoerd	3.5 Uitrusting serverruimte
	Onderhoudscontracten	3.7 Afgesloten onderhoudscontracten
	Uitwijkfaciliteit	3.4 Uitwijkprocedure
	Recovery	3.9 Backup en recovery
Storing externe Netwerkverbinding	Onderhoudscontract	3.7 Afgesloten onderhoudscontracten
	Uitwijkfaciliteit	3.4 Uitwijkprocedure

2.4 Data in handen van onbevoegden

Bedreiging	Maatregel	Zie
Eigen personeel	Geheimhoudingsbeding	T&T Intranet: arbeidsvoorwaarden
	Privacy Reglement	T&T Arbeidsvoorwaarden
	Toegangsbeveiliging systemen	3.8 Toegangsbeveiliging systemen
	Pre Employment Screening	
Hacking	Toegangsbeveiling systemen	3.8 Toegangsbeveiliging systemen
Verlies tijdens transport	Aangetekend verzenden	
	Informeren afnemer, politie en (bij GBA) Rijksdienst voor Identiteitsgegevens	

3 BEVEILIGINGS EN CONTINUÏTEITSMAATREGELEN

3.1 Escrow-overeenkomst

Een Escrow-overeenkomst geeft de gebruikers van ICT systemen de zekerheid dat de software die zij gebruiken beschikbaar en onderhoudbaar blijft als de leverancier ervan haar verplichtingen niet meer kan of wil nakomen. De betreffende software komt dan (alleen voor eigen gebruik) beschikbaar voor de afnemers die bij de Escrow-overeenkomst zijn aangesloten, zodat zij zelf, eventueel met de hulp van een andere leverancier, in het toekomstig onderhoud kunnen voorzien.

T&T is voor haar SaaS-toepassingen een Escrow-overeenkomst aangegaan met:

Escrow4All
MediArena 7
1114 BC AMSTERDAM
Telefoonnummer : (020) 342 02 50
Faxnummer : (020) 342 02 59
Internet : www.escrow4all.com
Contractnummer : SW2P09008 voor COMPET&T
SW2P09009 voor WOW
SW2P10043 voor de PR-Service

Alle afnemers van SaaS-diensten van T&T zijn daar automatisch bij aangesloten. In het kader van deze overeenkomst zal T&T minimaal 2 x per jaar een deponering bij Escrow4All doen.

Afnemers ontvangen een certificaat van Escrow4All, waaruit hun deelname aan de regeling blijkt. Zij ontvangen tevens toegangsgegevens tot een portal van Escrow4All waar zij de status van het laatst aangeleverde en geverifieerde depot kunnen raadplegen. Op het portal zijn ook de "Algemene bepalingen" te vinden die op de Escrow- en Continuïteitsregeling van toepassing zijn.

Dit depot zal bestaan uit:
- Broncode (source) van alle programmatuur;
- Alle hulpmiddelen en tools die nodig zijn om deze broncode om te zetten in uitvoerbare programmatuur;
- Alle technische en gebruikersdocumentatie.

Het depot zal corresponderen met de op het moment van deponering operationele versie van de toepassingen. Escrow4All zal de volledigheid, de leesbaarheid en de bruikbaarheid van het depot controleren.

Afnemers hebben (conform de regels uit de "Algemene Bepalingen") het recht om het depot bij Escrow4All op te vragen op het moment dat T&T haar verplichtingen niet meer kan of wil nakomen. De inhoud van het depot mag enkel voor "eigen gebruik" worden aangewend.

3.2 Continuïteitsregeling Sentia

De onder 3.1 genoemde Escrow-regeling geeft de gebruikers van de SaaS-diensten van T&T de zekerheid dat de software in een onderhoudbare vorm beschikbaar komt in het onverhoopte geval T&T haar verplichtingen niet meer na zou kunnen (of willen) komen. Voor toepassingen die zijn geïmplementeerd op eigen systemen van de afnemer volstaat dat om de continuïteit in het gebruik van deze systemen te garanderen. Het kenmerk van een SaaS-dienst is echter dat niet alleen de software, maar ook de data van de afnemer op systemen van de leverancier is opgeslagen. Dat heeft voor de afnemer onmiskenbare voordelen qua bedieningsgemak, en inspanningen op het gebied van systeem- en applicatiebeheer. Er staat evenwel tegenover dat de afhankelijkheid van de leverancier groot is. In theorie is het denkbaar dat met behulp van een Escrow-depot, een recente back-up tape en adequate computersystemen een draaiende toepassing kan worden opgebouwd. In de praktijk echter blijkt dat daar veel meer bij komt kijken. De juiste versies van allerlei hulpmiddelen, de instelling van configuratieparameters, de opzet van firewalls en last but not least "kennis omtrent opbouw en werking van de toepassing" zijn hiervoor noodzakelijk.

Zeker als er haast geboden is (en dat zal nagenoeg altijd het geval zijn als een leverancier niet meer aanspreekbaar is) zal de tijd ontbreken om alle benodigde resources in de juiste combinatie "up and running" te krijgen.

Om de afnemers van de SaaS-diensten van T&T een maximale continuïteitsgarantie te bieden heeft T&T een continuïteitsregeling gesloten met:

Sentia BV
MediArenda 7
1104 BC Amsterdam
Telefoonnummer : +31.88.4242200
Internet : www.sentia.nl
Contractnummer : 12200006

T&T maakt al meer dan 10 jaar gebruik van de diensten van Sentia (en haar zusterbedrijf Indivirtual). Indivirtual heeft de T&T website gebouwd, en Sentia beheert de firewalls van de T&T systemen. Sentia draagt ook zorg voor het beheer van de uitwijksystemen van T&T die in het Amsterdamse "Telecity datacenter" staan opgesteld. Daarnaast wordt Sentia structureel ingehuurd door T&T bij de systeem- en applicatiebeheerwerkzaamheden ten behoeve van de SaaS-diensten van T&T. Sentia is (en blijft) derhalve volledig op de hoogte van de technische architectuur en werking van COMPET&T, WOW en de PR-Service.

Essentie van de overeenkomst is dat Sentia garandeert dat ze de SaaS-diensten van T&T voor de duur van minimaal 3 maanden operationeel zal houden in het geval T&T dat zelf niet meer kan of wil doen. Gedurende die 3 maanden kunnen de afnemers, Sentia, en eventueel T&T zich dan beraden over een definitieve oplossing.

Sentia en T&T hebben daartoe onderling geregeld dat:

- Sentia de garantie geeft aan afnemers van SaaS-diensten van T&T, dat ze die diensten ten minste 3 maanden operationeel zal houden vanaf het moment dat T&T dat zelf niet meer kan of wil;
- Sentia altijd kan beschikken over de infrastructuur die daarvoor nodig is. Als de productiesystemen bij T&T niet meer gebruikt zouden kunnen worden, kan Sentia hiervoor terugvallen op de uitwijksystemen die zij toch al in beheer heeft. Doordat deze systemen middels "data mirroring" zijn gekoppeld aan de productiesystemen is altijd een alternatief voor de productiesystemen voorhanden dat snel operationeel kan zijn;
- Sentia altijd voldoende kennis paraat heeft om de SaaS-diensten operationeel te houden. T&T zal Sentia hiertoe structureel inhuren om te assisteren bij de reguliere beheerwerkzaamheden;
- Sentia betrokken is bij de jaarlijkse uitwijktest die T&T uitvoert, en ook beschikt over de betreffende procedure.

De continuïteits- en escrowregeling zijn in een tripartiete overeenkomst tussen T&T, Escrow4all, en Sentia geregeld. Escrow4all zal afnemers na het sluiten van een geldige serviceovereenkomst voor één van de SaaS-diensten van T&T bevestigen dat de afnemer begunstigde is geworden van de continuïteits- en escrowregeling. Escrow4all zal de afnemer tevens toegangscodes verstrekken tot een beveiligde sectie op haar webportal waar de "Algemene bepalingen" te vinden zijn die op de regelingen van toepassing zijn. Tevens zijn daar de actuele gegevens te vinden over de escrowdeponeringen die T&T 2x per jaar zal uitvoeren.

3.3 Afgesloten verzekeringen

Hoe zorgvuldig er ook gewerkt wordt, in iedere organisatie gaan er dingen mis. Menselijk tekort schieten, technische storingen, calamiteiten en kwaadwillend handelen zijn nooit volledig uit te sluiten. Met een goede risicoanalyse en daarop afgestemde maatregelen zijn deze bedreigingen in belangrijke mate te voorkomen. Er blijft evenwel een kleine kans bestaan dat ondanks alle voorzorgsmaatregelen er schade voor T&T en/of haar afnemers ontstaat. Deze schade zou in potentie zo groot kunnen zijn dat zij het voortbestaan van T&T in gevaar zou kunnen brengen.

T&T heeft met het oog hierop de volgende verzekeringen afgesloten:

Soort verzekering	Verzekeraar	Polis	Dekking
Inventaris	Meeus	5229-MA9828450	Inventaris Pastoriestr. 143/145
Computer	Meeus	5229-MM11083464	Computerapparatuur T&T in Eindhoven en Amsterdam
Aansprakelijkheid	Meeus/Zurich	17209	Algemene Aansprakelijkheid
Beroepsaansprakelijkheid	Meeus/Zurich	17209	Beroepsaansprakelijkheid

3.4 Uitwijk procedure

De productiesystemen van T&T zijn geplaatst in een professionele serverruimte, en omgeven met vele voorzieningen die een hoge beschikbaarheid zoveel als mogelijk moeten waarborgen. Toch zouden zich situaties kunnen voordoen waarin deze systemen (te lang) niet operationeel zijn.

Te denken valt dan aan:
- Natuurramp;
- Zeer langdurige uitval van electravoorziening;
- Dubbele hardwarestoring (nagenoeg alle kritieke componenten zijn dubbel uitgevoerd);
- Schade als gevolg van inbraak/brand, etc.

Ook in het onverhoopte geval T&T niet meer aan haar verplichtingen kan of wil voldoen, zal Sentia (zie 3.2 Continuïteitsregeling Sentia) van deze procedure gebruik maken om op de uitwijksystemen van T&T de SaaS-dienstverlening aan afnemers te continueren.

De uitwijksystemen van T&T zijn ondergebracht in een eigen "kooi" in het "Telecity datacenter" aan de Gyroscoopweg in Amsterdam. Deze systemen zijn (uiteraard alleen door geautoriseerde personen) te bedienen vanaf de kantoorlocaties van T&T en Sentia.

De uitwijksystemen zijn gedimensioneerd op ongeveer 2/3 van de capaciteit van de productiesystemen. Dat geldt voor de hardware, maar ook voor de gereserveerde bandbreedte op de internetaansluiting, en voor de GemNetverbinding die nodig is voor COMPET&T.

In de operationele situatie is op de uitwijksystemen altijd een volledige kopie voorhanden van de productiesystemen.

Dit doordat de volgende voorzieningen zijn getroffen:
- De productiesystemen en uitwijksystemen zijn op hetzelfde moment aangeschaft en van begin af aan voorzien van dezelfde versie van besturingssysteem en middleware;
- De firewalls voor de productie- en uitwijksystemen worden geautomatiseerd gesynchroniseerd;
- Zodra op de productiesystemen een nieuwe versie/release in de productieomgeving wordt geplaatst, gebeurt dat ook op de uitwijksystemen;
- De uitwijksystemen staan middels "data mirroring" continu in verbinding met de productiesystemen in Eindhoven. Hierdoor is op de uitwijksystemen altijd een exacte kopie van de productieomgevingen aanwezig.

Indien moet worden uitgeweken dan zal het daarvoor opgestelde draaiboek worden gevolgd. De uitwijkprocedure wordt 1 x per jaar met medewerking van Sentia, en eventuele afnemers die te kennen hebben gegeven deel te willen nemen aan de test, getest. Het met goed gevolg doorlopen van de stappen van het draaiboek wordt middels parafen in (een kopie van) het draaiboek vastgelegd.

In grote lijnen komt de procedure op het volgende neer.
- Controleer of configuratie uitwijksystemen actueel en consistent is (besturingssysteem, middleware, firewall, release toepassingsprogrammatuur, klantdata);
  Zo niet dan dienen deze eerst geactualiseerd te worden.
- Wijzig IP-adres gekoppeld aan de domeinnamen van de productieomgevingen;
- Vraag eventueel afnemers die te kennen hebben gegeven deel te willen nemen aan de test van alle drie de SaaS-diensten om de toegang en actualiteit van hun data te toetsen;

- Check werking van batchprocedures en externe koppelingen;

De uitwijk procedure is zodanig vormgegeven dat binnen 1 x 24 uur kan worden overgeschakeld op de uitwijksystemen als niet teruggevallen hoeft te worden op de back-up (m.a.w. als de uitwijksystemen actueel en consistent met de productiesystemen zijn). Als dat wel nodig zou zijn kan binnen maximaal 2 x 24 uur worden overgeschakeld.

3.5 Uitrusting serverruimte

De systemen van T&T zijn ondergebracht in een professionele serverruimte. De serverruimte is ingericht, en wordt onderhouden door bedrijven die middels bemiddeling van ICT-Room zijn gecontracteerd.

Bouwkundige voorzieningen
- De ruimte is (behoudens 1 toegangsdeur) geheel gesloten;
- Alle wanden, vloeren plafonds en de toegangsdeur zijn uitgevoerd in minimaal 60 minuten brandwerend materiaal;
- De ruimte is voorzien van een brandvertragend overdrukrooster;
- De toegangsdeur is voorzien van een deurdranger en valt automatisch in het elektronisch slot;
- Het elektronisch slot is alleen te bedienen met een "digitale sleutel";
- De ruimte is voorzien van een verhoogde vloer met een antistatische toplaag, waaronder de koelingskanalen en kabels zich bevinden.

Koeling
- De ruimte is voorzien van 2 gespecialiseerde computerairconditioners;
- Deze zijn zodanig geschakeld dat ze ieder om de beurt een week functioneren;
- Ingeval 1 van de 2 een storing meldt, zal de andere direct actief worden;
- De koelsystemen zijn aangesloten op het alarmsysteem;
- De koelsystemen zijn voorzien van een bevochtiger waardoor ook de vochtigheidsgraad in de serverruimte gereguleerd wordt;
- Er zijn losse sensoren voor temperatuur en vochtigheid die zijn aangesloten op het alarmsysteem.

Brandmeldsysteem
- De ruimte is voorzien van een "Prolnert brandblusinstallatie" (3 cilinders met 44 kg IG-55). Deze installatie zorgt er voor dat ingeval van (vermeende) brand de ruimte wordt gevuld met blusgas, waardoor zuurstof uit de ruimte verdwijnt en (vermeende) brand zou moeten doven;
- De ruimte is voorzien van een Aspiratie detectie systeem (Very Early Smoke detection). Dit signaleert in een zeer vroegtijdig stadium rook, en geeft dan een alarm, zowel via de alarmcentrale als ook middels een flitslicht in de serverruimte zelf. Enkele seconden na het alarm zal de brandblusinstallatie pas in werking treden zodat eventueel aanwezig personeel tijdig de ruimte kan verlaten.

Watersensor

- Onder de verhoogde vloer, alsmede onder de beide koelunits is een watersensor aangebracht, die is aangesloten op het alarmsysteem. Deze sensoren signaleren eventuele wateroverlast vroegtijdig.

Camerabewaking

- De ruimte is voorzien van een tweetal camera's die geactiveerd worden door een bewegingssensor. De opgenomen beelden worden vastgelegd op een harddisk;
- De ruimte is altijd voldoende verlicht om herkenbare opnamen te maken

Elektravoorziening

- Ten behoeve van de elektravoorziening van de productiesystemen zijn twee verdeelkasten aangelegd die voor de spanningsverdeling naar en in de serverruimte zorgen;
- In één van de "feeds" is een UPS van 20kVA opgenomen die de productiesystemen minimaal 9 uur operationeel kan houden als de netspanning wegvalt;
- De UPS is gekoppeld aan het alarmsysteem en signaleert automatisch als de accu's niet meer aan de vereisten voldoen.

Systemen

- De productiesystemen waarop de SaaS-diensten van T&T zijn geïnstalleerd zijn opgebouwd uit industriestandaard INTEL systemen van DELL;
- De systemen zijn gemonteerd in Wright Line Paramount serverracks;
- Voor de externe opslag wordt gebruik gemaakt van een Equallogic storage array;
- Doordat de productiesystemen in een VMware omgeving zijn geconfigureerd zijn ze redelijk eenvoudig uitbreidbaar;
- Alle kritische componenten (voeding, processoren, schijven etc) zijn dubbel uitgevoerd;
- De productiesystemen zijn ondergebracht in een "Enterprise support" contract bij Dell (24x7 telefonisch support, 4 uur on-site).

Externe verbindingen

- T&T beschikt ten behoeve van haar SaaS-diensten over een 3-tal externe verbindingen
  - Een 100mbps glasvezelverbinding van Eurofiber/Signet, gecombineerd met een (failover) 6mbps DSL verbinding;
  - Een 50mbps Entry glasvezelverbinding van KPN (via GemNet);
  - Een 100mbps glasvezelverbinding van KPN t.b.v. datamirroring naar de uitwijklokatie;
- De Eurofiber verbinding wordt normaal gebruikt voor de beveiligde internetcommunicatie met de afnemers van SaaS-diensten. Indien deze verbinding uit mocht vallen, wordt door de router van de ISP automatisch overgeschakeld op de 6mbps DSL verbinding, met behoud van dezelfde IP-adressen.
- De ISP (Signet) is middels twee fysiek gescheiden lokaties gekoppeld aan de Eurofiber backbone;
- De KPN verbinding wordt gebruikt voor de beveiligde communicatie met de GBA mailboxserver, GBA-V, BSN en de TMV.
- De uitwijklokatie in Amsterdam is aangesloten op een internet backbone waarop het Telecity datacenter is aangesloten. Daar is tot 20Mb/s direct beschikbaar voor T&T.
- De uitwijklokatie in Amsterdam beschikt tevens over een 5Mb/s KPN verbinding t.b.v. de communicatie met de GBA (mailboxserver, GBA-V, BSN en TMV);
- Voor zowel de Eurofiber-, als de KPN- verbindingen zijn onderhoudscontracten afgesloten op basis van 24x7 telefonische support, en 4 uur on-site support).

3.6 Fysieke Toegangsbeveiliging

Achter het pand waar T&T is gevestigd bevindt zich een omheind parkeerterrein. Dit terrein wordt in het weekend en van 's avonds 20:00 tot 's morgens 7:00 afgesloten middels een rolhek door de huismeester. T&T heeft 1 sleutel voor dit rolhek, die op een centrale plaats wordt bewaard voor het geval medewerkers 's avonds of in het weekend werkzaamheden moeten/willen verrichten. Overdag is het parkeerterrein afgesloten met een elektrische slagboom. Personen die beschikken over een passende magneetstrip kunnen dan het parkeerterrein betreden. T&T beschikt over 12 magneetstrips, die zijn verdeeld onder de werknemers die (vaak) met auto naar het bedrijf komen. De slagboom kan voor bezoekers ook op afstand worden bediend vanaf de recepties van de bedrijven die in het pand gevestigd zijn. De 12 parkeerplaatsen van T&T zijn voorzien van het T&T logo.

Het pand waar T&T is gevestigd heeft van de buitenzijde 2 toegangsdeuren. Deze zijn overdag gesloten, en kunnen niet zonder sleutel van buitenaf worden geopend. De recepties van de in het pand gevestigde bedrijven kunnen (na verificatie van de bezoeker via een intercom) de voordeur op afstand voor de bezoeker openen. De deur valt daarna (door een deurdranger) automatisch weer in het slot.
Alle T&T medewerkers beschikken over een sleutel voor deze 2 deuren.
T&T houdt kantoor op de tweede verdieping, en heeft daar beide kantoorvleugels gehuurd.
Tussen de trappenhal (waar ook de lift deel van uitmaakt) en de toegang naar de kantoorvleugels staat een glazen pui met dubbele toegangsdeur. Deze is voorzien van een deurdranger, en kan (zonder sleutel) niet worden geopend. De T&T medewerkers beschikken allen over een sleutel voor deze deur.
Verder is de deur voor bezoekers van afstand te bedienen vanaf de receptie.
Achter de glazen toegangsdeur bevindt zich de receptie. Deze wordt buiten kantoortijd afgesloten met een metalen rolhek.
Aan de linker en rechterzijde (eveneens achter de glazen pui bevindt zich de toegang tot de beide kantoorvleugels. De toegangsdeuren daarnaar toe zijn voorzien van dezelfde sloten als die van de glazen pui. De sleutels zijn zonder bijbehorend certificaat niet te dupliceren.
Zodra de laatste medewerker het pand verlaat worden ook deze beide deuren met een metalen rolhek afgesloten.

Het pand beschikt over een alarmsysteem dat is aangesloten op de continu bemande alarmcentrale van SMC (Security Monitoring Centre). Het systeem is primair bedoeld voor het melden van ongeoorloofde toegang. Alle T&T medewerkers beschikken over een eigen code om het alarmsysteem aan- en uit te zetten. De codes zijn uitgegeven door de systeembeheerder, en worden ook door hem bewaard. Hij zorgt er ook voor dat codes worden gewist zodra medewerkers uitdienst treden. In geval van twijfel is via de alarmcentrale te achterhalen door wie (of beter gezegd met welke code) het alarmsysteem is in- of uitgeschakeld. Op het alarmsysteem zijn ook diverse sensoren van de serverruimte aangesloten. De alarmcentrale kan zien welke sensor het alarm veroorzaakt heeft, en waarschuwt ingeval van alarm een T&T medewerker, en eventueel de politie. De alarmcentrale beschikt hiertoe over de huis- en mobiele telefoonnummers van: de directie, de ICT-manager en de systeembeheerder.

De serverruimte is alleen toegankelijk voor personen die beschikken over een digitale toegangssleutel (tag).

De directie beschikt over een door medewerkers ondertekend formulier waarop staat aangegeven welke (digitale) sleutels ze hebben ontvangen. Bij uitdiensttreding dienen deze (digitale) sleutels te worden ingeleverd.

3.7 Afgesloten onderhoudscontracten

Naast de gebruikelijke onderhoudscontracten voor kantoor interieur, heeft T&T de volgende onderhoudscontracten afgesloten die zowel preventief als correctief bijdragen aan de betrouwbare beschikbaarheid van de SaaS-diensten van T&T.

Onderwerp	Leverancier	Contract	Omschrijving
Telefooncentrale	KPN	42335739	Indien op afstand te verhelpen: • Binnen 2 kantooruren Op locatie: • Minor storing: next business day • Major storing: binnen 4 kantooruren • Calamiteit : binnen 2 kantooruren
Serverruimte reiniging	ICT-Room/De Vos	S11494	Eenmaal per 4 weken ESD veilige schoonmaak Eenmaal per jaar "deep clean"
Computersystemen	Dell	-	24x7 telefonisch/4 uur on site (contract is begrepen in aankoopbedrag hardware componenten)
UPS	ICT-Room/Newave	S11494	Onderhoud 1x per jaar Storing 24x7 telefonisch, 8 uur on site
Airconditioning	ICT-Room/T&S	S11494	Onderhoud 2x per jaar Storing 24x7 telefonisch, 3 uur on site
Brandblus installatie	ICT-Room/Hi-safe	S11404	Inspectie/onderhoud 3x per jaar
KPN glasvezel	KPN	1033/71224	24x7 telefonisch/4 uur on site
Eurofiber glasvezel	Eurofiber	RC000214	24x7 telefonisch/4 uur on site

3.8 Toegangsbeveiliging systemen

De toegang tot de productiesystemen van T&T is uiteraard gedegen beveiligd.
Hierbij wordt een onderscheid gemaakt naar:

- medewerkers (en eventuele inhuurkrachten), die deze systemen vanuit de T&T kantoorlokatie en/of vanuit huis kunnen benaderen;
- derden (afnemers en personen die ongewenst toegang zoeken).

Medewerkers kunnen vanuit de kantoorlokatie toegang krijgen tot de productiesystemen op basis van een gebruikersnaam/wachtwoordcombinatie.

Daarbij kan per medewerker worden aangegeven of deze toegang heeft tot:

- Kantooromgeving T&T;
- COMPET&T ontwikkel-, test- en acceptatieomgeving;
- COMPET&T productieomgeving;
- WOW ontwikkel-, test- en acceptatieomgeving;
- WOW productieomgeving;
- PR-Service ontwikkel-, test- en acceptatieomgeving;
- PR-Service productieomgeving.

De systeembeheerder kent (op aangeven van de ICT-manager) deze bevoegdheden toe, en registreert ook de toegekende gebruikersnaam/wachtwoord combinaties. Bij uitdiensttreding zorgt hij er ook voor dat de toegangscombinatie wordt verwijderd.

Medewerkers kunnen bij de systeembeheerder toegang tot de T&T systemen vanuit thuis (of een andere externe locatie) aanvragen. Dit gebeurt dan via een VPN tunnel die met behulp van Open-VPN software wordt opgebouwd. De systeembeheerder kan dit (na goedkeuring door de ICT-manager) inrichten. Medewerkers krijgen voor de toegang de beschikking over een invividueel geprogrammeerde token. Met behulp van een tokencode, alsmede een gebruikersnaam – wachtwoord combinatie, kan men inloggen.

Ook hier registreert de systeembeheerder voor welke medewerkers deze faciliteit is ingesteld, en is hij er verantwoordelijk voor deze mogelijkheid te verwijderen zodra toegang vanuit een externe locatie niet meer nodig of wenselijk is.

De toegang tot de systemen van T&T voor derden is op 3 niveaus beveiligd:

- Allereerst moet het IP-adres dat toegang zoekt worden opgenomen in de firewall van T&T. Alleen geregistreerde IP-adressen krijgen toegang. Iedere afnemer van SaaS-diensten dient hiertoe een vast IP-adres (of een beperkte range IP-adressen) op te geven. Op basis van het IP-adres wordt degene die toegang zoekt doorgeleid naar zijn productieomgeving op de systemen van T&T;
- De toegang wordt beveiligd met een SSL client certificaat dat door T&T wordt uitgegeven. Dit certificaat is getekend door een eigen CA root-certificaat, en wordt door T&T per afnemer gegenereerd. De afnemer is verantwoordelijk voor het verspreiden van dit cliëntcertificaat onder de personen die hij toegang wil geven tot de SaaS-dienst van T&T. Het certificaat dient geladen te worden in de browser(s) van de PC('s) die toegang moeten krijgen tot de systemen van T&T. Indien een afnemer contact zoekt met de productiesystemen van T&T, en als hij afkomstig is van een geregistreerd IP-adres, dan zal hij automatisch worden doorgeleid naar zijn eigen productieomgeving op de systemen van T&T. Daar vindt vervolgens verificatie plaats van het certificaat. Enkel indien dit met goed gevolg plaats vindt, wordt aan de afnemer toegang verleend. De data die over internet wordt uitgewisseld tussen de systemen van T&T en de afnemer is SSL versleuteld;
- Eenmaal binnen op de systemen van T&T, dient de afnemer zich kenbaar te maken met een toegangscombinatie van gebruikersnaam en wachtwoord. Initieel kent T&T aan iedere nieuwe afnemer één combinatie van gebruikersnaam en wachtwoord toe, die wordt gecommuniceerd naar de eerste contactpersoon van de afnemer. Met deze toegangscombinatie kunnen alle functies van de SaaS-toepassing worden uitgevoerd. Deze eerste contactpersoon kan vervolgens andere personen binnen de eigen organisatie autoriseren. Hij kan hierbij ook deelautorisaties toekennen zodat niet iedereen alle functies kan uitvoeren. Vanzelfsprekend krijgt hij ook direct het advies van T&T om het door T&T toegekende initiële wachtwoord te wijzigen.

Naast bovenstaande toegangsprocedure heeft T&T continu een monitoring systeem operationeel. Dit systeem, ORACLE RUEI (Oracle Real User Experience Insight), is direct na de T&T firewall geplaatst en registreert alle data die over de lijn gaat. Hiermee is te achterhalen welke IP-adressen toegang zoeken, wat ze proberen te doen etc. Deze registratie wordt enerzijds gebruikt om performanceproblemen die afnemers ondervinden te onderzoeken, maar is ook heel bruikbaar bij het signaleren van pogingen tot ongewenste toegang tot de systemen.
De systeembeheerder evalueert dit wekelijks, en rapporteert eventuele signaleringen aan de ICT manager.

Alle communicatie die niet plaats vindt via beveiligde verbindingen wordt bewaakt middels actuele virusscanners. T&T is aangemeld bij de "waarschuwingsdienst" van het Nationaal Cyber Security Center van het Ministerie van Veiligheid en Justitie, en reageert alert op signalen die via dat kanaal worden ontvangen. Met ingang van 27 oktober 2014 is de "waarschuwingsdienst" opgegaan in

"veiliginternetten.nl" . Op dit moment is het nog niet mogelijk een abonnement te nemen op een nieuwsbrief. Wel kunnen signalen van "veiliginternetten.nl" gevolgd worden via Twitter. T&T volgt deze.

3.9 Backup en recovery procedures

Door replicatie is altijd een kopie van de gegevens beschikbaar op de uitwijklocatie in Amsterdam.

Daarnaast geldt de volgende backup procedure:

- Dagelijks wordt er een backup vervaardigd naar schijf.
- Deze back-up wordt elke dag via de mirrorlijn (dit is een zogenaamde "private" (besloten) lijn) gerepliceerd naar de uitwijksystemen in Amsterdam.
- In het weekend (van zaterdag op zondag) wordt een full backup vervaardigd. Doordeweeks worden incremental backups vervaardigd.
- De dagelijkse backups worden 1 maand bewaard; de full backups 1 maand tot 1 jaar.
- Het resultaat van deze procedure is dat T&T altijd beschikt over de volgende back-ups:
    - Iedere dag van de afgelopen week ;
    - Een backup van elk weekend van minimaal de afgelopen maand.

  Deze backups zijn zowel beschikbaar op locatie van T&T als op de uitwijklocatie.

Eenmaal per jaar wordt door de systeembeheerder een recoverytest uitgevoerd, waarbij wordt beproefd of vanaf de back-up disks de systemen kunnen worden herladen.
Hij brengt hiervan verslag uit aan de ICT-manager.