Service Level Agreement

Archive-IT SaaS

Datum	**19-05-2019**
Versie	**1.0**

smart. safe. solid.

Inhoudsopgave

Versiehistorie

Auteur	Versie	Datum	Wijziging(en)
Roy Peeters	Concept	02-07-2018	
Hein Boots	1.0	09-05-2019	Aanvullingen n.a.v. onderling overleg

1. Algemeen

1.1 Inleiding

In deze Service Level Agreement (SLA) worden de service levels van Archive-IT nader uitgewerkt nader uitgewerkt/toegelicht. Dit SLA maakt onderscheid tussen software en dienstverlening.

1.2 Begrippen en definities

De in deze SLA met een hoofdletter geschreven begrippen hebben de betekenis zoals opgenomen in onderstaande begrippenlijst, dan wel indien deze hieronder ontbreekt, de betekenis die hieraan is gegeven in één van de andere onderdelen van de Overeenkomst:

Begrip	Definitie
Afdeling Support	Hiermee word de afdeling Support van Archive-IT aangeduid.
Beheer	Het proactieve, reactieve en adaptieve beheer van de SaaS-dienst gericht op de beschikbaarheid en continuïteit daarvan. Waaronder het implementeren van patches, nieuwe releases en nieuwe versies van de onderliggende applicaties en systeemprogrammatuur.
Beschikbaarheid	De norm voor de beschikbaarheid van de SaaS-dienst wordt weergegeven als een percentage van de tijd dat, gedurende het Service Venster, gebruik kan worden gemaakt van de SaaS-dienst. Formule: [(Service Venster – Downtime)/ Service (Venster)] X 100% Onder beschikbaarheid wordt verstaan de technische mogelijkheid tot het kunnen inloggen op de portal van Archive-IT die toegang verleent tot de SaaS-dienst en het bieden van de overeengekomen functionaliteit.
Change	Een wijziging/aanpassing van (een onderdeel van) de SAAS-dienst.
Change Advisory Board (CAB)	Degene die verantwoordelijk zijn voor de fiattering van RFC's verzoeken.
Change Manager	Eindverantwoordelijke van Change Advisory Board.
Downtime	Periode dat de SaaS-dienst niet beschikbaar is binnen het Service Venster.
Incident	Operationele gebeurtenis die geen deel uitmaakt van de standaard werking van de SaaS-dienst en een degradatie van de overeengekomen operationele dienstverlening tot gevolg heeft.
Melding	Algemene vragen, wensen en klachten, niet zijnde een Incident.
Onderhoud	Het uitvoeren van correctieve, adaptieve of preventieve onderhoudswerkzaamheden.

	Denk hierbij aan reguliere updates van onder andere omgeving en software (firewall updates, security patches, operating system etc.).
Onderhoudsvenster	De periode waarin Archive-IT (a) geplande onderhoudswerkzaamheden verricht; en (b) noodzakelijk extra onderhoud verricht waarvoor geen uitstel mogelijk is (denk hierbij aan beveiligingsrisico's e.d.) uitvoert.
Oplostijd	Het aantal werkuren dat ligt tussen het moment van in behandeling nemen van een Incident en het oplossen van het Incident.
Patch of Fix	Een aanpassing aan de onderliggende applicatie(s) of systeemprogrammatuur om fouten te verhelpen.
Probleem	Een ongewenste situatie geïdentificeerd uit gerelateerde Incidenten, waarvan de oorzaak nog niet bekend is.
Responstijd	De tijd die verstrijkt tussen het door Opdrachtgever conform de overeengekomen meldingswijze melden van het Incident en het moment dat de melding in behandeling genomen wordt door Archive-IT.
RFC – Request for Change	Een RFC is synoniem voor een Change Ticket. Een verzoek tot wijziging van (een onderdeel van) de SaaS-dienst.
Service Venster	Periode waarbinnen de SaaS-dienstverlening plaatsvindt minus het onderhoudsvenster.
Werkdagen	Maandag t/m vrijdag met uitzondering van de nationale (Nederlandse) erkende feestdagen (zoals aangegeven op de website van de rijksoverheid).
Werkuren	Van 08:15 uur tot 17:00 uur op werkdagen.
Workaround	Een tijdelijke oplossing voor een Incident.

2. Software

2.1 Indienen incidenten/meldingen

Voor Incidenten/Meldingen met betrekking tot Archive-IT software wendt u zich tot de afdeling Support via de beveiligde **online support portal**. Incidenten/meldingen kunnen 24/7 worden geregistreerd. U kunt in deze online support portal tevens de voortgang en geschiedenis van uw Incidenten/Meldingen inzien.

Heeft u nog geen toegang hiertoe? Dan kunt u dit aanvragen via support@archive-it.nl

2.1.1 Bereikbaarheid supportdesk

De afdeling Support bewaakt de voortgang en terugkoppeling van Incidenten/Meldingen. De afdeling Support is bereikbaar op reguliere werkdagen tussen 8.15 en 17.00 uur. In het weekend- en op feestdagen is er geen bezetting.

In geval van hoge urgentie/spoed kan ook via telefoon (op reguliere werkdagen/werkuren) een Incident worden gemeld/toegelicht. De afdeling Support is bereikbaar via telefoonnummer +31 77 750 11 00.

Archive-IT stelt alles in het werk om Incidenten op te lossen binnen de gestelde Oplostijden (zie hoofdstuk respons- en oplostijden).

2.1.2 Incident management

De volgende stappen worden na ontvangst van een Incident/Melding doorlopen:

- Classificeren en prioriteren
- Bewaking op voortgang tot de uiteindelijke afmelding
- Communicatie van statusinformatie
- Afhandeling van Incidenten/Meldingen

Een Incident kan leiden tot een Request For Change (RFC)

Incidenten/Meldingen kunnen leiden tot een RFC. Het Incident/de Melding zal daarbij tijdelijk on hold worden gezet - met een referentie naar de RFC. In geval van hoge urgentie kan er besloten worden een Workaround voor te stellen of Fix door te voeren binnen de gestelde Oplostijd.

2.1.3 Respons- en oplostijden

De respons- en oplostijden worden gedefinieerd op basis van de opgegeven impact en de classificatie. De combinatie hiervan is bepalend voor de prioriteit.

Vaststellen impactcode

Impactcode	Omvang van het Incident
Hoog	Meer dan 10 gebruikers of bedrijf kritische processen
Middel	2-10 gebruikers
Laag	1 gebruiker

Vaststellen incident classificatie

Impactcode	Gevolg van het Incident
Hoog	Doorwerken is niet mogelijk of het raakt bedrijf kritische processen
Middel	Doorwerken is moeilijk
Laag	Doorwerken is mogelijk

Prioriteitsbepaling

De combinatie van **impactcode** en **classificatie** bepalen de prioriteit van een Incident.

Prioriteit Classificatie			
Impactcode	Hoog (doorwerken niet mogelijk)	Middel (doorwerken moeilijk)	Laag (doorwerken mogelijk)
Hoog (> 10 gebruikers)	I	I	II
Middel (2-10 gebruikers)	I	II	III
Laag (1 gebruiker)	III	III	III

Urgentiebepaling

Afhankelijk van de prioriteit zal de urgentie worden bepaald, volgens onderstaande matrix.

Oplos- en responstijd		
Prioriteit	Responstijd	Oplostijd
I (urgent)	< 1 werkdag	< 1 werkdag
II (minder urgent)	< 1 werkdag	< 1 werkweek
III (niet urgent)	< 1 werkdag	< 1 maand

Archive-IT zal ook, indien de oorzaak van het Incident niet aan Archive-IT is toe te rekenen, zich inspannen om Incidenten op te lossen. Archive-IT hanteert echter geen 'Oplostijden' voor dergelijke Incidenten. Archive-IT is gerechtigd om een vergoeding te vragen voor de door haar in dit kader verrichte werkzaamheden tegen de alsdan bij haar gebruikelijke tarieven.

2.1.4 Rapportages Incidenten/Meldingen

Via de online support portal kunt u de volgende zaken rapporteren:

- Het aantal Incidenten
- Per Incident de “Oplostijd” en “Responstijd”
- Het aantal Incidenten gegroepeerd per prioriteit
- Een lijst met openstaande Incidenten en RFC’s

2.2 Gepland onderhoud

Gepland onderhoud voor de SaaS-dienst vindt buiten werkuren/werkdagen plaats tijdens het onderhoudsvenster.

Onderhoud op Operating System en infrastructuurniveau

Dit betreft (beveiligings)-updates op OS-niveau (Windows updates) en eventueel onderhoud op infrastructuur gebied, welke wordt uitgevoerd door onze hosting partner. Dit onderhoud wordt één week voor de release in de productieomgevingen, eerst uitvoerig door Archive-IT in de acceptatie omgeving getest. Bij gebleken (te verwachten) problemen wordt de uitrol in de Archive-IT productie omgevingen uitgesteld.

In de regel vindt dit onderhoud op woensdagavond/nacht plaats tussen 20:00 uur en 01:00 uur. Per jaar worden zo’n 13 onderhoudsmomenten aangewezen, welke tijdig, doch minimaal 4 werkdagen van tevoren worden gemeld.

Onderhoud Archive-IT software

Tijdens het regulier onderhoud aan de Archive-IT software is de beschikbaarheid niet in het geding (tenzij in uitzonderlijke gevallen, dan wordt dit per omgaande door Archive-IT kenbaar gemaakt) omdat bij de SaaS architectuur van Archive-IT software en het overkoepelende uitrolmechanisme rekening gehouden is met een uitrol zonder gevolgen voor de beschikbaarheid. Mocht er zich desondanks een probleem voordoen kan eenvoudig en binnen korte tijd worden teruggegaan naar een vorige versie.

Dit onderhoud vindt – naar behoefte of noodzaak – plaats buiten de werkuren en wordt tijdig, doch minimaal 4 werkdagen van tevoren gemeld.

2.3 Change- en Release Management

Verzoeken tot wijzigingen in de software dient u eveneens te doen in de online support portal. Archive-IT beoordeelt de voorgestelde wijziging op haalbaarheid en consequenties (waaronder kosten) en bepaalt of/en in hoeverre de voorgestelde wijziging zal worden doorgevoerd. Een wijzigingsverzoek dat niet wordt geaccordeerd, zal met redenen door Archive-IT worden afgewezen.

Wat betreft Changes en releases:

- deze dienen te voldoen aan vigerende wet- en regelgeving
- er zullen nooit basisfunctionaliteiten van de software worden gewijzigd/verwijderd

Bij belangrijke updates worden Release Notes opgesteld.

2.4 Escrow software

Partijen hechten waarde aan continuïteit, voor wat betreft software en gehoste data. U bent daarvoor bij Archive-IT aan het juiste adres. Wenst u nog meer zekerheid: Archive-IT heeft een betrouwbare partij gevonden die een gedegen Escrow voorziening kan leveren. Bij verdere interesse neemt u contact op met Archive-IT voor een verdere invulling van Escrow.

2.5 Serviceparameters SaaS

2.5.1 Beschikbaarheid

De SaaS dienst wordt beschikbaar gesteld binnen een platform van Infrastructure-as-a-Service diensten en met een beschikbaarheidsgarantie* van 99,9% aangeboden. Dit gebeurt in samenwerking met de datacenter partner vanuit datacenters in Nederland.

*In dit kader wordt onder **niet beschikbaar** verstaan: het niet beschikbaar zijn voor alle gebruikers (volledige onbeschikbaarheid).

De onderliggende infrastructuur voldoet aan zware beveiligingseisen, een hoge beschikbaarheid en redundante uitvoering van alle primaire voorzieningen. Alle data en back-up hiervan staat redundant op twee verschillende locaties in Nederland.

Infrastructuur beheer richt zich op het beschikbaar en up-to-date houden van de beheerde servers en de daaraan gerelateerde infrastructuur componenten. Hiervoor kunnen de volgende werkzaamheden worden gedefinieerd:

- Server Beheer
- Security
- Monitoring
- Back-up

2.5.2 Regulier onderhoud

Onder regulier onderhoud wordt verstaan: het uitvoeren van correctieve, adaptieve of preventieve onderhoudswerkzaamheden. Denk hierbij aan reguliere updates van onder andere omgeving en software (firewall updates, security patches, operating system etc.).

2.5.3 Applicatie Services

De applicatie services zorgen voor alle activiteiten met betrekking tot het leveren van applicaties aan eindgebruikers. Applicatie services heeft betrekking op het leveren van applicatie gerichte diensten aan de gebruikers en omvat het plannen, uitvoeren en controleren van de dagelijkse beheertaken. Tevens wordt zorggedragen voor een optimale werking van één of meerdere applicaties, zodat de gewenste functionaliteit van het informatiesysteem te allen tijde voor de gebruikers beschikbaar zijn.

Het betreft de volgende diensten:

- Monitoring: bewaken van de beschikbaarheid van applicaties door monitoren van "key applicatie events"
- Patch Management: aanbrengen van patches, updates en nieuwe versies van de applicatie software
- Back-up & restore data
- Security services
- Beheren van de resources op applicatie level

2.5.4 Datacenter services

Datacenter services verzorgt het operationeel beheer, onderhoud en exploitatie van de ondergebrachte server configuraties in het datacenter, inclusief de bijbehorende Operating Systems (OS), overige besturing software producten en randapparatuur.

De diensten zijn:

- Monitoring: het monitoren van de beschikbaarheid en betrouwbaarheid van de server configuraties van servers geplaatst in het Datacenter
- Incident Management: het afhandelen van storingen met server configuratie(s) volgens het Incident Management proces
- Preventief Onderhoud ter voorkoming van Incidenten
- Patch Management: het aanbrengen van patches en updates op OS en niet applicatie gerelateerde software producten
- Documentatie

2.5.5 Back-up en restore services

Middels de back-up en restore services worden preventief kopieën gemaakt van de aanwezige data. Hierdoor worden deze gegevens veilig gesteld voor het geval de gegevens op de originele locatie verloren gaan of beschadigd raken. Indien nodig kan een back-up weer op de oorspronkelijke locatie teruggeplaatst worden.

De volgende activiteiten worden uitgevoerd:

- Monitoring: het monitoren of de back-up al dan niet gelukt is
- Uitvoeren van back-ups
- Uitvoeren van restores
- Controle: uitvoeren van een periodieke back-up controle

RPO: Wekelijks wordt een full back-up uitgevoerd. Tevens wordt elke 30 minuten een back-up uitgevoerd van SQL-transaction logs. Het maximale dataverlies bij succesvolle back-ups is hierdoor beperkt tot 30 minuten. Back-ups worden gedurende één maand bewaard.

Restoreverzoeken
Archive-IT zal een restore verzoek binnen 2 werkuren na ontvangst hiervan opstarten. De RPO (datum en tijdstip waarnaar terug dient te worden gegaan) van het restore verzoek dient door Opdrachtgever te worden aangegeven en kan maximaal een maand terug zijn. RTO (doorlooptijd van een restore) is afhankelijk van de hoeveelheid data. Gedurende een restore is de Virtual Archive omgeving niet bereikbaar.

Controle maatregelen restore en backups
Minimaal een keer per jaar, vinden test database restores plaats bij het hostingcenter ter controle van het restore proces. Waar nodig worden hierop verbeteracties uitgevoerd. Het backup proces wordt eveneens gecontroleerd, waar nodig worden hierop verbeteracties uitgevoerd.

2.5.6 Security services

Het beveiligingsbeleid is ingebracht in alle services van Archive-IT. Reguliere audits worden uitgevoerd om te controleren of dienstverlening wordt uitgevoerd conform de beveiligingsrichtlijnen. Verder zijn de securityrichtlijnen en procedures voor iedere medewerker van Archive-IT bereikbaar.

Servers en Storage
Het door Archive-IT gebruikte datacenter voldoet aan de algemene eisen ten aanzien van de physical security, zoals toegangscontroles, stroomvoorziening, brandveiligheid e.d. De infrastructuur wordt 24 uur per dag gemonitord, 7 dagen per week, 365 dagen per jaar. Tevens zijn er diverse preventieve beschermingsmaatregelen ingesteld zoals Firewall management, standaard antivirus en patch management.

Netwerk
Het netwerk is het fundament voor veilige applicaties en informatiestromen, en daarmee veilige bedrijfsprocessen. Vooral de integratie van beveiligingsmaatregelen levert voordelen. De netwerkonderdelen moeten zelf beveiliging bieden en intensief samenwerken met de verschillende security oplossingen (beveiligingsoplossingen), zonder dat daardoor de infrastructuur te star wordt.

Firewall Services

Een firewall heeft in een computernetwerken/of op een computer het doel te voorkomen dat ongewenst verkeer van de ene netwerkzone terecht komt in een andere, teneinde de veiligheid in de laatstgenoemde te verhogen. Het beschermde netwerk is vaak een intranet of intern netwerk, en dit wordt beschermd tegen het internet. Het ongewenste verkeer bestaat bijvoorbeeld uit aanvallen van hackers en crackers (krakers), computervirussen, spyware en denial of service attacks.

Firewall services verzorgt de inrichting en het operationele beheer van een firewall, inclusief één dmz-interface (demilitarized zone).

De volgende activiteiten worden uitgevoerd:

- Monitoring: het bewaken van de beschikbaarheid van de Firewall configuraties
- Firewall beheer: het zorgdragen voor operationeel beheer van de Firewall configuraties inclusief het bijbehorende besturing systeem
- Preventief onderhoud ter voorkoming van Incidenten
- Documentatie: het documenteren van de Firewall configuraties, systeemprogrammatuur en procedures

3. Dienstverlening (indien van toepassing)

3.1 Aanvragen dossiers

Het aanvragen van dossiers geschiedt via Archive-IT software Virtual Archive of JIM. De aangevraagde dossiers worden digitaal ter beschikking gesteld of per koerier naar u toegestuurd, dit conform uw opgave.

De diverse mogelijkheden van aanvragen staan in de overeenkomst (offerte) vermeldt.

3.2 Bereikbaarheid afdeling Dienstverlening

Onze afdeling Dienstverlening is bereikbaar op reguliere werkdagen tussen 8.15 en 17.00 uur. In het weekend- en feestdagen is er geen bezetting op de afdeling Dienstverlening.

Aanvragen van dossiers kunnen 24/7 worden gedaan, aanvragen die buiten de reguliere openingstijden zijn ontvangen, worden op de eerstvolgende werkdag in behandeling genomen.

Heeft u vragen/opmerkingen over een dossieraanvraag of wilt een spoedaanvraag ook telefonisch melden dan kan dit via telefoon. De afdeling Dienstverlening is bereikbaar via telefoonnummer +31 77 750 11 00.

4. Exit en retransitieplan

4.1 Scope

Bij het einde van de overeenkomst vindt overdracht van de dienstverlening/data plaats van Archive-IT naar Partijen die de dienstverlening overnemen. De overdracht van de dienstverlening/data tijdens de exit en retransitie gebeurt op basis van de beheersituatie 'as-is'. De bestaande dienstverlening loopt tijdens de exit en retransitie door op basis van de bestaande afspraken in de overeenkomst en bijbehorende bijlagen.

Indien de exit- en retransitie werkzaamheden na het einde van de overeenkomst nog niet zijn afgerond, zullen deze werkzaamheden door Archive-IT – tegen overeengekomen kosten net zolang worden voortgezet tot de finale decharge door opdrachtgever. Reguliere wijzigingen op de bestaande dienstverlening tijdens de exit- en retransitie vinden dan ook plaats binnen die afspraken en vallen niet onder de scope van dit exit- en retransitieplan.

Infrastructurele wijzigingen als gevolg van de overdracht verlopen via de op dat moment geldende standaard changeprocedures. Waar nodig wordt de aanvang van de change voorafgegaan door een inhoudelijke afstemming van de technisch specialisten van partijen.

4.2 Continuïteit

Opdrachtgever zal zo min mogelijk hinder ondervinden door de contractbeëindiging en de exit en retransitie. Partijen committeren zich aan een samenwerking gedurende het exit- en retransitieproces. Archive-IT is er voor verantwoordelijk dat de afgesproken serviceniveaus voor de dienstverlening die onder het beheer zijn van Archive-IT tot de finale decharge door Opdrachtgever en overdracht van de dienstverlening gehandhaafd blijven.

4.3 Organisatie

Ten behoeve van de uitvoering van de exit en retransitie stellen partijen ieder een exit- en retransitiemanager aan. De exit- en retransitiemanagers zijn voor elke partij het aanspreekpunt en krijgen voldoende mandaat om de overeengekomen afspraken in dit exit- en retransitieplan na te komen. Voor wat betreft de reikwijdte van het mandaat dient rekening gehouden te worden met interne mandatering, governanceregels en -beperkingen. De uitvoering van dit exit- en retransitieplan zal voortvarend aangepakt worden. Partijen zullen naar beste vermogen planningen op elkaar afstemmen om zo de exit en retransitie zo snel mogelijk te doen plaatsvinden. Archive-IT stelt voldoende en goed gekwalificeerd personeel en overige resources ter beschikking ten behoeve van de uitvoering van een gecontroleerde exit en retransitie.

4.4 Acceptatie, decharge

Decharge vindt plaats bij acceptatie van overdracht van de betreffende dienstverlening door Opdrachtgever. Bij decharge kunnen er restpunten zijn. Na decharge kijken Partijen welke restpunten nog openstaan en afgewerkt moeten worden. Deze punten worden in een restpuntenlijst opgenomen. Het einde van de exit en retransitie wordt bij acceptatie door Opdrachtgever bevestigd in de vorm van een schriftelijke akkoordverklaring.

4.5 Activiteiten en deliverables

De activiteiten die door Archive-IT in het kader van de exit en retransitie worden uitgevoerd dienen door Archive-IT te worden opgeleverd, alsook de deliverables. In ieder geval dient er een beveiligde en transparante data-export plaats te vinden op een op dat moment gangbare, voor Opdrachtgever leesbare en beveiligde gegevensdrager. Tevens zal Archive-IT dienen mee te werken aan de overdracht van en het verhuizen van de papieren dossiers c.q. archieven.

Archive-IT zal zijn onvoorwaardelijke medewerking verlenen aan het beschikbaar stellen van antwoorden op gestelde vragen binnen overeengekomen termijnen (vragen van opdrachtgever en/of derden betrokken bij de overdracht). Als Opdrachtgever de termijnen niet redelijk vindt en hier last van ondervindt, dan dient hiervoor door partijen een nieuwe termijn afgesproken te worden. De voorzieningen van Archive-IT met betrekking tot data- en informatiebeveiliging blijven gehandhaafd totdat de data en eventuele andere informatie is overgedragen. Archive-IT zal zijn verplichtingen uit dit exit- en retransitieplan niet opschorten als er een conflict ontstaat over de beëindiging van de samenwerking.

4.6 Deliverables Archive-IT

Digitale data (dossiers/images)

- Analyse maken van export en afstemmen met opdrachtgever
- Vastleggen of bepalen van:
  - In welk formaat de data en metadata moet worden aangereikt: xml bestanden erbij of csv
  - Of de historie van de dossiers moet worden meegenomen
  - Of de versies van de digitale documenten moeten worden meegenomen
- Verder vragen uitzoeken, zoals:
  - Hoeveel export runs we dienen uit te voeren (testruns en productierun)
  - Hoe vaak moeten we de data dienen af te leveren en hoe?

Archive-IT zal binnen vier weken na het verzoek tot exit een analyse afronden en uitwerken. Archive-IT start na opdracht binnen twee weken met het maken van de exportservice.

Fysieke data (individuele dossiers/pallets)
Voor wat de vernietiging/opheffing (retourneren) van dossiers per nieuw kalenderjaar kan opdrachtgever een opdracht verstrekken. Deze opdracht dient uiterlijk drie maanden voor het eind van het kalenderjaar zijn verstrekt. Er worden geen beheer- en opslagkosten meer berekend voor het nieuwe kalenderjaar voor de vernietigde populatie.

4.7 Vertrouwelijke informatie

Partijen respecteren ieders belang, intellectuele eigendom en vertrouwelijkheid van informatie.
De geheimhoudingsplicht van Archive-IT blijft ook na de exit- en retransitie bestaan voor onbepaalde tijd.

4.8 Kosten exit/transitie

Archive-IT draagt er zorg voor om bij beëindiging van de Samenwerkingsovereenkomst de exit- en retransitie-activiteiten en deliverables uit te voeren dan wel op te leveren zoals beschreven in dit document. De kosten verbonden aan de exit en retransitie m.b.t. de digitale/fysieke data zijn voor rekening van opdrachtgever. Alvorens een exit- of transitieproject uit te voeren, brengt Archive-IT een offerte uit.

5. KPI's software SaaS software

Nr	KPI	Omschrijving	Norm	Toelichting
1	Beschikbaarheid	Beschikbaarheid van de SaaS omgeving omgeving	99,9%	Gemeten binnen service window 24/7, m.u.v. gepland onderhoud.
2	Security management	Actueel houden antivirus software	100% < 36 uur na uitkomen updates	Nadat een virus/antispam update uitkomt voor de virusscanner wordt deze op de betrefende sytemen uitgerold
3	Security management	Doorvoeren kritieke beveiligingsupdates	100% < 72 uur	Archive-IT zorgt dat meeste recente security updates heeft staan.
4	Backup	Uitvoeren backup en restore	Continue elke 30 minuten	Dagelijkse backup van binnen de gehoste omgeving opgeslagen gegevens van opdrachtgever.
5	Restore	Maximaal gegevens verlies	30 minuten	De maximale tijdsduur waarin toegevoegde of gewijzigde data verloren mag gaan. Geldt voor alle productie data.
6	Performance Virtual Archive	Een beeld is binnen vijf seconden beschikbaar	90% van de opgevraagde beelden is binnen de tijdslimiet van vijf seconden beschikbaar	De definitie is dat het overzicht met gescande dossiers binnen vijf seconden op het scherm staat. Een specifiek dossier aanklikken daarna is ook binnen vijf seconden in te zien. E.e.a. gaat uit van een optimaal beschikbare bandbreedte van het Internet.