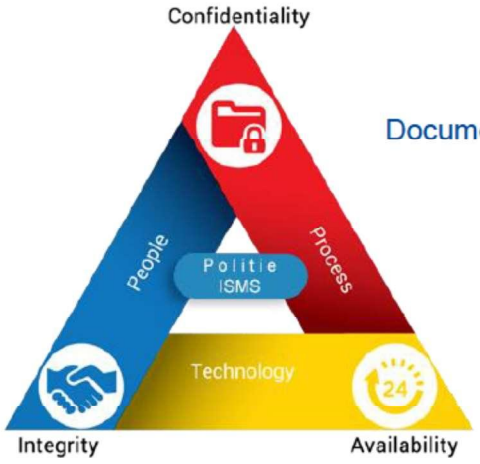
Back-up & Restore/Recovery

Tactisch beleid



Document referentienummer:	ISMS-A12.03.01-01
Document auteur:	Kwartier IB – Cluster Beleid
Document eigenaar:	5.1.2.e
Status:	Definitief
Versie nummer:	2.0
Versie datum:	20 april 2021
Geldigheidsduur:	2 jaar na ondertekening
Rubricering:	Pol. INTERN

Documentinformatie

Document referentienummer:	ISMS-A12.03.01-01
Document auteur:	Kwartier IB – Cluster Beleid
Document eigenaar:	5.1.2.e
Status:	Definitief
Versie nummer:	2.0
Versie datum:	20 april 2021
Geldigheidsduur	2 jaar na ondertekening
Rubricering:	Pol. INTERN
Documentnaam	ISMS-A12.03.01-01 Beleid back up en recovery versie 2.0.docx

Deze tabel vult automatisch

Deze versie vervangt alle voorgaande versies van dit document.

Accordering

Naam	Functie	Handtekening	Datum
5.1.2.e	5.1.2.e i.o.	5.1.2.e	20-05-2021

Distributielijst

Versie	Datum	Verspreidingsvorm	Naam/Functie/Opmerking
1.3	16-11-2020	Via e-mail	Reviewers
1.5	26-01-2021	Via e-mail	Extra review – Review bij Infrabedrijf Tevens naar Kwartiermakers Sector IB i.o.
1.7		Via e-mail	Security tafel
1.8	15-04-2021	Via e-mail	Security tafel ter goedkeuring
2.0	27-05-2021	Via e-mail	Regietafel IV ter goedkeuring en vaststelling

Reviews

Versie	Datum	Door	Functie
1.3		5.1.2.e	Kwartier IB – SOC
		5.1.2.e	Kwartier IB
		5.1.2.e	Productiehuis – Compliance Office
		5.1.2.e	IV Architectuur – Security Architect
		5.1.2.e	RSLM
		5.1.2.e	Kwartier IB
1.5	18-02-2021	5.1.2.e	
1.6	02-03-2021	*PL IS Storage*	
		5.1.2.e	PL IS DLM
		5.1.2.e	PL IS Storage Backup
		5.1.2.e	PL IS Storage Backup
		5.1.2.e	PL IS Storage Backup
		5.1.2.e	PL IS Storage SAN
		5.1.2.e	PL IS Storage NAS
		5.1.2.e	PL IS SA
		5.1.2.e	PL IS LE

		5.1.2.e	LMS
		Securitytafel	Diverse onderdelen
1.6	30-03-2021	5.1.2.e	Team Hosting
		5.1.2.e	Team Hosting
		5.1.2.e	Sector IB i.o. – Beleid & Bewustwording

Versiegeschiedenis

Versie	Datum	Door	Opmerkingen
1.0	14-06-2018	V&C et. al.	Vorige vastgestelde versie
1.1	24-09-2020	5.1.2.e & 5.1.2.e	Interne versie cluster Beleid & Bewustwording
1.2	30-10-2020	5.1.2.e & 5.1.2.e	Interne versie cluster Beleid & Bewustwording
1.3	30-10-2020	5.1.2.e & 5.1.2.e	Versie voor review
1.4	19-01-2021	5.1.2.e	Verwerken reacties reviewers
1.5	26-01-2021	5.1.2.e	Markering maatregelen specifiek tegen cyberaanvallen
1.6	03-03-2021	5.1.2.e	Verwerken reacties van reviewers
1.7	24-03-2021	5.1.2.e	Verwerken reacties n.a.v. Securitytafel Verwerken reactie LMS
1.8	14-04-2021	5.1.2.e	Alle wijzigingen van versie 1.7 na extra consultatie Infrabedrijf verwerkt.
2.0	20-05-2021	5.1.2.e	Definitieve versie, goedgekeurd door Securitytafel

Bijbehorende documenten

Versie	Datum	Omschrijving

Voorwoord

De vorige versie van het “Back-up en Restore beleid” (v1.0 d.d. 14-06-2018) had als hoofdboodschap dat het back-up mechanisme alleen bedoeld was voor het herstellen van de dienstverlening. In het verleden werden back-ups ook gebruikt als archivering en voor het bewaren van de logging. Mede door dit beleid worden de historisch gegroeide verwachtingen ten aanzien van de back-up dienstverlening niet langer gehonoreerd. Het oneigenlijke gebruik van de back-up voorziening is de afgelopen paar jaar afgebouwd.

Mede door het gewijzigde dreigingsbeeld is het noodzakelijk om het Back-up en Restore Beleid te herzien en aan te vullen.

Een voorbeeld van het gewijzigde dreigingsbeeld is de succesvolle aanval met ransomware op de Universiteit van Maastricht[1, 2] eind 2019. Doordat de universiteit geen offline back-ups bewaarde was het voor de aanvaller ook mogelijk om de back-ups te versleutelen. De universiteit had geen mogelijkheid om de versleutelde gegevens van back-ups te herstellen. Uiteindelijk heeft de universiteit de aanvaller betaald om de decryptiesleutel te krijgen om daarmee de versleutelde bestanden te herstellen.

Een ander voorbeeld is de geslaagde ransomware aanval in december 2020 op de gemeente Hof van Twente[3]. Bij deze aanval werd niet alleen productiedata versleuteld. Ook de back-ups waren door versleuteling onbruikbaar geworden.

[1] Zie website van de universiteit voor de lessons learnt: https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt [laatst gezien 03-03-2021]
[2] Zie rapport: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2020/06/12/definitief-rapport-cyberaanval-universiteit-maastricht-21pj-docx/definitief-rapport-cyberaanval-universiteit-maastricht-21pj-docx.pdf [laatst gezien: 03-03-2021]
[3] Zie: https://www.hofvantwente.nl/actueel/veelgestelde-vragen-cyberaanvalhack-gemeentehuis [laatst gezien: 03-03-2021]

Inhoudsopgave

Lijst van Afbeeldingen

Lijst van Tabellen

1. Inleiding

Een goed back-up en restore/recovery proces zorgt ervoor dat er na een incident snel weer de juiste informatie teruggeplaatst kan worden, er zo min mogelijk informatie verloren gaat en dat de dienstverlening na uitval weer hersteld is.

1.1. Doelstelling Back-up en Restore/Recovery

Back-up en restore/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 bij Windows). Voor system states, databases, e-mail kunnen andere back-up mechanismen nodig zijn dan de gebruikelijke (bestands) back-up. Back-up & Restore/Recovery heeft een relatie met calamiteitenbeheersing en uitwijkvoorzieningen. Een goede back-up in een passend schema zorgt ervoor dat een restore/recovery ook daadwerkelijk succesvol kan zijn. Die restore/recovery moet minimaal jaarlijks getest worden.
Doelstelling is het herstellen van gegevens, configuraties en/of programmatuur bij verlies of beschadiging door bijvoorbeeld:

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

Back-up en Restore/Recovery moet ingericht worden om de (IV-)dienstverlening na calamiteiten te herstellen.

1.2. Kaders

Dit document is een uitwerking van de gestelde kaders voor Informatiebeveiliging.
Die kaders zijn vastgelegd in:

- Informatiebeveiligingsbeleid 2014 – 2017 (versie 1.1b – januari 2019)
- Informatiebeveiligingskader v1.0a 2014 (versie 1.0a – 29 januari 2014)
- Enterprisearchitectuur Informatiebeveiliging (versie 2.0 7 mei 2019)

1.2.1. ISO27001 & ISO27002 & BIO

Ondanks dat informatiebeveiliging in principe op basis van risicoafweging wordt uitgevoerd kunnen een aantal (standaard) controls houvast bieden voor lijnmanagers om beslissingen te kunnen nemen. Om deze houvast te bieden en om consistentie te vergroten tussen verschillende bestuursorganen is de Baseline Informatiebeveiliging Overheid (BIO) opgesteld.
Binnen de politie is de Baseline Informatiebeveiliging Overheid (BIO) aangenomen als handreiking voor bepalen van maatregelen om risico's te mitigeren. De BIO is gebaseerd op de Nederlandse normen NEN-EN-ISO/IEC 27001:2017 en NEN-EN-ISO/IEC 27002:2017.

Onderstaande doelstellingen en maatregelen zijn in dit document nader uitgewerkt.

1.2.2. Uit ISO27001 – Annex A

A.12.3.1	Back-up van informatie	Beheersmaatregel Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.

Tabel 1 - ISO27001 - Annex A

1.2.3. Uit BIO v1.04

12.3.1	**Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.**		
12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	12.3.1.1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld.
12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	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.
12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	12.3.1.3	2 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.
12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	12.3.1.4	Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.
12.3.1	Back-up van informatie: Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.	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.

Tabel 2 - BIO

1.3. Doel van dit document

Het doel van dit document is om ten aanzien van back-up en restore/recovery de algemene beveiligingsdoelstellingen, zoals verwoord in bovengenoemde documenten; 'Beleidsdocument Informatiebeveiligingsbeleid 2014-2017' en 'Beleidsdocument Informatiebeveiligingskader v10a', te vertalen naar concrete doelstellingen voor de Diensten ICT/IM.

Het doel van het beleid voor back-up en restore/recovery is het beschermen tegen verlies van gegevens, configuratie en programmatuur. In geval van gedeeltelijk of geheel verlies of beschadiging van data en/of programmatuur, ondervindt de dienstverlening van de politie minimale hinder.

Voor het bereiken van dit beleidsdoel wordt dit vertaald naar concrete tactische kaders voor de Diensten ICT/IM om Back-up & Restore/Recovery in te richten en de benodigde activiteiten te verrichten. Deze doelstellingen geven houvast om Back-up & Restore/Recovery in te richten en/of bij te stellen.

2. Back-up & Restore/Recovery

In de IV-Diensten catalogus (IDC) zijn de CIO en de diensthoofden van de Dienst ICT en Dienst IM overeengekomen welke IV dienstverlening wordt geleverd aan de Politie en haar partners.
In de IDC zijn de beschikbaarheidseisen voor de dienstverlening vastgelegd. Afspraken met betrekking tot back-up en Restore/Recovery zijn per dienstverlening vastgelegd in de Dossiers Afspraken en Procedures (DAP's)

Een back-up is een kopie van de data op een medium. Met een back-up wordt data beschermd tegen bijvoorbeeld het per ongeluk verwijderen van bestanden of technische problemen. Dankzij een back-up is er data om op terug te vallen. De originele gegevens kunnen in de loop der tijden veranderen en moeten daarom regelmatig opnieuw worden geback-upt om deze gegevens veilig te stellen (back-up cyclus).

Met een restore kan de data die met behulp van een back-up veilig gesteld is worden teruggezet naar een eerder bekende en stabiele status.

Om de back-up cyclus goed in ter regelen moet per IV-dienst het maximale toegestane dataverlies (RPO) en de maximale hersteltijd (RTO) vastgesteld zijn.

Back-up alleen is géén Disaster Recovery. Back-ups zijn vaak een laatste redmiddel in het proces van disaster recovery.

2.1. Ransomware

Dit document is geschreven met in het achterhoofd dat het in principe niet uitmaakt op welke wijze de data verloren is gegaan. Er is geen verschil of de data verloren is gegaan door natuurlijke calamiteiten (brand, overstroming, aardbeving), menselijke fouten (configuratiefout of per ongeluk bestanden verwijderen) of cyberaanvallen (zoals ransomware). Het Back-up en Restore/Recovery beleid en de daaruit voortvloeiende inrichting van processen en procedures moet bij alle calamiteiten geschikt zijn om de dienstverlening weer op orde te krijgen.

Van alle in dit beleid genoemde uitgangspunten zijn er een aantal die extra aandacht verdienen. Zij zijn nodig om de gevolgen van cyberaanvallen zoals ransomware te kunnen pareren. Omdat deze uitgangspunten mogelijk ingrijpende consequenties hebben qua financiën (extra kosten voor hard- en/of software) en procesinrichting (extra handelingen en controles), zijn die uitgangspunten *op deze manier* aangegeven.

3. Informatiebeveiligingsbeleid Back-up & Restore/Recovery

3.1. Gehanteerde brondocumenten

Versie	Datum	Omschrijving	Verwijzing
1.1b	Januari 2018	Informatie Beveiligingsbeleid Nationale Politie	https://intranet.politie.local/downloads/1206/informatiebeveiligingsbeleid-2014-2017.html
1.0a	29-01-2014	Informatiebeveiligingskader nationale Politie	https://intranet.politie.local/downloads/1206/informatiebeveiligingskader.html
27001: 2020	Februari 2020	NEN-EN-ISO/IEC 27001:2017+A11:2020 nl [4]	https://connect.nen.nl/standard/openpdf/?artfile=3626254&RNR=3626254&token=3af6eb8d-7bac-4b3c-8600-af336cadb053&type=pdf#pagemode=bookmarks
27002: 2017	Maart 2017	NEN-EN-ISO/IEC 27002:2017 nl	https://connect.nen.nl/standard/openpdf/?artfile=3565433&RNR=3565433&token=10775015-a059-4bb6-b5d0-09f5c1b8123f&type=pdf#pagemode=bookmarks
1.04	04-11-2019	Baseline Informatiebeveiliging Overheid (BIO)	https://agora.portal.politie.local/sites/150423135311/SiteAssets/Kennisbank/09.%20Uitvoeringsregelingen/ISMS-A05.01.01-01-Baseline%20Informatiebeveiliging%20Overheid-v1.04.docx
1.0	15-04-2020	BIO Addendum voor de Politie	https://agora.portal.politie.local/sites/150423135311/SiteAssets/Kennisbank/09.%20Uitvoeringsregelingen/ISMS-A05.01.01-02-Addendum%20BIO-Politie%20Specifieke%20Maatregelen-v1.1.pdf
2.0	07-05-2019	Enterprisearchitectuur Informatiebeveiliging	https://intranet.politie.local/downloads/2000/informatiebeveiligingsarchitectuur.html
	27-04-2016	Algemene Verordening Gegevensbescherming (AVG)	https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32016R0679&from=NL
	01-01-2020	Wet Politie Gegevens	https://wetten.overheid.nl/BWBR0022463/2020-01-01
2.0	23-04-2018	Privacy en Security by Design – uitvoeringskader voor de omgang met gegevens	https://agora.portal.politie.local/sites/150311110511/Onze%20documenten/Privacy%20and%20Security%20by%20Design/Uitvoeringskader/Privacy%20and%20Security%20by%20Design%20-%20Uitvoeringskader%20v2.0.pdf
1.0	13-02-2020	Beleid Bewaartermijnen	https://agora.portal.politie.local/sites/150311110511/Onze%20documenten/Privacy%20and%20Security%20by%20Design/Bewaartermijnen.pdf
1.0	12-12-2017	Uitvoeringsregeling vernietigen elektronische gegevensdragers	https://agora.portal.politie.local/sites/150423135311/SiteAssets/Kennisbank/09.%20Uitvoeringsregelingen/ISMS-A05.01.01-02-Addendum%20BIO-Politie%20Specifieke%20Maatregelen-v1.1.pdf
2.2	December 2020	IBD Handreiking Backup-up en recovery	https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2020/12/202012-Handreiking-Back-up-en-recovery-gemeente-v2.2.docx
1.0	Maart 2015	Rubriceringsregeling Politie 2015	https://intranet.politie.local/downloads/1206/rubriceringsregeling.html
1.1	07-07-2020	Hardening beleid	https://agora.portal.politie.local/sites/150423135311/SiteAssets/Kennisbank/09.%20Uitvoeringsregelingen/ISMS-A12.06.01-03-beleid%20Hardening%20v1.1-Definitief-20200707.pdf
1.1	10-07-2017	Referentiemodel Beveiliging Politiegebouwen (RmBPG)	https://agora.portal.politie.local/sites/1606071131/Gedeelde%20%20documenten/Referentiemodel%20beveiliging%20politiegebouwen%20RmBPG%20v1_1_d.d.%2010-07-2017.pdf#search=rmbpg

Tabel 3 - Gehanteerde brondocumenten

[4] Deze en andere NEN-normen zijn beschikbaar bij NEN onder de licentie van de politie

3.2. Relaties / samenhang

Dit Back-up & Restore/Recovery Beleid heeft relaties met de volgende onderwerpen:

- Business Impact Analyse (BIA)
- Business Continuity Management
- IT Service Continuity Management (ITSCM)
- Business Continuity Planning
- Service Level Agreements
- IV Diensten Catalogus
- Incidentmanagement
- Hardening van systemen

3.3. Begrippen

Voor de uitleg van begrippen wordt verwezen naar "Security Woordenboek – van cybersecurity naar Nederlands" uitgegeven door Cyberveilig Nederland. Termen en begrippen die niet in het Security woordenboek voorkomen of een nadere uitleg nodig hebben zijn hieronder opgenomen.

Begrip	Definitie
Dienstverlening Derden	Onderdeel van de Dienst ICT die diensten verleend aan derde partijen
Back-up	Een reservekopie van gegevens of digitale systemen. Hiermee kan men gegevens of systemen herstellen als het origineel beschadigd of weg is. Een back-up is niet bedoeld voor archivering of lange termijn opslag.
BCM	Business Continuity Management.
BIA	Business Impact Analyse.
Restore/Recovery	Restore/Recovery is het herstel van gegevens, een applicatie of omgeving naar de staat van vóór het incident. Restore/Recovery is noodzakelijk na het verloren gaan van een applicatie of gegevens. Voor dit herstel wordt gebruik gemaakt van een actuele back-up.
EBO	Eigen Beheerde Omgeving.
LMS	Landelijke Meldkamer Samenwerking.
RPO	Recovery Point Objective: Het maximale dataverlies gemeten in uren.
RTO	Recovery Time Objective: De maximale hersteltijd na een incident gemeten in uren.

3.4. Toepassingsgebied

Dit beleid is van toepassing op alle onder de Dienst ICT ressorterende infrastructuur en dienstverlening. Dit beleid geldt ook voor de Eigen Beheerde Omgevingen (EBO's).

Dit Back-up en Restore/Recovery Beleid geldt voor de volgende functies:

- Back-up
- Restore
- Ondersteuning van Disaster Recovery.

Back-ups zijn niet bedoeld als (gedeeltelijke) vervanging voor archivering en logging.

3.5. Verantwoordelijkheden

De dienst-, systeem- of applicatie eigenaar is verantwoordelijk voor het aangeven van de eisen die gesteld worden aan de Back-up & Restore/Recovery mogelijkheden. Deze eisen volgen uit de Business Impact Analyse en de opgestelde Business Continuity Plannen die voor het systeem, de dienst of applicatie is opgesteld.

De Dienst ICT is belast met het uitvoeren van het back-up, restore en recovery beleid voor de onder de Dienst ICT ressorterende infrastructuur (ook als deze infrastructuur wordt ingezet ten behoeve van LMS en Dienstverlening Derden.

De Eigen Beheerde Omgevingen (EBO's) zorgen zelf voor uitvoering van dit beleid.

Er is vastgelegd welke afdelingen/teams verantwoordelijk zijn voor de uitvoering en de correctheid van de back-up, restores en recovery op de diverse delen van de infrastructuur (applicatie, databases, operating systems, storage).

3.6. Beleidsregels Back-up & Restore/Recovery

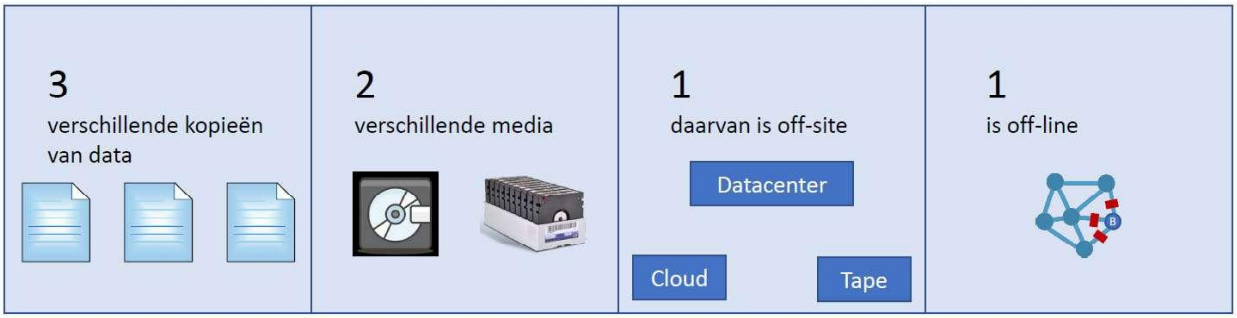
De politie hanteert voor Back-up & Restore/Recovery onderstaande beleidsuitgangspunten.
Deze uitgangspunten zijn ontleend aan het "Informatiebeveiligingsbeleid en -kader Nationale Politie". Voor de beleidsregels zijn ook de Baseline Informatiebeveiliging Overheid en het BIO Addendum voor de Politie gehanteerd.

3.6.1. Back-up gebruiksdoel en strategie

Back-up wordt gebruikt om de gevolgen van de uitval en/of het verlies van informatie (restore) dan wel om de gevolgen van uitval en/of verlies van IT-functionaliteit (recovery) te minimaliseren.

Voor back-up geldt een 3-2-1-1 strategie als uitgangspunt:

- Er zijn minimaal 3 kopieën van de gegevens, inclusief de gegevens van de productieomgeving;
- De gegevens zijn op tenminste 2 verschillende opslagmedia opgeslagen;
- Eén kopie daarvan is opgeslagen op een andere locatie (deze back-up is off-site)
- Eén kopie daarvan is geïsoleerd opgeslagen (deze backup is *off-line*)



Figuur 1 - 3-2-1-1 Strategie [5]

*In de literatuur die aandacht schenkt aan de bescherming tegen ransomware aanvallen wordt vaak de term **off-line** back-up gebruikt. Vaak wil men hiermee aangeven dat die back-ups zodanig worden opgeslagen en beschermd dat het onmogelijk is die back-ups te manipuleren.*
Het doel bij off-line is dus om die set zodanig te beveiligen dat alleen geautoriseerde bewerkingen de set kunnen versleutelen, muteren, manipuleren, veranderen, etc.

3.6.2. Inrichten en uitvoeren Back-up & Restore/Recovery

- Back-ups worden bewaard conform de afgesproken termijnen van de back-up dienstverlening.
- Back-ups vallen onder dezelfde wet- en regelgeving als de oorspronkelijke gegevens.
- Om de vertrouwelijkheid van back-ups te garanderen worden de Back-ups versleuteld
- De back-upcyclus van back-up wordt bepaald door de snelheid waarop de gegevens gewijzigd worden.
- De back-up cycli worden vooraf op basis van RPO en RTO bepaald.

[5] Deze illustratie is hier slechts opgenomen als voorbeeld van een 3-2-1-1 strategie. De aangegeven technieken kunnen/zullen in de praktijk mogelijk anderen zijn dan hier weergegeven

- De bewaartermijn van de reserve kopieën wordt bepaald door het kritieke karakter van de gegevens en wetgeving.
- De maximale bewaartermijn van de oorspronkelijke gegevens is eveneens van toepassing op de back-up gegevens.
- Bij ketensystemen wordt de data-integriteit van de informatie keten gewaarborgd door het back-up & restore/recovery mechanisme.
- Het maximale toegestane dataverlies (RPO) en de maximale hersteltijd (RTO) is, in geval van een incident, gekoppeld aan het toegekende dienstenniveau (serviceprofiel laag, midden en hoog). De RPO en RTO zijn bepaald op basis van een expliciete risicoafweging en/of BIA. De BIA en BCM stellen de eisen en randvoorwaarden aan Back-up & Restore/Recovery.
- De RPO en RTO eisen passen binnen de afspraken die gemaakt zijn in de ICT Dienstencatalogus (IDC)
- Als er geen RPO en RTO zijn vastgesteld dan gelden de termijnen zoals genoemd in de BIO (artikel 12.3.1.3)
- Een volledige overzicht van applicaties met hun bijbehorende RPO en RTO is beschikbaar en wordt beheerd.
- Elke nieuwe versie van dit overzicht wordt gerapporteerd aan de proces / data eigenaar en aan de tweede lijn (zie paragraaf 3.8).
- Back-up (cyclus), restore en recovery worden zodanig ingericht dat wordt voldaan aan de eisen voor RPO en RTO.
- Back-up documentatie omvat ook 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 restore of recovery proces moet procedures omvatten voor het herstel van systeem- of applicatiestoringen, en, indien van toepassing, ook voor een totale datacenter ramp scenario (in geval van uitwijk).
- Indien als gevolg van een calamiteit restore/recovery moet plaatsvinden voor meerdere systemen gebeurt dit in een vooraf met proces/data eigenaren overeengekomen en prioriteitsvolgorde.
- Deze prioriteitsvolgorde is vastgelegd in de Business Continuity Plannen
- De overeengekomen prioriteitsvolgorde wordt gerapporteerd aan de proces / data eigenaar en aan de tweede lijn (zie paragraaf 3.8).
- Procedures voor back-up en restore/recovery zijn formeel vastgesteld.
- Procedures voor back-up en restore/recovery worden bewaard op een locatie die bij calamiteiten beschikbaar is.
- Back-up en recovery procedures worden beschikbaar gesteld aan de medewerkers en beheerders betrokken bij de uitvoering hiervan en zijn tevens beschikbaar in geval van calamiteiten.
- Bedieningsprocedures monitoren de uitvoering van back-ups om eventuele fouten in geplande back-ups aan te pakken om de volledigheid van back-ups in overeenstemming met het back-upbeleid te waarborgen.
- Voor transport van back-up data wordt minimaal gebruik gemaakt van veilige protocollen (encryptie).
- 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-up (bijvoorbeeld een *fysieke off-line back-up* op een andere locatie).

3.6.3. Betrouwbaarheid

- De media waarop de back-ups worden vastgelegd is voorzien van een duidelijke, heldere, unieke en accurate identificatie.
- Verwijderbare media worden behandeld conform het beleid voor verwijderbare media en volgens de daarin aangegeven procedure(s).
- Back-up en restore / recovery faciliteiten worden deugdelijk onderhouden (zowel preventief, correctief als adaptief onderhoud) conform de specificaties van de fabrikant van de verschillende onderdelen van deze faciliteit.
- De media waarop de back-ups zijn vastgelegd worden conform de specificaties van de fabrikant van deze media opgeslagen.
- Het medium dat wordt ingezet voor back-up, wordt preventief vervangen na een bepaalde aantal keren of aantal uren te zijn gebruikt. Dit aantal keren gebruik of totaal aan uren inzet wordt bepaald op basis van de MTBF waarde voor het medium waarop de back-up is vastgelegd. De preventieve vervanging geschiedt op het moment van 95% van de aantallen of maximale gebruiksduur zoals door de fabrikant van het medium is aangegeven.
- Voor het waarborgen van de correcte en veilige bediening van back-up, restore en recovery faciliteiten en voorzieningen zijn bedieningsprocedures en systeemdocumentatie voorhanden.

- Beveiliging van de back-up- & restore/recovery-faciliteiten of voorzieningen voldoen aan de rubriceringseisen (Politie Intern, Politie Confidentieel, Politie Geheim) van de originele data.
- Beveiliging van de back-up, restore en recovery faciliteiten of voorzieningen voldoen aan de eisen die gesteld worden aan de bescherming van persoons- en politiegegevens van de originele data.
- Alle maatregelen (zoals noodstroom en koeling) ter bescherming van apparatuur zijn tevens van toepassing op apparatuur die gebruikt wordt voor de back-up en recovery procedures.
- Toegang tot de back-ups wordt beperkt tot de medewerkers die de back-up en recovery procedure mogen uitvoeren. Regelmatig wordt conform het geldende autorisatiebeleid of deze toegangsrechten nog valide zijn.

3.6.4. Weerbaarheid

- Alle systemen voor de back-up en recovery faciliteiten en -voorzieningen moeten zodanig ingesteld zijn dat compromitering wordt verlaagd. Daarom geldt voor deze systemen het hardening beleid.
- *Back-up en recovery faciliteiten en voorzieningen beschikken over functionaliteiten. of capaciteiten voor de preventie, detectie en correctie in geval van een malware aanval. Een malware aanval tijdens en na afronding van het back-up proces wordt gedetecteerd.*
- *Voorafgaand aan het maken van de back-up is (geautomatiseerd) gecontroleerd dat het systeem waarop de back-up wordt geplaatst niet met malware is geïnfecteerd.*
- *De benodigde middelen voor het uitvoeren van het recovery proces zijn niet afhankelijk van IT-systemen die geraakt of onbeschikbaar kunnen worden door malware.*
- *Ondersteunende systemen voor de toegang en toegankelijkheid tot de ruimte en kasten en conditionering van de ruimte waarin de back-up media worden bewaard, zijn gesegmenteerd ten opzichte van de systemen waarvan de gegevens worden geback-upt en zijn voorts niet afhankelijk van de beschikbaarheid en juiste werking van productieomgevingen*.
- *Toegang(srechten) tot back-up en recovery faciliteiten en voorzieningen is (zijn) niet afhankelijk van de productieomgeving.*
- Het fysieke transport van de back-up media wordt uitgevoerd door geautoriseerd personeel dat gebruik maakt van daarvoor geschikte middelen.
- Indien voor het transport van fysieke media zoals bijvoorbeeld data tapes een externe partij wordt ingezet, dan wordt met deze partij voorafgaand aan de uitvoering een overeenkomst afgesloten. Medewerkers van deze externe partij beschikken over de juiste en geldige screening en hebben een geheimhoudingsplicht.

3.6.5. Restore/Recovery

- Voor recovery is altijd toestemming nodig van de eigenaar van het systeem of de gegevens.
- Het restoren van bestanden die door een medewerker zijn gecreëerd wordt aan die medewerker een standaard restore proces aangeboden als onderdeel van de ICT dienstverlening.[6]
- *Bij grotere incidenten, bijvoorbeeld als een database corrupt is geraakt of bij een ransomware aanval, wordt altijd overlegd 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.
- Voor het recoveren van applicaties of (bedrijfskritische) systemen wordt een installatie of security baseline opgesteld waarin handleidingen en alle parameters die noodzakelijk zijn om een applicatie of systeem draaiende te krijgen (zoals licenties, serienummers, applicatieparameters en hardening settings), zijn opgenomen.
- *Voordat een back-up wordt gebruikt voor recovery, wordt vastgesteld welke versie (aan de hand van de datum) van de back-up niet met malware is geïnfecteerd.*

3.6.6. Registratie & verificatie

- Alle back-up activiteiten worden gelogd.
- Alle restore/recovery activiteiten worden gelogd.
- De verblijfplaats van de media wordt in een logboek bijgehouden.
- Transport van media naar een off-site locatie wordt in een logboek vastgelegd.
- Bij transport van media van een site naar een andere locatie wordt bij ontvangst op de andere locatie getoetst of het ontvangen medium het van de initiële site verzonden medium is.
- Van logboeken worden back-ups gemaakt.
- De back-ups van logboeken worden op wordt op een andere dan de oorspronkelijke locatie opgeslagen.

[6] Dit standaard proces stelt de gebruiker in staat om zelfstandig een bestand te restoren.

- De logboeken worden regelmatig, bij voorkeur conform de back-up cyclus, gecontroleerd.
- De logging kan gebruikt worden binnen andere beheerprocessen.
- Er wordt gecontroleerd of de back-up activiteit succesvol is afgerond.
- Er wordt gecontroleerd of de gemaakte back-up leesbaar is en volledig is.
- Na een restore/recovery wordt gecontroleerd of die activiteit succesvol is afgerond.
- Na een restore/recovery van een of meerdere systemen die in een keten moeten samenwerken wordt gecontroleerd of de data integriteit over de gehele keten correct is gerestored/recoverd. Deze controle moet ook bij restoretest worden uitgevoerd.

3.6.7. Toetsen, testen, actualiseren en aanpassen

- De back-up, restore en recovery documentatie worden minimaal jaarlijks getoetst en eventueel aangepast (PDCA cyclus) om er voor te zorgen dat andere nieuwe technologieën of veranderingen in de organisatie in de documentatie worden geactualiseerd. De documentatie die specifiek betrekking heeft op malware aanvallen, wordt per kwartaal geactualiseerd zodat deze rekening houden met nieuwe malware dreigingen.
- De back-up, restore en recovery procedures worden minimaal jaarlijks of na een grote wijziging getest conform de afspraak met de eigenaar van de betreffende data. Dit om te waarborgen dat ze voldoen aan de eisen van de bedrijfscontinuïteitsplannen voor het tijdige herstel van de dienstverlening.
- Restore/Recovery testen vinden plaats in een omgeving die afgeschermd is van de oorspronkelijke omgeving. Dit om te voorkomen dat de originele media overschreven wordt.
- Back-up, restoren en recovery worden periodiek getest conform de onderstaande tabel afgestemd op het dienstenniveau:

	Serviceprofiel Laag	Serviceprofiel Midden	Serviceprofiel Hoog
Frequentie voor periodiek uitvoeren testen (oefenen) van back-up, restore en recovery	Minimaal eenmaal per jaar	Minimaal eenmaal per 9 maanden	Minimaal eenmaal per 6 maanden, bij voorkeur per kwartaal

Tabel 4 – Serviceprofielen

- De resultaten van de tests en evaluaties van de procedures worden vastgelegd en beoordeeld. Aan de hand van deze beoordelingen worden de procedures zo nodig geactualiseerd. De wijzigingen worden gecommuniceerd naar de betrokken medewerkers

3.6.8. Clouddiensten en back-up

- Voor Clouddiensten gelden dezelfde doelstellingen voor back-up & restore/recovery als voor de interne dienstverlening
- Bij het afsluiten van contracten met Cloudleveranciers is er specifieke aandacht voor Back-up & Restore/Recovery.
- *De clouddienst is weerbaar tegen malware in het bijzonder ransomware, en voldoet ook in geval van dergelijke aanvallen aan de eis van het minimaliseren van verlies van gegevens en metagegevens.*
- De Cloud leverancier toont aan dat hij in opzet en bestaan kan voldoen aan bovenstaande eisen. De vereiste bewijskracht en omvang van de bewijsstukken is afhankelijk van de omvang, complexiteit, afhankelijkheid (van de clouddienst), soort clouddienst en de te verwerken gegevens.

3.7. Afwijkingen

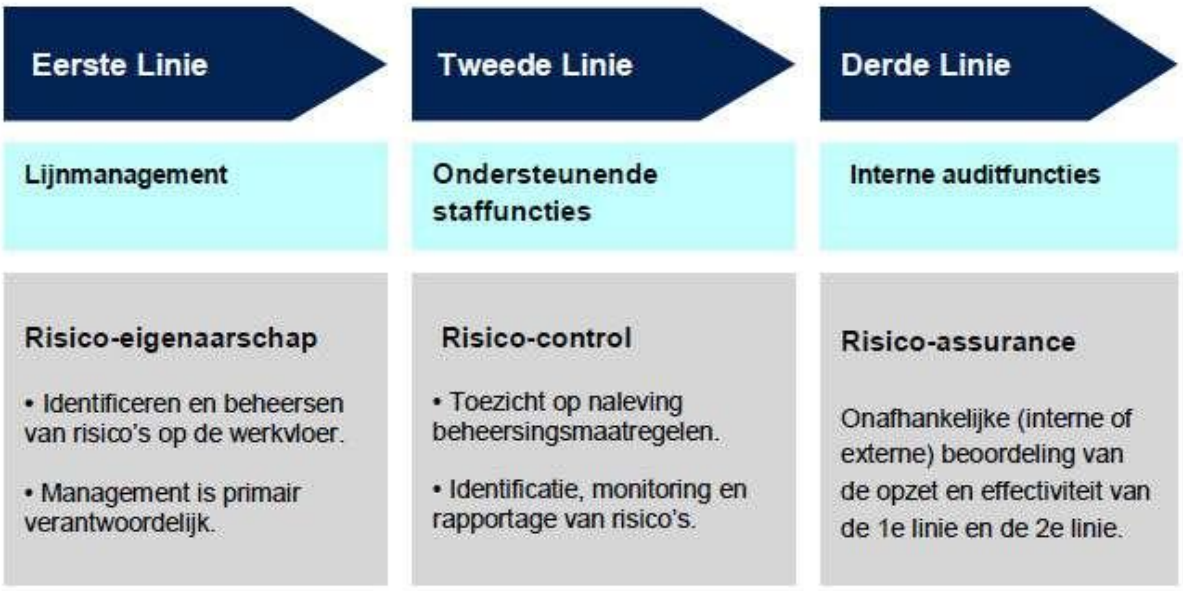
Als het niet mogelijk is om de beleidsregels voor back-up & restore/recovery toe te passen dan geldt:

- Afwijkingen op de beleidsregels voor back-up en restore/recovery worden gedocumenteerd en zijn altijd gebaseerd op een risicoafweging en een risico acceptatie.
- Afwijkingen op de beleidsregels voor back-up en restore/recovery worden gerapporteerd aan de proces / data eigenaar en aan de tweede lijn (zie paragraaf 3.8).

3.8. Toezicht en Rapportage

Voor toezicht en rapportage werkt de IV organisatie volgens het 'Three Lines of Defence' model. De volgende paragrafen gaan hier nader op in.

3.8.1. Toezicht en controle op naleving



- De eerste lijn, het lijnmanagement, is op de diverse organisatieniveaus verantwoordelijk op de goede sturing en beheersing van de organisatie, op het managen van de risico's die met de bedrijfsvoering samenhangen en op de volledigheid en betrouwbaarheid van de verantwoordingsinformatie.

- De tweede lijn is verantwoordelijk voor het ontwikkelen van voorschriften over de toe te passen wet- en regelgeving. De tweede lijn ondersteunt het verantwoordelijke management bij het identificeren en bewaken van risico's. De tweede lijn ontwikkelt systemen voor procesbeheersing, planning & control, informatieverwerking, communicatie en rapportage. Dit ter ondersteuning van de lijnmanager bij het bijsturen van de procesvoering, het uitvoeren van evaluaties en het afleggen van verantwoording. Het Kwartier IB monitort de werking van de processen en het voldoen aan wet- en regelgeving. Bij afwijking van de compliance zal zij dit rapporteren.

- De derde lijn is de interne auditor en voorziet de leiding van aanvullende zekerheid over de kwaliteit van sturing en beheersing. De interne auditor geeft een onafhankelijk oordeel over het geheel van beheersingsmaatregelen die de organisatie heeft genomen ten aanzien van de naleving van beleid en wet- en regelgeving. Doorgaans vervult Korpsaudit deze functie.

3.8.2. Rapportage

- Binnen de 1e lijn zijn rapportages beschikbaar die inzicht geven in de effectiviteit en efficiëntie van Back-up & Restore/Recovery
- Er zijn KPI's vastgesteld die de werking van het Back-up & Restore/Recovery proces inzichtelijk maken.
- Minimaal jaarlijks wordt het Back-up & Restore/Recovery proces en de bijbehorende documentatie gereviewed om te zien of ze voldoen aan de beleidsregels. Dit wordt aan de 2e lijn gerapporteerd.
- De 1e lijn rapporteert elke versie van het applicatieoverzicht met de met data/proces eigenaren overeengekomen RTO en RPO aan de 2e lijn.
- De 1e lijn rapporteert elke versie van het overzicht van de met data/proceseigenaren overeengekomen prioriteitsvolgorde voor restore/recovery aan de 2e lijn.
- De 1e lijn rapporteert afwijkingen op de beleidsregels voor back-up en restore/recovery aan de 2e lijn.
- Aan de 3e lijn worden op verzoek van de intern auditor rapportages verstrekt.