Memo kwaliteit en beveiliging binnen het sevenP platform

1 Kwaliteit

sevenP wil op een controleerbare, herhaalbare wijze de kwaliteit van de dienstverlening waarborgen. Wij hebben daarom als middel om dit te bereiken en te waarborgen ons ISO9001 gecertificeerd. Daarnaast stellen wij ons desgewenst open voor formele en informele klantenaudits.

2 Beveiliging

sevenP voert haar dienstverlening op basis van vertrouwen uit. Dat vindt zijn weerslag in interne maatregelen die we hebben genomen om beveiliging op een goed niveau te kunnen handhaven. Wij stellen ons daarnaast open voor opmerkingen en suggesties van onze klanten. Wij worden jaarlijks geaudit op basis van de ISO27001 certificering die wij hebben behaald.

Informatiebeveiliging richt zich op de volgende drie aspecten van de informatievoorziening:

- *Beschikbaarheid* - de informatie moet op de gewenste momenten beschikbaar zijn;
- *Integriteit* - de informatie moet juist en volledig zijn
- *Vertrouwelijkheid* - de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is

Vanuit dit perspectief hebben we technische en organisatorische maatregelen genomen om beveiliging van de ICT-infrastructuur te realiseren. Vanuit de ISO 27001 norm betreft dit 133 controls die getoetst worden. Hieronder een paar voorbeelden.

2.1 Beschikbaarheid

De beschikbaarheid van het sevenP platform is afgesproken binnen de huidige SLA. Dit betreft beschikbaarheid van het systeem buiten de geplande onderhoudsmomenten.

Voor de berekening van de beschikbaarheid wordt de volgende formule gehanteerd:

Aantal dagen in 3 maanden = 365 / 4 = 91,25

Operationele tijd = (91,25 dagen*24uur*60minuten)-/-(vooraf aangekondigd onderhoud in minuten)

Beschikbaarheid = ((Operationele tijd –/- storingsduur in minuten)/Operationele tijd)*100%

sevenP zal de infrastructuur volgens deze normen beschikbaar houden. SevenP is verantwoordelijk voor het functioneren van de onderliggende infrastructuur voor zover deze zich in het datacenter van sevenP bevindt. Het functioneren van de bedrijfsapplicaties is echter niet uitsluitend afhankelijk van de beschikbaarheid van de onderliggende ICT-infrastructuur (het sevenP platform).

sevenP zal al haar kennis en kunde inzetten om de applicatie beschikbaar te stellen en met de partner en/of dealer en/of leverancier samenwerken om storingen op applicatieniveau op te lossen. Bestede tijd aan het uitvoeren van werkzaamheden, die het gevolg zijn van deze interactie tussen de applicatiesoftware en ICT-infrastructuurcomponenten, kan worden gefactureerd.

Het sevenP platform wordt geacht beschikbaar te zijn wanneer de gebruikers zich kunnen aanmelden en zij de ter beschikking gestelde applicaties op het platform kunnen benaderen.

De volgende applicaties worden in het kader van de beschikbaarheid geacht naar behoren te functioneren:

- Microsoft Office
- Outlook / E-mail
- Verkenner

2.1.1 Windows updates en andere software componenten

sevenP voert op haar platform beveiligingsupdates uit, zoals deze maandelijks door Microsoft worden uitgebracht. Deze updates worden regelmatig – minimaal eenmaal per maand- door sevenP uitgevoerd. Ook ten aanzien van andere componenten die de beveiliging kunnen beïnvloeden zoals Java, Flash of Interet Explorer updates voert sevenP een actief preventief patch beleid uit.

2.1.2 Beschikbaarheid en windows updates

Het kan incidenteel voorkomen dat, als gevolg van een Windows update (zoals deze elke maand door Microsoft wordt uitgebracht), een applicatie van een klant niet meer goed functioneert. Het niet beschikbaar zijn van een applicatie als gevolg van een Windows update telt niet mee in de beschikbaarheid zoals hierboven in deze SLA beschreven is.
sevenP adviseert om de applicatie-leverancier te verzoeken bekende problemen als gevolg van Windows updates proactief te melden.
Indien deze informatie tijdig bij sevenP bekend is, kan daarmee rekening worden gehouden bij het installeren van de Windows updates.

In de SLA zijn er verder aanvullende afspraken gemaakt rondom standaard en aanvullend onderhoudmomenten.

2.1.3 Back-up en restore

Back-up
Data van klant wordt elke nacht back-upt. De standaardbewaartermijn van de back-up is 30 dagen. Op verzoek van de klant kan deze bewaartijd eventueel worden uitgebreid. De back-up slaagt minstens 29 maal, gemeten over een periode van 30 dagen.

Restore
Het terugzetten van een enkel databestand vanaf de dataschijven op de fileserver wordt binnen twee werkdagen uitgevoerd. Deze werkzaamheden worden naar redelijkheid kosteloos uitgevoerd.
Het terugzetten van andere bestanden, databases, mail data en dergelijke wordt uiterlijk binnen twee werkdagen uitgevoerd.
Deze restore-werkzaamheden zullen op basis van de bestede tijd tegen het geldende uurtarief uitgevoerd worden.

2.1.4 Beschikbaarheid van data

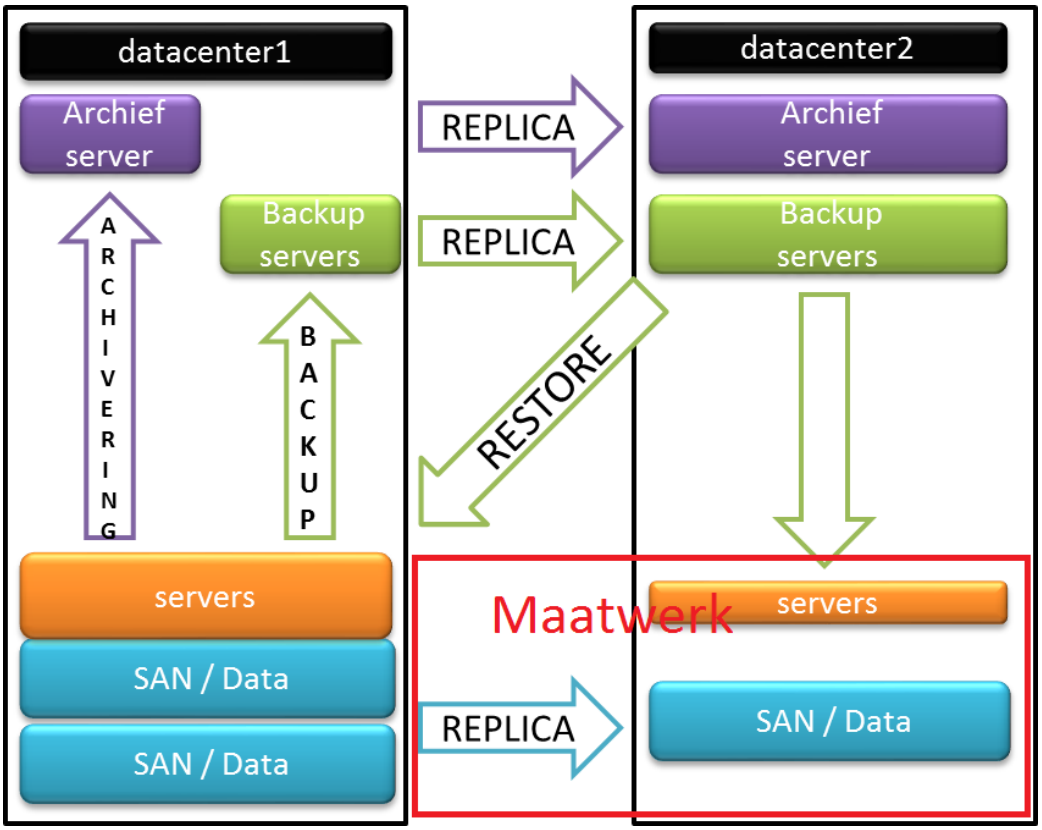
Indien niets anders is afgesproken wordt data geback-upt, zoals beschreven in de paragraaf ‘back-up en restore’. Aanvullend kunnen afspraken gemaakt worden over een eventuele langere bewaartermijn en frequentere back-up.

2.1.5 Disaster recovery

sevenP heeft zaken zodanig geregeld dat de kans op het optreden van een langdurige storing die het hele platform niet beschikbaar maakt zo klein mogelijk is in relatie tot de gehanteerde tarieven.
Hiervoor heeft sevenP de volgende maatregelen genomen:

- Meervoudig uitgevoerde componenten;
- Meervoudige internetverbindingen;
- Onderhouds- en supportcontracten;
- Back-up van data naar twee verschillende locaties.

Ondanks deze maatregelen kan sevenP niet 100% garanderen dat er nooit iets (een disaster) zou kunnen gebeuren waardoor de infrastructuur gedurende langere tijd niet beschikbaar zou zijn.
Onderstaande tekening is een weergave van de technische inrichting.



2.2 Integriteit

2.2.1 Self -service

Door middel van selfservice kan de klant zelf wijzigingen uitvoeren in de toewijzing van resources (waaronder toegang tot applicaties en data en nieuwe gebruikers aanmaken). Ingrijpender wijzigingen, die niet met selfservice zijn geautomatiseerd, voert sevenP in opdracht van klant uit.

2.2.2 Gebruik van accounts en vrijwaring

Het gebruik van een account is voorbehouden aan personen aan wie deze is uitgereikt. sevenP is nooit verantwoordelijk voor of aan te spreken op handelingen die met het account van eindgebruikers zijn uitgevoerd.
sevenP raadt uitdrukkelijk aan bij toegang van buiten kantoor en bij toegang zonder VPN gebruik te maken van extra authenticatie door middel van token of SMS om zo het risico van ongewenste toegang tot bedrijfsapplicaties tot een minimum te beperken.

2.3 Vertrouwelijkheid

Fysieke beveiliging

2.3.1 Verbindingen op kantoor

sevenP adviseert op kantoor gebruik te maken van een beveiligde VPN-verbinding naar het sevenP platform. Toegang van buitenaf kan via een web-interface worden bewerkstelligd, waarbij een additioneel token wordt ingezet voor extra beveiliging, bovenop naam- en wachtwoordbeveiliging.

2.3.2 Fysieke beveiliging

De fysieke beveiliging van het datacentrum ligt op een zeer hoog niveau. Het is vrijwel onmogelijk dat iemand daar binnendringt. Bovendien is de ruimte geconditioneerd en beschermd tegen brand, stroomuitval en waterschade. De datacenter is gecertificeerd volgens ISO27001 en de Payments Card Industry Data Security Standard.

2.3.3 Locatie van de data

De data bevindt zich in datacenters van de Telecity Group in Nederland. De data zal niet zonder toestemming van de klant verplaatst worden buiten Nederland of buiten datacenters van de Telecity Group.
Zie ook http://www.telecitygroup.nl/datacenter-beveiliging.htm

Logische beveiliging

2.3.4 Algemeen

De beheerde ICT-infrastructuur maakt gebruik van de algemene gedeelde sevenP infrastructuur. De logische beveiliging (kort: wie is waarvoor geautoriseerd) van de applicaties en data van klant is geïmplementeerd door de inrichting van een eigen afgeschermde omgeving binnen de sevenP infrastructuur. Dit betekent dat de klant o.a. eigen databaseservers heeft die alleen door de klant te benaderen zijn. Hierdoor kunnen andere gebruikers/klanten niet bij de applicaties en data van de klant. Op deze servers draaien de klantprocessen afgeschermd van andere klanten. De data van de klant is opgeslagen op opslagsystemen in de datacenter. De back-up van de data wordt in twee verschillende datacenters opgeslagen.

2.3.5 Geheimhouding

De medewerkers van sevenP hebben bij het aangaan van hun arbeidscontract een geheimhoudsingclausule ondertekend waarin zij erkennen dat door sevenP geheimhouding is opgelegd van alle bijzonderheden betreffende alle gegevens en informatie van alle klanten voor zover deze niet publiek bekend zijn.

3 Verantwoordelijkheden

Informatiebeveiliging is een zaak die dicht bij elke organisatie staat. sevenP spant zich in om op alle belangrijke gebieden een hoog niveau van beveiliging te bereiken. Echter deze maatregelen zijn slechts een deel van de informatiebeveiliging en moeten deel uit maken van een totaal continuïteits- of beveiligingsplan van de klant. sevenP kan niet verantwoordelijk gehouden worden voor incidenten die veroorzaakt worden door niet het niet naleven of het ontbreken van afspraken door en bij de klant.