INFORMATIE
BEVEILIGINGS
DIENST

Handreiking

BACK-UP EN RECOVERY GEMEENTE

Een van de producten van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)

INFORMATIE
BEVEILIGINGS
DIENST

Colofon

Naam document

Back-up en recovery gemeente

Versienummer

1.1

Versiedatum

01-05-2018

Versiebeheer

Het beheer van dit document berust bij de Informatiebeveiligingsdienst voor gemeenten (IBD).

Copyright

Rechten en vrijwaring

De IBD is zich bewust van haar verantwoordelijkheid een zo betrouwbaar mogelijke uitgave te verzorgen. Niettemin kan de IBD geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. De IBD aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

Met dank aan

De expertgroep en de reviewgemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Wijzigingshistorie:

Versie	Datum	Wijziging / Actie
1.0	September 2013	
1.0.1	Juli 2016	Taskforce BID verwijderd, GBA vervangen door BRP, IT vervangen door ICT en contactgegevens IBD aangepast
1.1	Mei 2018	Update m.b.t. AVG en enkele kleine textuele wijzigingen

Over de IBD

De IBD is een gezamenlijk initiatief van alle Nederlandse Gemeenten. De IBD is de sectorale CERT / CSIRT voor alle Nederlandse gemeenten en richt zich op (incident)ondersteuning op het gebied van informatiebeveiliging. De IBD is voor gemeenten het schakelpunt met het Nationaal Cyber Security Centrum (NCSC). De IBD beheert de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en geeft regelmatig kennisproducten uit. Daarnaast faciliteert de IBD kennisdeling tussen gemeenten onderling, met andere overheidslagen, met vitale sectoren en met leveranciers. Alle Nederlandse gemeenten kunnen gebruik maken van de producten en de generieke dienstverlening van de IBD.

De IBD is ondergebracht bij VNG Realisatie.

Leeswijzer

Dit product maakt onderdeel uit van de operationele variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).

1.1 Doel

Het doel van dit document is een aanwijzing te geven over hoe het back-up en recovery beleid van een gemeente opgezet en uitgevoerd kan worden.

1.2 Doelgroep

Dit document is van belang voor het management van de gemeente, de systeemeigenaren, applicatiebeheerders en de ICT-afdeling.

1.3 Relatie met overige producten

- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
  - Strategische variant van de Baseline Informatiebeveiliging voor Gemeenten
  - Tactische variant van de Baseline Informatiebeveiliging voor Gemeenten
- Informatiebeveiligingsbeleid van de gemeente

Maatregelen tactische variant Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
10.1.1
10.4.1
10.5
10.10.2
12.6
14

Inhoudsopgave

1. Inleiding

De Baseline Informatiebeveiliging voor Gemeenten heeft maatregelen beschreven die te maken hebben met back-up en recovery. Zie hiervoor hoofdstuk 6.5 'back-up en recovery' in het gemeentelijk informatiebeveiligingsbeleid en hoofdstuk 12.6 van de Tactische BIG. Back-up en recovery is een van de maatregelen die een directe link heeft met bedrijfscontinuïteitsbeheer (BCM).

1.1. Doelstelling Back-up en Recovery

Back-up en recovery is een belangrijke beschikbaarheidsmaatregel die ervoor zorgt dat corrupte, verloren of vernietigde bedrijfsinformatie hersteld kan worden. Niet alleen bedrijfsinformatie dient meegenomen te worden in een back-up, maar ook de system states (dit zijn machine instellingen en bijvoorbeeld de (Active Directory) AD (bij Windows). Voor system states, databases, e-mail kunnen andere back-up mechanismen nodig zijn dan de gebruikelijke (bestands) back-up. Back-up en recovery heeft een relatie met calamiteiten en uitwijk. Een goede back-up in een juist schema zorgt ervoor dat een recovery ook daadwerkelijk succesvol kan zijn. De recovery moet minimaal jaarlijks beoefend worden.
Doelstelling is het herstellen van gegevens en/of programmatuur bij verlies of beschadiging door bijvoorbeeld:

- Fouten in software
- Menselijke fouten, zoals bedienfouten
- Corruptie van data of programmatuur
- Herstellen van dienst in geval van incident of een calamiteit (denk aan ransomware of uitwijk)

De indeling van dit document is als volgt:

Hoofdstuk 2: Back-up
Hoofdstuk 3: Recovery
Hoofdstuk 4: Voorbeeld back-up en recovery beleid gemeenten

Aanwijzing voor gebruik

Deze handleiding is qua opzet geschreven om informatiebeveiligingsmaatregelen met betrekking tot back-up en recovery uit te werken en daarbij handreikingen te geven voor het eigen back-up en recovery beleid en aanverwante procedures. Deze handleiding is niet een volledige procesbeschrijving. Back-up en recovery processen worden vaak uitgevoerd binnen de IT-afdeling.

De gemeentelijke beleidsregels met betrekking tot back-up en recovery zijn[1]:

- In opdracht van de eigenaar van de data, maakt ICT reservekopieën van alle essentiële bedrijfsgegevens en programmatuur, zodat de continuïteit van de gegevensverwerking kan worden gegarandeerd;
- De omvang en frequentie van de back-ups is in overeenstemming met het belang van de data voor de continuïteit van de dienstverlening en de interne bedrijfsvoering, zoals gedefinieerd door de eigenaar van de gegevens en systemen;
- Bij ketensystemen dient het back-up mechanisme de data-integriteit van de informatieketen te waarborgen;
- De back-up en herstelprocedures worden regelmatig (tenminste 1 x per jaar) getest om de betrouwbaarheid ervan vast te stellen en hiervan wordt een verslag gemaakt.

De BIG schrijft het volgende over back-up en recovery:
Hoofdstuk 10.1.1 van de BIG gaat over gedocumenteerde bedieningsprocedures:
Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.

1. Bedieningsprocedures bevatten informatie over opstarten, afsluiten, back-up- en herstelacties, afhandelen van fouten, beheer van logs, contactpersonen, noodprocedures en speciale maatregelen voor beveiliging
2. Er zijn procedures voor de behandeling van digitale media die ingaan op ontvangst, opslag, rubricering, toegangsbeperkingen, verzending, hergebruik en vernietiging

[1] Zie ook het algemene informatiebeveiligingsbeleid

Paragraaf 10.4.1 van de BIG beschrijft maatregelen tegen virussen:
Er zijn continuïteitsplannen voor herstel na aanvallen met virussen waarin minimaal maatregelen voor back-ups en herstel van gegevens en programmatuur zijn beschreven.

Paragraaf 10.5 van de BIG beschrijft over back-up het volgende:
Er behoren back-upkopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest conform het vastgestelde back-upbeleid.

1. Er zijn (geteste) procedures voor back-up en recovery van informatie voor herinrichting en foutherstel van verwerkingen
2. Back-up strategieën zijn vastgesteld op basis van het soort gegevens (bestanden, databases, enz.), de maximaal toegestane periode waarover gegevens verloren mogen raken, en de maximaal toelaatbare back-up- en hersteltijd
3. Van back-up activiteiten en de verblijfplaats van de media worden een registratie bijgehouden, met een kopie op een andere locatie. De andere locatie is zodanig gekozen dat een incident/calamiteit op de oorspronkelijke locatie niet leidt tot schade aan of toegang tot de kopie van die registratie
4. Back-ups worden bewaard op een locatie die zodanig is gekozen dat een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-ups
5. De fysieke en logische toegang tot de back-ups, zowel van systeemschijven als van data, is zodanig geregeld dat alleen geautoriseerde personen zich toegang kunnen verschaffen tot deze back-ups

In Paragraaf 10.10.2 van de BIG wordt het volgende geschreven gerelateerd aan back-up en recovery:
Controle systeem gebruik, logging

- De volgende gebeurtenissen worden in ieder geval opgenomen in de logging:
    - Gebruik van technische beheerfuncties, zoals het wijzigingen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of recoveryore

Hoofdstuk 14 van de BIG gaat over BCM en beschrijft het volgende:
Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vooraf afgesproken niveau en binnen in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen.

1. In de continuïteitsplannen wordt minimaal aandacht besteed aan:
    - Identificatie van essentiële procedures voor bedrijfscontinuïteit
    - Wie mag het continuïteitsplan wanneer activeren
    - Wanneer wordt er gecontroleerd teruggegaan naar de standaard situatie
    - Veilig te stellen informatie (aanvaardbaarheid van verlies van informatie)
    - Prioriteiten en volgorde van herstel en reconstructie
    - Documentatie van systemen en processen
    - Kennis en kundigheid van personeel om de processen weer op te starten

Bedrijfscontinuïteitsplannen behoren regelmatig te worden getest en ge-üpdate, om te bewerkstelligen dat ze actueel en doeltreffend blijven.

1. Er worden minimaal jaarlijks oefeningen en/of testen gehouden om de bedrijfscontinuïteitsplannen en mate van readiness van de organisatie te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold

2. Back-up

Back-up is noodzakelijk om gegevens en applicaties te kunnen herstellen in verband met verlies, vernietiging en manipulatie van gegevens of software. Bijvoorbeeld:

- Een virus kan gegevens veranderen overschrijven of ontoegankelijk maken (bijvoorbeeld ransomware)
- Een gemeentehuis kan verwoest worden door brand
- Onjuiste software kan gegevens onbedoeld aanpassen
- Een gebruiker let niet op en gooit te veel weg

Er dient rekening mee gehouden te worden dat in principe van alle data en applicaties back-ups gemaakt moeten worden. Echter er kan een verschil zijn per systeem. Bijvoorbeeld in de gevoeligheid van de gegevens, de belangrijkheid van het proces of de soort data. Daarnaast zijn er ook back-ups nodig van de machine (server) instellingen, de zogenaamde system state back-up. Deze zorgt ervoor dat bij een volledige vervanging van een server de basis instellingen weer snel gerecovered kunnen worden. Meerdere soorten back-ups op verschillende media kunnen bestaan. Back-ups kunnen worden gemaakt op verschillende soorten media. Bijvoorbeeld tape, disk, beschrijfbaar medium (DVD, CD-ROM) of USB sticks.
Vaak wordt voor een back-up tape als medium gebruikt, opslag op disk is ook mogelijk. Er zijn organisaties die kiezen voor online offsite back-up, twee gemeenten zouden er voor kunnen kiezen om over en weer elkaars back-up data op disk op te slaan. Hiervoor is dan wel een goede dataverbinding noodzakelijk.

3-2-1 regel

Voor back-ups wordt algemeen de 3-2-1 regel gehanteerd. Er moeten minimaal drie kopieën zijn, op minimaal twee verschillende media waarvan één op een andere locatie. Het is belangrijk dat er door ICT registratie plaatsvindt van alle back-up media en locaties waar back-ups zich bevinden. Ook dient er een logboek te zijn van uitgevoerde back-ups. De back-up dient qua classificatie dezelfde classificatie te krijgen als het systeem waarvan de back-up gemaakt is, tenzij de back-up op de juiste manier versleuteld is. Als backups off-site worden opgeslagen bij een andere partij moet in principe de inhoud ook bexchermd worden voor onbevoegde toegang door middel van versleuteling. Het toepassen van versleuteling op back-ups vereist een goed ingeregeld sleutelbeheer proces binnen de de gemeente, immers het verliezen van sleutelmateriaal betekent dat de back-up voorgoed onbruikbaar is.

Back-up cyclus

Het maken van back-ups dient in een cyclus te gebeuren. Dit omdat anders het aantal back-up media onbeheerst zal groeien en de administratie ervan ook. Een goede stelregel bij het gebruiken van back-up media is als volgt:

- Het maken van dagback-ups (iedere werkdag) (cyclus wordt wekelijks herhaald)
- Het maken van weekback-ups (één keer per week)
- Het maken van 4-wekelijkse (maand) back-ups. De 4^{e} week is dan de maand, of op de laatste dag van de maand
- Het maken van kwartaalback-ups. Om de 16 weken of op de laatste dag van het kwartaal

Er kunnen ook andere schema's gebruikt worden, of er kan ook gewerkt worden met incrementele back-ups. Dat wil zeggen dat alleen de gewijzigde data wordt geback-upt. Het moet dan wel mogelijk zijn om op basis van een start medium bijvoorbeeld de weekback-up, van de dagen erna incrementele dagback-ups te maken. Het voordeel is dat de back-up sneller klaar is als het om veel data gaat. Het nadeel is dat de tape set altijd in zijn geheel bij elkaar hoort en bij herstel ook vanaf de eerste tape ingelezen moet worden (dat kost meer tijd).
De back-up media worden altijd off site bewaard en alleen de media die nodig is voor de back-up is on site bij de gemeente. Back-up media moeten worden geregistreerd en gecontroleerd op ouderdom en uitgevoerde back-ups worden bijgehouden in een logboek.

Back-upsoorten

Een back-up kan gemaakt worden op een tape, maar tegenwoordig ook steeds vaker op een disk of gelijk offsite en daar op een disk. De manier van back-uppen wordt mede bepaald door de soort van informatie en tot hoe ver

teruggegaan mag worden voor herstel. Als er niets verloren mag gaan, tot het moment van de laatste mutatie of bericht, dan is replicatie een optie, aangevuld met logboeken om bijvoorbeeld gegevens te kunnen reconstrueren.

Als het venster waarbinnen een back-up gemaakt wordt (bijvoorbeeld de uren tussen 19 uur in de avond en 7 uur in de morgen) niet meer groot genoeg is om de gehele back-up te draaien, dan kan een andere back-up strategie uitkomst bieden. Door bijvoorbeeld door de week incrementeel te backuppen en in het weekend volledig. Als dit ook niet meer past, kan er gekozen worden voor een lokale continue back-up op disk en van daaruit een tape back-up of een offsite back-up op disk.
Back-ups moeten zoveel als mogelijk automatisch gemaakt worden wat de kans op menselijke fouten verkleint.
Bedenk ook dat er backups gemaakt dienen te worden van log-informatie.

2.1. Back-up en wetgeving

Het is bijvoorbeeld noodzakelijk om een back-up te maken van belangrijke systemen om te kunnen voldoen aan wetgeving. Nederlandse gemeenten zijn verplicht om na een calamiteit de Basisregistratie personen (BRP) en eventueel andere systemen binnen 48 uur weer volledig operationeel te hebben op een alternatieve locatie. Zonder een goede back-up, procedures en uitwijktesten is dit niet mogelijk.

AVG

Met het back-uppen van gegevens kunnen ook persoonsgegeven worden geback-upt. Op het moment dat op de back-up media persoonsgegevens worden opgeslagen vallen deze back-up media ook onder de AVG-wetgeving. Dit houdt in dat u in bepaalde gevallen verplicht bent om iemands gegevens te verwijderen als diegene hierom vraagt. Bijvoorbeeld als de gegevens niet meer nodig zijn of als die persoon of op het moment dat iemand zijn toestemming intrekt en dat er geen wettelijke basis meer is om deze gegevens te bewaren.

Verder, om persoonsgegevens te beschermen moeten deze worden versleuteld, dus ook op het back-up medium.

Bewaartermijnen back-ups

In principe is een back-up geen digitaal archief. Dat wil zeggen dat de bewaartermijn van back-ups bepaald wordt door de roulatie van de back-upmedia of tapes. Op basis van het bovenstaande schema zijn de termijnen vast te stellen:

- De dagback-up wordt altijd 1 week bewaard voordat deze tape weer op dezelfde werkdag gebruikt wordt.
- De weekback-up wordt 4 weken of een maand bewaard
- De maandback-up wordt 12 weken of een kwartaal bewaard. Dan begint weer een nieuw blok van 3 maanden, tenzij voor alle maanden een eigen tape gebruikt wordt, dan is het een jaar
- De kwartaalback-up of 16 weekse back-up wordt een jaar bewaard voordat deze tape of medium weer gebruikt wordt

Door het bovenstaande schema zijn er bij volledige back-ups altijd 11 versies van data en programmatuur aanwezig.

Back-up media die versleten zijn, of niet meer gebruikt worden, moeten vernietigd worden conform het beleid voor behandeling van digitale media.[2] Er dient een tape roulatie schema te zijn op basis van een veilige marge ten opzichte van de MTBF (mean time between faillure).

Digitaal archief

Een back-up van een digitaal archief, als er een digitaal archief is en de originele stukken zijn vernietigd (substitutie), krijgen back-up tapes van dat archief mogelijk dezelfde status als de reproducties in het archiefsysteem. Deze tapes dienen langer bewaard en gelezen te kunnen worden. Afhankelijk van de soort data gelden dus andere bewaartermijnen en daarmee ook uitdagingen om gedurende die bewaartermijnen de data te kunnen reproduceren. Dit heeft gevolgen voor bijvoorbeeld de apparatuur om de media te kunnen lezen in stand moet worden gehouden.
Kijk voor bewaartermijnen van archieven naar de selectielijst gemeenten en intergemeentelijke organen[3].

2 https://www.informatiebeveiligingsdienst.nl/product/afvoer-ict-middelen/
3 https://vng.nl/selectielijst

2.2. Back-up en SaaS / cloud

Software-as-a-Service (SaaS) en en andere Cloud oplossingen worden steeds vaker gebruikt om informatie te verwerken. Het probleem bij SaaS en cloud is dat de informatie binnen de systemen bij de SaaS en cloud leverancier in de databases verwerkt is. U zult zich bij SaaS en cloud leverancier de volgende vragen moeten stellen en daarop antwoorden moeten krijgen:

- Welke garanties geeft uw SaaS / cloud provider?
- Welke beschikbaarheid levert uw SaaS / cloud provider (en wordt dat gerapporteerd)?
- Heeft u een back-up van de gegevens (uw informatie) van de SaaS/cloud-provider?
- In welk formaat is deze back-up?
- Zijn de gegevens leesbaar, of te importeren in een platform dat u bezit of naar wilt overstappen?
- Heeft u een verwerkersovereenkomst met uw SaaS/cloud leverancier waarin ook de backup is opgenomen?
- Hoe zou u de functionaliteit terug online brengen voor de lokale gebruikers en voor de externe gebruikers?
- Het belangrijkst: is het herstel getest?

Testen back-ups en restore

Back-ups dienen regelmatig te worden getest. Er is niets vervelender dan een onleesbare back-up, zeker op het moment dat deze teruggezet moet worden.

3. Recovery

Recovery is het herstel van gegevens, een applicatie of omgeving naar de staat van vóór het incident. Recovery is noodzakelijk na het verloren gaan van een applicatie of gegevens.

Voor het recoveren is altijd toestemming nodig van de eigenaar van het systeem of de gegevens. In de dagelijks praktijk is het recoveren een normaal proces en maakt onderdeel uit van de ICT service dienstverlening. Bijvoorbeeld om een verloren bestand of e-mail terug te zetten.

Bij grotere incidenten, bijvoorbeeld als een database corrupt is geraakt of een rasnomware aanval, is altijd overleg nodig met de proces / data eigenaar over de opties én hoe verder herstel kan worden uitgevoerd. De proces eigenaar bepaalt en de ICT-afdeling heeft een adviserende/uitvoerende rol.

Het recoveren van applicaties is vaak alleen nodig bij grootschalige recovery van hele systemen. Applicaties veranderen minder vaak dan de data en daarbij komt dat er ook vaak software installatie media zijn. Voor het recoveren van applicaties of systemen zijn goede handleidingen en alle parameters die noodzakelijk zijn om een applicatie of systeem draaiende te krijgen. Denk bijvoorbeeld aan licenties, serienummers, applicatieparameters en hardening sesstings. Het is een goed gebruik om voor (bedrijfskritische) systemen een installatie of security baseline te hebben waarin dit beschreven is.

Alle recovery operaties dienen te worden gelogd. Deze logging kan gebruikt worden binnen andere beheerprocessen om te bepalen of er bijvoorbeeld andere storingen op komst zijn.
Recovery heeft ook een link naar de SLA-afspraken en of de servicelevels gehaald worden of niet.

Business continuity management en planning

Grootschalige recovery wordt vaak uitgevoerd als een of meerdere systemen niet meer beschikbaar zijn. Hiervoor dient een proces uitgevoerd te worden, business continuity management (BCM). Dit proces zorgt ervoor dat in het geval van een serieus incident ICT-systemen weer operationeel kunnen worden en dat alle plannen en procedures voor het recoveren van ICT- diensten in place zijn. Een stap verder gaat Business Continuity Planning (BCP). BCP draagt zorg voor alle processen binnen de gemeente, niet alleen ICT. Zie hiervoor ook de IBD website[4].

Aandachtspunten bij BCM zijn:

- Bepalen van de belangrijkste bedrijfsprocessen door uitvoeren van een BIA (Business Impact Analyses);
- Uitvoeren Risicoanalyses voor het vaststellen van alle bedrijfsmiddelen, bedreigingen, zwakheden en tegenmaatregelen voor iedere dienst;
- Evalueren van alle recovery opties;
- Maken van contingency plannen;
- Testen en reviewen en periodiek herzien van deze plannen.

[4] https://www.informatiebeveiligingsdienst.nl/producten/?zoek=continuiteit&category=

4. Bijlage: back-up en recovery beleid gemeente

Beleidsuitgangspunten Back-up en recovery gemeente

Ten behoeve van de beveiliging van informatie is er back-up en recovery beleid voor alle gemeentelijke voorzieningen. Het doel van dit beleid is te voorkomen dat in geval van gedeeltelijk of geheel verlies of beschadiging van data en /of programmatuur de dienstverlening van de gemeente geen hinder ondervindt.

De gemeente <naam gemeente> hanteert de volgende beleidsuitgangspunten en deze zijn ontleend aan de BIG en aanvullend op het algemene beveiligingsbeleid van de gemeente:

- De gemeente gebruikt back-up en recovery om de gevolgen van de uitval en/of het verlies van informatie te minimaliseren;
- De afdeling I&A / systeembeheer / ICT is belast met het uitvoeren van dit beleid
- De back-ups van alle gemeentelijke informatie, software en besturingssystemen (en instellingen) moeten worden bewaard, zodat de computer besturingssystemen, applicaties en informatie volledig hersteld kunnen worden in geval van een calamiteit. Dit kan worden bereikt met behulp van een combinatie van kopieën, incrementele back-ups, differentiële back-ups en transactielogboeken en systeem baselines;
- De frequentie van back-ups wordt bepaald door de volatiliteit van de gegevens. De bewaartermijn voor reservekopieën wordt bepaald door het kritieke karakter van de gegevens en wetgeving;
- Minstens drie versies van een back-up moeten worden bewaard;
- Er dient minimaal één volledige back-up te worden opgeslagen in een veilige, off-site locatie. Een off-site locatie dient een veilige ruimte in een apart gebouw van de gemeente te zijn of een locatie van een een off-site storage-leverancier, waarbij deze off-site storage door de CISO dient te zijn goedgekeurd;
- Alle gemeentelijke informatie welke staat op werkstations, laptops of andere draagbare apparaten moeten worden opgeslagen op een netwerk file server om back-up mogelijk te maken;
- Vereiste back-up documentatie omvat de identificatie van alle belangrijke gegevens, programma's, documentatie en support items die nodig zijn om essentiële taken tijdens een herstelperiode te voeren. Documentatie van het restauratieproces moet procedures omvatten voor het herstel van single-systeem of applicatiestoringen, alsmede voor een totale datacenter ramp scenario (in geval van uitwijk), indien van toepassing;
- Er zijn geteste ICT-procedures voor back-up en recovery;
- De back-up en recovery documentatie moet worden getest conform de documentatie en deze moet regelmatig worden bijgewerkt om rekening te houden met nieuwe technologie, veranderingen in het bedrijf, en de migratie van toepassingen naar alternatieve platforms;
- Recovery procedures moeten op jaarbasis worden getest;
- Van back-up en recovery activiteiten en de verblijfplaats van de media wordt een logboek bijgehouden;
- De back-up tapes worden vernietigd in overeenstemming met het beleid omtrent behandeling van digitale media van de gemeente.

Aldus vastgesteld door burgemeester en wethouders van *[gemeente]* op *[datum]*

[Naam. Functie] [Naam. Functie]

_____ _____

Kijk voor meer informatie op: www.IBDGemeenten.nl

Nassaulaan 12
2514 JS Den Haag
CERT: 070 373 80 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)
info@IBDGemeenten.nl / incident@IBDGemeenten.nl

VNG Realisatie