Richtlijn back-up en herstel

Vastgesteld op:	12-3-2024
Beleidskader:	Beleidskader informatiebeheer H.7 Informatiebeveiligingsbeleid Privacy beleid

Inleiding

Door middel van back-ups wil de provincie Noord-Holland ervoor zorgen dat haar informatie: *PNHinformatie*[1], en de systemen waarin deze informatie staat opgeslagen bij een calamiteit weer te herstellen zijn. Back-up en herstel moeten daarom voor alle *informatiesystemen*[2] goed geregeld zijn. In deze richtlijn staan de minimale eisen. Deze richtlijn gaat niet over systemen waar geen informatie of data van de PNH in staat opgeslagen.

Scope

In deze richtlijn vind je de eisen aan back-up en herstel die voortvloeien uit het beleidskader informatiebeheer, het informatiebeveiligingsbeleid en het privacy beleid. Het zijn de minimale eisen, nodig om te voldoen aan dit interne beleid en dus aan de Archiefwet, Algemene Verordening Gegevensbescheiden (AVG) en de Baseline Informatiebeveiliging Overheid (BIO). Mogelijke eisen en wensen vanuit het perspectief van bedrijfsvoering zijn in deze richtlijn niet meegenomen. Deze kunnen in een later stadium wel worden toegevoegd, of als extra eisen- en wensenpakket worden meegegeven aan een dienstverlener. Nieuwe versies van deze richtlijn moeten worden goedgekeurd door de Chief Information Officer (CISO) en de Functionaris Gegevensbescherming (FG).

Doel(groep)

Het doel van deze richtlijn is duidelijkheid scheppen over de minimale eisen die de provincie stelt aan backup en herstel. De richtlijn is dan ook geschreven voor projectleiders, initiatiefnemers, service level managers, informatiemanagers en andere informatieprofessionals die hierover afspraken maken met dienstverleners of monitoren op de naleving.

Uitgangspunten

De eisen in deze richtlijn gelden voor informatiesystemen met de kwalificatie basis beveiligingsniveau (BBN) 1 en BBN 2. De Provincie Noord-Holland heeft geen informatiesystemen met BBN3 classificatie. Het basis beveiligingsniveau wordt voor ieder informatiesysteem bepaald bij de uitvoering van de Business Impact Analyse (BIA). Voor meer informatie zie de intranetpagina informatiebeveiliging & privacy.

[1] Vastgelegde (sets van) gegevens en informatie ongeacht vorm en drager die de PNH opmaakt of ontvangt bij de uitvoering van haar taken en bedrijfsprocessen.

[2] Applicaties waarin PNH-informatie wordt opgeslagen.

Afspraken met dienstverleners

Bij het aangaan, verlengen of herzien van een overeenkomst met een dienstverlener maakt de initiatiefnemer van de Provincie Noord-Holland afspraken over back-up en herstel van het informatiesysteem en de informatie die daarin is opgeslagen. Met deze afspraken moet tenminste kunnen worden voldaan aan de minimale eisen uit deze richtlijn. De initiatiefnemer legt de gemaakte afspraken vast in de overeenkomst en zorgt ervoor dat deze worden opgenomen in een registratie, die wordt beheerd door de unit Regie, Service & Beheer van de sector Concern Informatievoorziening en Datatechnologie (CID).

Beschikbaarheid

- Maximale uitvalsduur (MUD/RTO):
    - BBN1: maximaal vijf werkdagen ○ BBN2: maximaal twee werkdagen
- Maximaal gegevensverlies (MGV/RPO):
    - BBN1&2: maximaal 28 uur[3]

3-2-1 regel

Om aan bovenstaande eisen te kunnen voldoen moeten back-ups worden gemaakt. De provincie Noord-Holland houdt hierbij, voor IAAS en On Premise, vast aan de 3-2-1 regel. Dit houdt in dat er naast de originele data twee kopieën (back-ups) zijn, waarvan er minimaal één fysiek op een andere locatie staat. Er zit minimaal 10 km hemelsbreed tussen beide locaties. Voor SAAS en PAAS diensten geldt deze eis niet.

Indien een back-up op een locatie buiten de Europese Economische Ruimte (EER) wordt opgeslagen is de kans groot dat er aanvullende afspraken moeten worden gemaakt om te voldoen aan de AVG. Welke afspraken nodig zijn is afhankelijk van de situatie. De initiatiefnemer van de provincie NoordHolland zorgt ervoor dat de Functionaris Gegevensbescherming (FG) tijdig wordt betrokken.

Bewaartermijnen

Ongewild verlies van data wordt niet altijd meteen opgemerkt. De provincie Noord-Holland wil data gedurende minimaal één maand met een maximaal gegevensverlies van 28 uur kunnen herstellen. Daartoe moeten dagelijkse[4] back-ups worden gemaakt, die één maand worden bewaard.[5]

Om ook ná een maand nog data te kunnen herstellen zijn naast de dagelijkse en wekelijkse back-ups ook maandelijkse back-ups nodig die minimaal zeven maanden[6] worden bewaard. Dataherstel uit een maandelijkse back-up kan meer gegevensverlies met zich meebrengen: maximaal één maand.

[3] Eén etmaal + 4 uur.

[4] Om precies te zijn iedere 28 uur minus de tijd die het kost om de back-up te maken.

[5] In het geval BBN3 is vastgesteld moeten er zelfs 5 back-ups per dag worden gemaakt, ook ieder met een bewaartermijn van één maand, om het maximaal gegevensverlies de eerste maand tot 4 uur te beperken. [6] Back-ups mogen nooit langer dan een jaar bewaard worden, omdat anders niet wordt voldaan aan de plicht vanuit de Archiefwet en de AVG om informatie te vernietigen na verloop van de wettelijke bewaartermijn.

Back-up strategie

Bovenstaande eisen aan beschikbaarheid en bewaartermijnen resulteren in het volgende globale back-up schema:

Back-up	**Bewaartermijn**
Dagelijks	1 maand
Wekelijks	1 maand
Maandelijks	7 maanden

Dienstverleners kunnen zelf kiezen voor een combinatie van verschillende back-up methodes zoals volledig, incrementeel en differentieel; zolang aan de eisen uit deze richtlijn wordt voldaan. De 3-2-1 regel geldt per cyclus: de dagelijkse back-up, wekelijkse en maandelijkse moeten hier ieder afzonderlijk aan voldoen.

Consistentie

Een back-up van statische data, zoals een fileshare, mag een momentopname (snapshot) zijn (inconsistent). Bij een back-up van dynamische data, zoals een database, mogen geen lopende transacties[6] worden onderbroken. De dynamische data moet dus eerst in een statische toestand worden gebracht (consistent).

Goedkeuring

De back-up strategie van een dienstverlener, incl. toelichting op methodes en consistentie, wordt goedgekeurd door de sectormanager CID. Hij toetst of het schema voldoet aan de eisen in deze richtlijn.

Vernietigen

Back-ups worden na afloop van hun bewaartermijn op dusdanige wijze vernietigd, dat de informatie niet meer te reproduceren is vanuit de hard- en/of software waar het in opgeslagen stond.

Beveiliging

- Back-ups zijn duurzaam opgeslagen, dat wil zeggen: op een veilige plek, beschermd tegen invloeden van buitenaf.
- Back-ups staan fysiek op minimaal 10 kilometer afstand van elkaar om een fysieke calamiteit op één locatie te kunnen doorstaan.
- Back-ups zijn beschermd tegen onbevoegde toegang d.m.v. versleuteling.
- Alleen de noodzakelijke beheerders kunnen via een speciaal back-up account[7] toegang krijgen tot back-ups. Indien zij toegang hebben tot de informatie op de back-ups zijn zij aan geheimhouding gebonden.
- Het beveiligingsniveau van de back-up dient minimaal gelijk te zijn aan dat van het informatiesysteem (BBN 1 of 2).

[6] Schrijfacties tussen werkgeheugen en opslagruimte.

[7] Dus niet via hun eigen ‘persoonlijk’ account.

- Alle back-up- en herstelactiviteiten vinden enkel na akkoord van de eigenaar van een informatiesysteem plaats en worden vastgelegd in een voor de unit Regie, Service & Beheer toegankelijk logboek.

Herstel

- De dienstverlener hanteert een herstelprocedure die is goedgekeurd door de sectormanager CID, na overleg met de FG en de beleidsadviseur informatiebeheer.
- Bij het terugzetten van een back-up wordt voorkomen dat ook data die in de tussentijd conform de Archiefwet uit een informatiesysteem is vernietigd wordt teruggezet.[8] Lukt dit niet, dan moet die data direct na het terugzetten opnieuw onherstelbaar worden vernietigd. In de herstelprocedure dient te zijn aangegeven hoe aan dit punt invulling wordt gegeven.

- Data moet uiterlijk binnen twee werkdagen na akkoord van de eigenaar op de herstelactie zijn hersteld.

Kwaliteitszorg

Herstel

- De dienstverlener plant tenminste jaarlijks[9] een hersteltest[10], voert deze uit en stuurt het verslag naar de sectormanager CID, die de testresultaten voor alle informatiesystemen bijhoudt in een registratie. De scope van de hersteltest bepaalt de leverancier voorafgaand aan de test samen met de sector CID. De sector CID legt de afspraken vast.
- Voorafgaand aan iedere grote wijziging in systeem en/of proces zorgt de dienstverlener voor een volledige back-up ten behoeve van een roll-back scenario. Nadat de wijziging in productie is gebracht voert de dienstverlener een hersteltest uit. Ook hiervan gaat het verslag naar de sectormanager CID, die de testresultaten bijhoudt in de bij het voorgaande punt genoemde registratie.
- Procedures (kwaliteitscontrole en herstel) worden naar aanleiding van uitgevoerde hersteltests door de dienstverlener herijkt, waarna ze opnieuw worden goedgekeurd door de sectormanager CID, na overleg met de FG en de beleidsadviseur informatiebeheer.

Back-up

- De kwaliteit van de back-ups wordt dagelijks gecontroleerd door de dienstverlener op basis van een eigen procedure die is goedgekeurd door de sectormanager CID, na overleg met de FG en beleidsadviseur informatiebeheer. De procedure bevat minimaal een controle van de logging op niet-geslaagde back-ups.

---

[8] Hiervoor kunnen de verklaring van vernietiging en vernietigingslijst van de betreffende vernietigingsronde gebruikt worden, deze zijn beschikbaar bij de unit DIV.

[9] Indien een dienstverlener meer dan drie informatiesystemen levert kan volstaan worden met een jaarlijkse steekproef.

[10] Op dit moment zijn er geen nadere kwaliteitseisen aan hersteltests. Het verdient de aanbeveling deze wel op te stellen.

- Indien de dienstverlener bij de dagelijkse kwaliteitscontrole onregelmatigheden constateert rapporteert deze hierover nog dezelfde dag aan de unitmanager Regie, Service & Beheer.

Contractmanagement

- De unit Regie, Service & Beheer controleert tenminste jaarlijks of gemaakte afspraken met een dienstverlener worden nagekomen, acteert op de uitkomsten ervan en houdt een registratie[11] bij van de afspraken en de controle.

[11] Bijvoorbeeld in een contractmanagementtool of in een CMDB.