

BACK-UP EN RESTORE PLAN PA

Documentbeheer

Eigenaar en beheerder document			
Documenteigenaar			
Functie: PL		Naam: Philip Roodzant	
Document beheerder			
Functie: [naam functienaam]		Naam: [naam document beheerder]	
Versiebeheer			
Versie	Datum	Omschrijving	
0.1	03-04-2023	Eisen lijst aangepast (hoofdstuk 4)	
0.9	06-02-2023	Stempel voorblad toegevoegd	
1.0	21-12-2022	Opmerkingen van OTI Fube verwerkt, Distributielijst en figuur 2 aangepast.	
Vaststelling en periodieke validatie			
Vastgestelde versie	Datum vaststelling	Wie	Functie
[versienummer]	[datum]	[naam vaststeller]	[naam functienaam]
Volgende validatie	[datum volgende validatie]		
Classificatie	Intern		

Managementsamenvatting

Doel van dit document

Dit document vormt de basis voor de back-upplannen van de PA-omgeving. Met als doel inzicht te geven welke applicatiegroepen binnen de PA-omgeving te onderscheiden zijn en welke back-up- en restore plannen noodzakelijk zijn om functie van de PA mogelijk te maken van de PA.

Samenvatting

In dit document is de structuur vastgelegd van de onderliggende documenten welke PA applicatiegroepen, onderdelen/systeemgroepen onder dit plan vallen.

Hoofdstuk **Fout! Verwijzingsbron niet gevonden.** geeft een toelichting op verschillende aspecten van back-ups.

In hoofdstuk **Fout! Verwijzingsbron niet gevonden.** is uitgewerkt en vastgelegd welke applicatiegroepen onderscheiden worden en uit welke, onderdelen/systeemgroepen deze applicatiegroepen bestaand.

Tevens is hier vastgelegd back-up plannen er zijn en wie de eigenaar/beheerder is van de betreffende back-upplannen.

INHOUDSOPGAVE

1. Documenteigenschappen	4
1.1. Goedkeuring	4
1.2. Distributielijst	4
2. Back-up en restore plan PA	5
2.1. Doelstelling van dit document	5
2.2. Inleiding	5
2.3. Bronnen/Documenten van belang	5
2.4. Bereik	5
2.5. Eisen	5
2.6. Documentstructuur	5
2.7. Afwegingen	7
2.7.1. Wat te Back-uppen	7
2.7.2. Wanneer te back-uppen	9
2.7.3. Waar en hoelang back-ups op te slaan	10
3. Systeem decompositie	11
4. Eisen aan dit document	13
5. Afstemming en rapportages	16
6. Verbetercyclus	17
6.1. Algemeen	17
6.2. Aandachtspunten	17
7. Bijlagen overige documenten	18

1. Documenteigenschappen

1.1. Goedkeuring

Dit document heeft de volgende goedkeuringen nodig.

Naam	Rol	Handtekening
Jaap den Haan	Voorzitter Stuurgroep (SG)	

1.2. Distributielijst

Naam	Rol
Casper Braamse	TL
Frank Verhagen	Programma manager (PA BIOlogisch)
Jurian Hage	PL Deelproject
Leo van Oudenaarden	PA Adviseur
Ben Bruinink, Eric Gunst, Jeroen de Vries	Functioneel Beheerders (waterketen)
Jeroen den Ouden, Tom vd Merwe	Functioneel Beheerders (watersysteem)

2. Back-up en restore plan PA

2.1. Doelstelling van dit document

Het doel van dit document is:

- Het vastleggen van de scope qua PA systemen waarvan back-ups gemaakt moeten worden.
- Het bieden van herbruikbare templates om per applicatie- en systeemgroep randvoorwaarden voor PA back-ups uniform vast te leggen.
- Back-up en restore plannen overdraagbaar en beheersbaar te houden.
- Aantoonbaarheid van hoe invulling wordt gegeven aan het beleid en regelgeving en andere kaders (zoals o.a. CSIR) met betrekking tot back-up en restore van PA systemen.

2.2. Inleiding

In dit document wordt de basis gelegd voor de back-up en restore plannen en back-up en restore handboeken van de verschillende applicaties.

Omdat applicaties andere doelen hebben kunnen hier ook andere eisen aan worden gesteld.

Daarnaast kan de architectuur van de verschillende systemen zodanig verschillen dat hier een andere back-up strategie wordt gehanteerd.

Het hoofddoel om de back-ups te maken is om ingeval van incidenten en/of calamiteiten systemen, functies en gegevens efficiënt te kunnen herstellen naar de situatie van voor het incident of calamiteit.

Incidenten en calamiteiten kunnen zijn:

- Kapotte apparatuur;
- Security incidenten;
- Mislukte installaties van software/upgrades/patches;
- Mislukte Applicatie wijzigingen;
- Het moedwillig dan wel per ongeluk verwijderen of beschadigen van bestanden.

2.3. Bronnen/Documents van belang

Tabel 1: Documenten van belang

Documentnaam	Beschrijving
PA BIOlogisch afkortingen en begrippen	Toelichting op afkortingen en begrippen

2.4. Bereik

De reikwijdte van dit document beperkt zich tot de PA omgeving en de software, data en systeemconfiguraties. Back-up en restore plannen en handboeken beperken zich tot het back-uppen van systemen. Afwegingen om applicaties, omgevingen of systemen eerder of later te herstellen anders dan een technische noodzaak worden hier niet gemaakt.

Herstel van infrastructuur zoals netwerken en virtuele platformen zoals ESX en hardware behoren niet tot de scope van dit document.

De onderliggende PA systemen zijn vastgelegd in hoofdstuk 3 Systeem decompositie Tabel 3: Watersysteem, onderverdeling in applicatie- en syste.

2.5. Eisen

Gebaseerd op BIO/CSIR, zie ook hoofdstuk **Fout! Verwijzingsbron niet gevonden..**

2.6. Documentstructuur

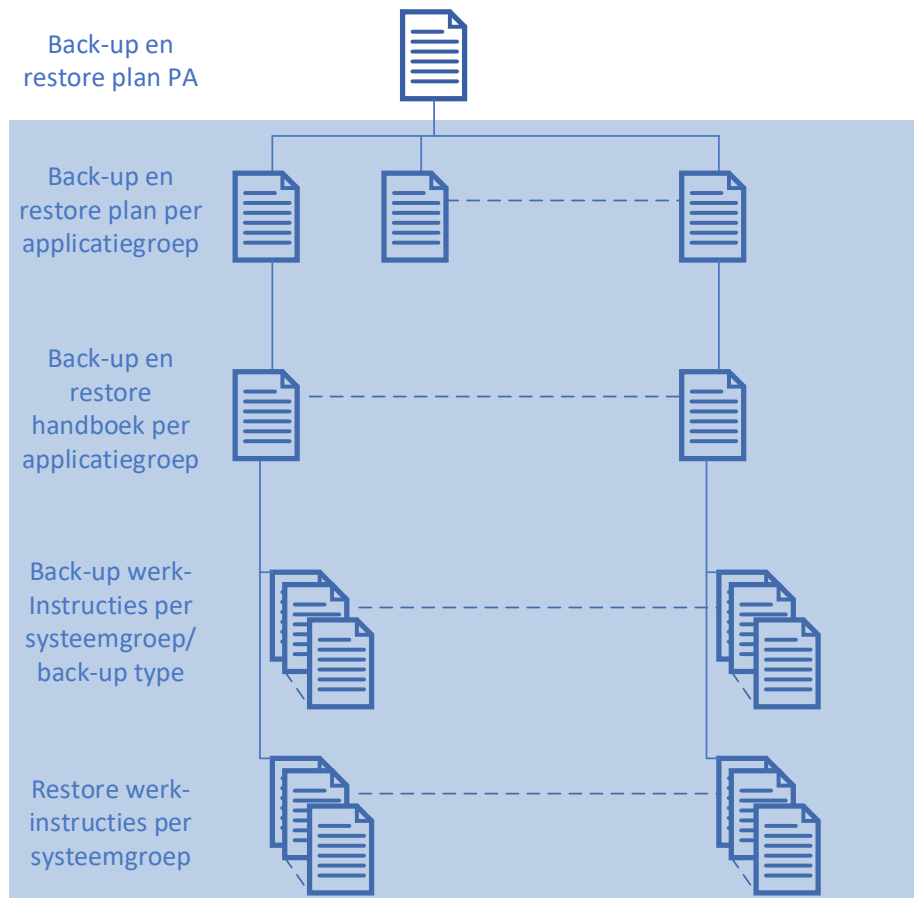
Dit document maakt onderdeel uit van meerdere documenten en is hiervan het top document.

De set aan documenten bestaat uit:

- Back-up en restore plan PA;

- Back-up, restore plan (per applicatiegroep);
- Back-up, restore handboek (per applicatiegroep);
- Back-up werkinstructies (per systeemgroep/back-up type);
- Restore werkinstructies (per systeemgroep).

Zie ook Figuur 1, Document structuur Back-up en restore plan PA



Figuur 1, Document structuur Back-up en restore plan PA

Het "Back-up plan PA" beschrijft de verschillende omgevingen/applicatiegroepen en eigenaar/beheerder van de betreffende omgeving, en de onderliggende Back-up- en restore plannen per applicatiegroep.

De "Back-up en restore plannen per applicatiegroep" beschrijven hoog over de uitgangspunten en randvoorwaarden waar het back-uppen en het herstellen van de betreffende applicatiegroep aan moet voldoen.

In de "Back-up- en restore handboeken per applicatiegroep" is vastgelegd uit welke onderdelen de omgeving/applicatiegroep bestaat welke back-ups er gemaakt worden. Tevens wordt hier voor een deel invulling gegeven aan de uitgangspunten en randvoorwaarden.

In de "Back-up werkinstructies per systeemgroep/back-up type" wordt stap voor stap aangeven hoe een back-up wordt uitgevoerd, compleet met eventuele voorwaarden. Tevens wordt hierin beschreven hoe een back-up leestest wordt uitgevoerd.

In de "Restore werkinstructies per systeemgroep" wordt stap voor stap aangegeven hoe een restore wordt uitgevoerd, compleet met voorwaarden. Tevens wordt hierin beschreven hoe een restore test wordt uitgevoerd.

Het kan voorkomen dat het herstellen van een systeem niet m.b.v. een back-up wordt uitgevoerd maar op een andere wijze, bijvoorbeeld door een rebuild of andere methode. In dat geval zal dit worden aangegeven.

Ook kan het voorkomen dat de Back-up wordt uitgevoerd door een andere partij, bijvoorbeeld ICT of een externe partij (ingeval van bv een SAAS) oplossing. In dat geval zullen de inhoudelijke werkinstructie voor het maken van een back-up een verantwoordelijkheid zijn van de betreffende partij. De werkinstructies voor HHDelfland bestaan dan uit instructies om op verzoek van HHDelfland een back-up te maken. Restore werkinstructies zullen in deze situatie worden opgesteld en bevatten de acties die nodig zijn de restore uit te laten voeren door de derde partij en de acties voor die door HHDelfland moeten worden uitgevoerd het systeem weer in bedrijf te nemen.

2.7. Afwegingen

Deze en onderliggende paragrafen hebben ten doel toelichting te geven op diverse afwegingen en keuzen m.b.t. back-up en restore.

Afwegingen die gemaakt moeten worden zijn:

- Wat te back-uppen;
- Wanneer te back-uppen;
- Waar en hoelang back-ups op te slaan.

Bij de afwegingen zal er rekening gehouden moeten worden met de BIV classificatie en het weerstandsniveau zoals gedefinieerd in de BIO en de in 2.2 Inleiding genoemde incidenten en calamiteiten.

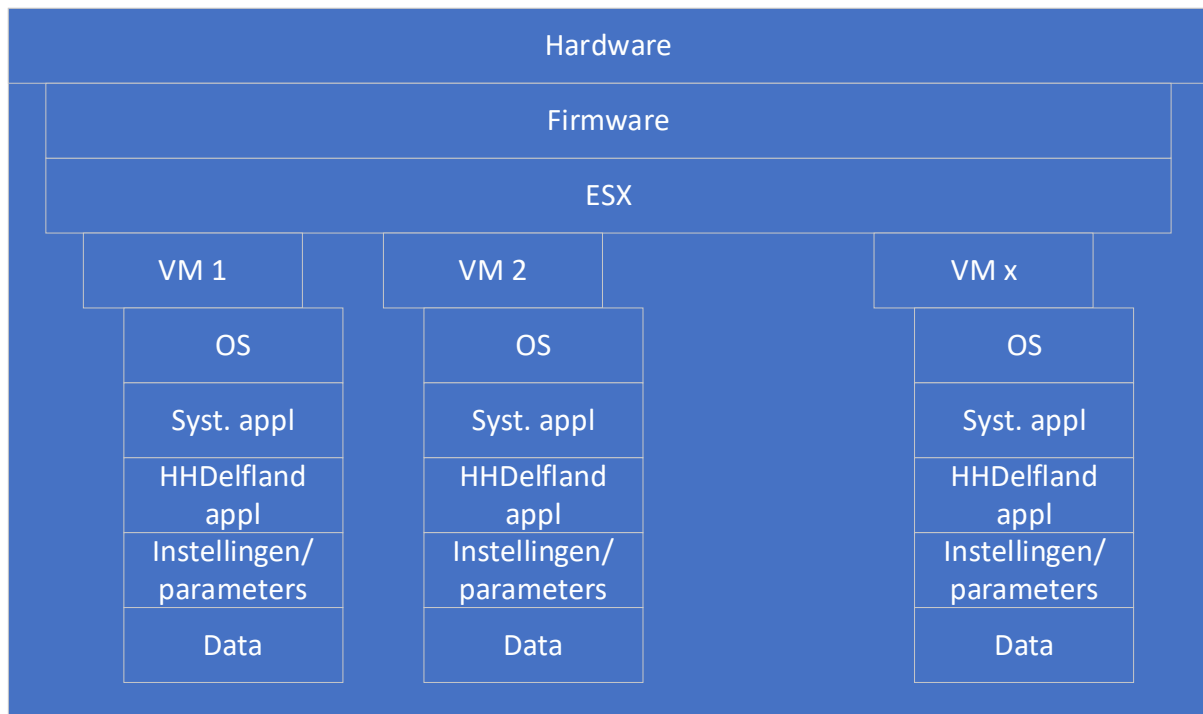
2.7.1. Wat te Back-uppen

Back-ups binnen de PA-omgeving kunnen om meerdere redenen worden gemaakt. Echter de belangrijkste reden is het mogelijk maken om PA-systemen te herstellen als gevolg van: kapotte apparatuur, security incidenten of een andere oorzaak. In veel gevallen kunnen back-ups hierbij helpen echter zijn er soms ook andere methoden om een systeem te herstellen die kunnen voldoen (bv het opnieuw inrichten van een systeem).

Wanneer gekeken wordt naar een systeemdecompositie van een ESX (virtuele omgeving). Kunnen verschillende onderdelen onderscheiden worden bv:

- Alle software die onder de hardware laag aanwezig is;
- VM en alles wat zich daaronder bevindt;
- Systeem applicatiesoftware;
- HHDelfland applicatie/configuratie;
- Instellingen/parameters;
- Data.

Zie ook Figuur 2.



Figuur 2, voorbeeld decompositie ESX omgeving

Daar waar een volledige back-up van alle software die onder de hardware laag aanwezig is, zal voldoen bij kapotte hardware. Zal een back-up van een VM kunnen volstaan bij het verkeerd gaan van een patch en een back-up van de HHDeffland appl. zal in het algemeen voldoende zijn bij de uitrol van bv een nieuwe release van deze applicatie of software aanpassing die moet worden hersteld.

Het kan ook voorkomen dat er meerdere soorten back-ups gemaakt worden voor 1 situatie. E.e.a. afhankelijk van de afwegingen en technische mogelijkheden/beperkingen.

In het uiterste geval zal een back-up niet voldoen en zal een systeem volledig opnieuw moeten worden ingericht via een zogenaamde rebuild procedure. Zaak is dan dat alle software onderdelen aanwezig en beschikbaar zijn om dit mogelijk te maken. Voor systemen die geen data bevatten kan een rebuild procedure ook voldoen in plaats van een back-up werkinstructie/procedure. Zaak is dan wel dat de instructies/procedures up-to-date wordt gehouden en getest.

Tabel 2: Voorbeeld doelen back-up

	Kapotte apparatuur	Security incidenten	Patches voor OS/system SW	Applicatie wijzingen	Moedwillig of per ongeluk Beschadiging van bestanden	motivatie
Een back-up van de ESX omgeving en alle VM's	x	x				Bij defecte apparatuur is het i.h.a. het snelst een Back-up van de gehele omgeving te restoren.
Back-up van de VM's		x	x			Bij een terug rol van een update en of patch kan het terug zetten van een VM snel worden uitgevoerd.
Appl. HHDelfland		x	x	x		Bij een terug rol van een update van de HHDelfland applicatie terug zetten van een de HHDelfland applicatie snel worden uitgevoerd.
Instellingen/Parameters		x	x	x	x	Om instellingen/parameters zeker te stellen
Data	x	x	x		x	Om data zeker te stellen

2.7.2. Wanneer te back-uppen

Wanneer geback-upt moet worden hangt sterk af van de data en eventuele wijzigingen in de betreffende systemen. Bijvoorbeeld wanneer dataverlies van een week catastrofaal is kunnen dagelijkse data back-ups een uitkomst zijn om dit te voorkomen. Systemen die geen data bevatten en niet of nauwelijks gewijzigd worden, zullen kunnen volstaan met minder back-ups. Bijvoorbeeld 1 x per jaar en voor en na een wijziging van het systeem.

Een en ander is afhankelijk van de impact van een incident en wordt in het algemeen bepaald op basis risico's.

2.7.3. Waar en hoelang back-ups op te slaan

De locatie waar back-ups op te slaan:

De locatie waar back-ups opgeslagen worden moet op veilige afstand van het systeem worden opgeslagen zodat een incident geen impact heeft op de back-ups. Dit houdt in dat back-ups zowel fysiek als logisch beveiligd moeten zijn tegen incidenten. Een back-up die online wordt opgeslagen in een ander datacenter is vaak wel fysiek beveiligd maar niet per definitie logisch. Back-ups opgeslagen op een tape of harde schijf opgeborgen in een kluis die staat op een andere locatie dan de systemen waarvan de back-ups zijn is een methode om Logisch en fysiek te scheiden.

Vaak kost het restoren van een tape meer tijd dan het restoren van een online variant.

Ook wordt de 3-2-1 back-up aanbevolen: minstens 3 kopieën, op minstens 2 verschillende typen opslag, minstens 1 kopie off-site bewaard.

Hoelang moeten back-ups worden opgeslagen:

Die afweging heeft onder andere te maken met de relevantie van een back-up, wanneer een data back-up na een maand niet meer relevant is, bijvoorbeeld de data is verouderd en niet meer bruikbaar. Ook kunnen afwegingen zijn back-ups langere tijd te bewaren i.v.m. aantoonbaarheid wanneer deze bijvoorbeeld van uit een wettelijk kader noodzakelijk is. Aandachtspunt is dan wel dat deze data ook teruggelezen kan worden zonder de operatie te verstoren. Systeemback-ups kunnen afhankelijk van de wijzigingen langer of korter bewaard worden. Vanuit de CSIR wordt aangegeven de laatste drie versies systeemimages /back-ups van (ICS)PA/SCADA systemen gewaarborgd moet zijn. Vanuit behoefte en noodzaak kan besloten worden dit aantal te verhogen.

3. Systeem decompositie

De PA omgeving van HH Delfland is op hoofdlijnen te splitsen in drie delen:

- Watersysteem (peilbeheer)
- Waterketen (o.a. waterzuivering)
- Gemeenschappelijke systemen

In de onderstaande tabellen is vastgelegd welke applicatiegroepen en daarmee ook welke back-upplannen er zijn, tevens is aangegeven wie eigenaar is van het betreffende back-upplan.

Tabel 3: Watersysteem, onderverdeling in applicatie- en systeemgroepen

Applicatiegroep	Eigenaar plan	Onderverdeling/ Systeemgroep	Opm.
WS PVSS	OTI/Fube		
		PVSS	
		T-Box	
		Panels	
WS ABB 800xA	OTI/Fube		
		VM's	
		Servers/werkstations	
		AC800M Controllers	
		Advant controllers	Betreffende controllers uit gefaseerd
		800xA Panels	
WS BOS	OTI/Fube		
		Servers/werkstations	
WS TerraTransfer	OTI/Fube		Wordt als dienst afgenomen

Onder de waterketen zijn de volgende applicaties en systemen/onderdelen aanwezig:

Tabel 4: Waterketen, onderverdeling in applicatie- en systeemgroepen

Applicatiegroep	Eigenaar plan	Onderverdeling/ Systeemgroep	Opm.
WK ABB 800xA	OTI/Fube		
		VM's	
		Servers/werkstations	
		AC800M controllers	
		Advant controllers	Betreffende controllers uit gefaseerd
		800xA Panels	
WK Aquaview	OTI/Fube		
		VM's	
WK-Z-Info	OTI/Fube		
		VM	

Onder de gemeenschappelijke systemen zijn de volgende applicaties en systemen/onderdelen aanwezig:

Tabel 5: Gemeenschappelijke Applicaties, onderverdeling in applicatie- en systeemgroepen

Applicatiegroep	Eigenaar plan	Onderverdeling/ Systeemgroep	Opm.
ABB SPH	OTI/Fube		
		VM's	
		Server	
		Data	
ABB Wsus	OTI/Fube		
		VM's	

ABB SPH is een gemeenschappelijke historische database voor zowel de ABB 800xA applicatiegroep van het Watersysteem als de Waterketen.

4. Eisen aan dit document

In dit hoofdstuk zijn de eisen m.b.t. Back-up opgenomen afkomstig uit de BIO en CSIR. Toelichting op de kolommen.

Tabel 6: Toelichting op kolommen Tabel 6: Overzicht eisen

B&R plan [applicatiegroep]	aan de betreffende eis/maatregel wordt invulling gegeven in het Back-up en restore plan [applicatiegroep]
B&R handboek [applicatiegroep]	aan de betreffende eis/maatregel wordt invulling gegeven in het Back-up en restore handboek [applicatiegroep]
Werkinstructies	Eis wordt ingevuld in de werkinstructies van betreffende systeemgroep

Tabel 7: Overzicht eisen

Bron	Ref.	Beschrijving	B&R plan [applicatiegroep]	B&R Handboek [applicatiegroep]	Back-up Werk-instructies	Restore Werk-instructies	Opm.
BIO	12.3.1	Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.		x			
	12.3.1.2	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.	x				Is handreiking
	12.3.1.3	In het back-upbeleid staan minimaal de volgende eisen: a. Dataverlies bedraagt maximaal 28 uur. b. Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.	x				Is handreiking
	12.3.1.4	Opslag van locatie van back-ups: een incident op de ene locatie mag niet leiden tot schade op de andere		x			Is handreiking
	12.3.1.5	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.		x			Is handreiking
CSIR	2..3\IP7	Er dient een operationeel recovery plan te bestaan voor recovery na incidenten of calamiteiten.					
	2..3\IP8	Jaarlijks dienen de incident response en recovery te worden beproefd aan de hand van een actueel oefenplan om te bewerkstelligen dat ze doeltreffend blijven. Onderdeel van de jaarlijkse oefening is het testen van de noodbediening.					

Bron	Ref.	Beschrijving	B&R plan [applicatie- groep]	B&R Handboek [applicatie- groep]	Back-up Werk- instructies	Restore Werk- instructies	Opm.
	2.5.1\AP3	Er dient een recoveryplan te zijn, waarin zijn opgenomen: alle nodige voorzieningen voor back-up en herstel, kopieën van gegevens en programmatuur, evenals benodigde herstelmaatregelen na een incident zoals b.v. een besmetting met malware.			x	x	Vwb de benodigde voorzieningen zijn hier opgenomen.
	2.7.1\TMe22	Onregelmatigheden, incidenten en storingen binnen het back-up en recovery proces moeten worden gemeld bij de Objectverantwoordelijke/ -beheerder.			x	x	
	2.10\BP1	Systeemimages/back-ups worden gemaakt vooraf en na iedere (functionele) systeemwijziging. Wanneer wijzigingen uitblijven wordt de systeemimage/back-up van de laatste versie op jaarbasis vernieuwd. Met deze back-up moet men in staat zijn middels een volledige roll-back naar de werkende situatie terug te kunnen gaan. Indien back-ups gedurende de operationele fase van een object gemaakt moeten worden, dan mag dit het operationele proces niet verstoren.		x			
	2.10\BP2	De integriteit en beschikbaarheid van de laatste drie versies van de ICS/SCADA systemen, programmatuur en besturingssystemen dient gewaarborgd te worden door het maken en testen van systeemimages/back-ups, conform een geborgde procedure: a. Deze back-ups worden opgeslagen op een locatie die zich op zodanige afstand bevindt dat geen schade aan de back-up kan worden aangericht als een calamiteit zich voordoet op de locatie waar het systeem zich bevindt; b. Back-ups en de ruimte waarin ze zijn opgeslagen behoren fysiek goed te worden beschermd volgens dezelfde normen die gelden voor de hoofdlocatie en zijn alleen toegankelijk voor bevoegden; c. Back-ups worden bewaard tot het moment van uitdienstname van het betreffend systeem; d. In geval de back-up terug wordt gezet, dient eventueel ook rekening te worden gehouden met ook het terugzetten van de dynamische gegevens over de systeemstatus.		x			
	2.10\BP3	Er zijn gedocumenteerde herstelprocedures en volledige en actuele registers van back-up kopieën.		x			
	2.10\BP4	Jaarlijks worden de herstelprocedures gecontroleerd en getest om te waarborgen dat ze doeltreffend zijn, dat ze werken en dat ze kunnen worden uitgevoerd binnen de daarvoor overeengekomen tijd. Jaarlijks wordt een recovery test gedaan om te zien of de media nog leesbaar is.		x		x	
	2.10\BP5	De gemelde incidenten en storingsmeldingen inzake back-up worden maandelijks geëvalueerd en waar nodig worden maatregelen getroffen.		x			

Bron	Ref.	Beschrijving	B&R plan [applicatie- groep]	B&R Handboek [applicatie- groep]	Back-up Werk- instructies	Restore Werk- instructies	Opm.
	2.10\BT1	De benodigde voorzieningen voor het back-up en restoreproces worden in overleg ingericht.			x	x	
Groen gemarkeerde cellen worden mogelijk overgeheveld naar een ander document / project							

5. Afstemming en rapportages

Incidenten en afwijkingen met betrekking tot back-ups worden minimaal 1 x per maand geëvalueerd in het PA-overleg.

6. Verbetercyclus

6.1. Algemeen

Dit back-up plan, de onderliggende Back-up en restore plannen en templates dienen minimaal **elk jaar** gereviewd en indien noodzakelijk aangepast te worden.

In Topdesk dient een melding te geven aan de proces-eigenaar om deze review uit te voeren.

6.2. Aandachtspunten

De hier onder vermelde aandachtspunten zijn aandachtspunten waarnaar gekeken moet worden bij de eerst volgende review.

No.	Beschrijving	Toelichting
1	Verbeteracties uit rapportages	Zowel intern als externe rapportages (van leveranciers)
2	BIV classificatie	Is de BIV classificatie gewijzigd
3	Controle van de eisen	Zijn er eisen toegevoegd/ gewijzigd (BIO,CSIR)
4	OTA systemen opnemen	OTA systemen zijn in de eerste oplevering niet opgenomen.
5	Netwerkinfra	(Vpn-concentrators, -Clients) Routers (microtik) etc.
6		

7. Bijlagen overige documenten

Template back-up en restore plan PA [applicatiegroep x]

Template back-up register PA [applicatiegroep x]