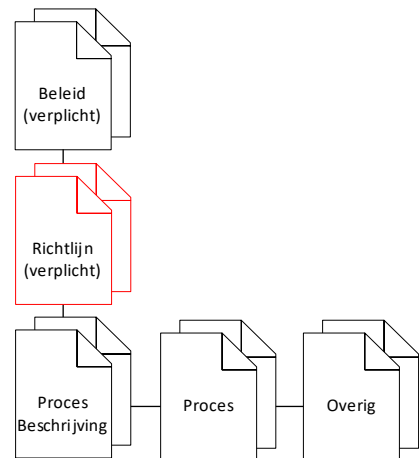


Informatiebeveiliging

DOC-BB-01J Richtlijn Back-Up en Recovery

Datum: 12-01-2022
Versie: 1.5
Auteur: P.H.W. van den Boogaard
Eigenaar: Directie
Status: Vastgesteld
Type: Richtlijn



LICENTIEBEHEER

Dit werk is verstrekt onder een Creative Commons-Licentie: Naamsvermelding-Niet Commercieel-Gelijk Delen 4.0 Internationaal.



Provincie Noord-Brabant 2021

De betreffende licentie houdt in dat het betreffende materiaal gebruikt en gedeeld mag worden onder de volgende voorwaarden:

- De Provincie Noord-Brabant wordt als bron vermeld zoals opgenomen in de naamsvermelding;
- Het betreffende document en de bijbehorende inhoud mogen niet commercieel geëxploiteerd worden;
- Iedere kopie van dit document, of een gedeelte daarvan, dient te zijn voorzien van de in deze paragraaf vermelde mededeling.

Wanneer dit werk wordt gebruikt, hanteer dan de volgende methode van naamsvermelding:

“Provincie Noord-Brabant / P.H.W. van den Boogaard”, licentie onder: [CC BY-NC-SA 4.0](#).

Voor vragen of meer informatie kunt u contact opnemen met:

[P.H.W. van den Boogaard](#)

Chief Information Security Officer
Provincie Noord-Brabant
Brabantlaan 1
5216 TV 's-Hertogenbosch

VERSIEBEHEER

Versie	Datum	Omschrijving reden nieuwe versie
0.2	08-05-2019	Verwerken opmerkingen en tekstuele opmerkingen
1.0	11-05-2019	Finale Controle
1.1	13-05-2019	Definitieve versie
1.2	27-01-2020	Toevoegen Creative Commons-Licentie
1.3	23-06-2020	Wijzigen BIO versie naar 1.04
1.4	15-03-2021	Tekstuele wijzigingen
1.5	12-01-2022	Tekstuele wijzigingen

VERSPREIDING

Versie	Datum	Verspreiding
0.2	08-05-2019	Strict, DigiTrust, Provincie Noord-Brabant
1.0	11-05-2019	Strict, DigiTrust, Provincie Noord-Brabant
1.1	13-05-2019	Strict, DigiTrust, Provincie Noord-Brabant
1.2	27-01-2020	Provincie Noord-Brabant, Relevante externe partijen
1.3	23-06-2020	Provincie Noord-Brabant, Relevante externe partijen
1.4	15-03-2021	Provincie Noord-Brabant, Relevante externe partijen
1.5	12-01-2022	Provincie Noord-Brabant, Relevante externe partijen

DOCUMENTGEGEVENS

Onderwerp	Omschrijving
Documentnaam:	DOC-BB-01J Richtlijn Back-up en recovery.docx
Aantal pagina's:	7
Opsteller:	P.H.W. van den Boogaard
Status:	Vastgesteld
Classificatie:	Bedrijfsvertrouwelijk

VERWIJZINGEN

Verwijzing	Titel	Versie/Datum
NEN-ISO 27001	NEN-EN-ISO_IEC 27001_2017+A11:2020 (NL)	Februari 2020
NEN-ISO 27002	NEN-EN-ISO_IEC 27002_2017 (NL)	Maart 2017
NEN-ISO 31000	Risicomanagement - Principes en richtlijnen	Oktober 2019
BIO 1.04	Baseline Informatiebeveiliging Overheid	November 2019

ACCEPTATIE

Acceptatie en goedkeuring	Datum	Corsa verwijzing
M.J.A van Bijnen	12-01-2022	C2293275

INHOUDSOPGAVE

- 1. Inleiding5**
 - 1.1. Doelstelling 5
 - 1.2. Reikwijdte 5
- 2. Termen, definities en afkortingen5**
 - 2.1. Termen en definities 5
 - 2.2. Gebruikte afkortingen 5
- 3. Maatregelen6**
 - 3.1. Back-up..... 6
 - 3.2. Recovery 6
 - 3.3. Opslag back-ups 6
 - 3.4. Vernietiging van back-up..... 6
 - 3.5. Bewaartermijn 6
 - 3.6. Documentatie en procedures 6
- 4. Relatie van de richtlijn met andere documenten7**
- 5. Relatie van de richtlijn met verschillende wet en regelgeving7**
- 6. Verantwoordelijkheden.....7**

1. INLEIDING

Door een technische storing, (on)opzettelijke verwijdering of manipulatie kan opgeslagen bedrijfsinformatie onbruikbaar worden of zelfs verloren raken. Door middel van back-ups wordt gewaarborgd dat via een redundante informatieopslag de bedrijfsinformatie hersteld kan worden, als er delen van de productiegegevens verloren raken. Het risico van verlies van productiegegevens en de reproductie van de beschadigde of verloren informatie, die nodig zijn voor het herstel van de bedrijfsvoering, wordt door het gebruik van back-ups gereduceerd. Deze richtlijn beschrijft de maatregelen die de Provincie Noord-Brabant hanteert in het kader van back-up en herstel.

1.1. Doelstelling

Het maken van back-ups waarborgt dat na verlies of beschadiging van data uit informatiesystemen door een gebeurtenis of een incident, de informatiesystemen of informatie hersteld kan worden. Informatieverlies wordt hierdoor zoveel mogelijk voorkomen, de integriteit en beschikbaarheid van informatie voor bedrijfsprocessen wordt hierdoor gewaarborgd.

1.2. Reikwijdte

Deze richtlijn is van toepassing op de gehele informatievoorziening waar de Provincie Noord-Brabant verantwoordelijk voor is en/of gebruik van maakt.

2. TERMEN, DEFINITIES EN AFKORTINGEN

In de onderstaande paragrafen worden de voor het document relevante termen, definities en afkortingen opgesomd.

2.1. Termen en definities

Informatievoorziening

De informatievoorziening van de Provincie Noord-Brabant, is het geheel van mensen, middelen en maatregelen die noodzakelijk zijn voor het invullen van de informatiebehoefte van de medewerkers van de provinciale organisatie. Bij informatievoorziening staat de mens centraal. Informatie begint immers bij de menselijke behoefte om iets te willen weten.

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.

2.2. Gebruikte afkortingen

Afkorting	Beschrijving
IB	Informatiebeveiliging
NEN-ISO 27001	Internationale standaard voor informatiebeveiliging
BIO	Baseline Informatiebeveiliging Overheid

3. MAATREGELEN

Back-up is noodzakelijk om gegevens en applicaties te kunnen herstellen in verband met verlies, vernietiging, beschadiging en manipulatie van gegevens of software. Onderstaande maatregelen dienen te worden gerespecteerd met betrekking tot back-ups:

3.1. Back-up

- De Provincie gebruikt back-up en recovery om de gevolgen van de uitval, beschadiging en/of het verlies van informatie te minimaliseren;
- Dataverlies wordt beperkt tot maximaal 24 uur;
- De back-ups van alle provinciale informatie, software en besturingssystemen (en instellingen) moeten worden bewaard, zodat de 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;
- Alle provinciale informatie welke staat op werkstations, laptops of andere draagbare apparaten moeten worden opgeslagen op een netwerk file server om back-up mogelijk te maken;
- Back-ups kunnen vertrouwelijke informatie bevatten. Deze back-ups dienen dan minimaal als "vertrouwelijk" te worden geclassificeerd (zie de classificatie richtlijn). Dit betekent dat eisen worden gesteld aan de opslag en toegankelijkheid van back-ups (zie de logische toegang richtlijn en de fysieke toegang richtlijn). Ook de cryptografie richtlijn kan van toepassing zijn.

3.2. Recovery

- De hersteltijd in geval van incidenten bedraagt maximaal 16 werkuren in 85% van de gevallen;
- Recovery procedures moeten minimaal per kwartaal worden getest.

3.3. Opslag back-ups

- Minstens drie versies van een back-up moeten worden bewaard, op tenminste twee verschillende opslagmedium, waarvan er 1 op een andere fysieke plek bewaard moet worden;
- Er dient minimaal één volledige back-up te worden opgeslagen in een veilige, off-site locatie.

3.4. Vernietiging van back-up

- De back-up tapes worden vernietigd in overeenstemming met het beleid omtrent behandeling van digitale media van de Provincie Noord-Brabant.

3.5. Bewaartermijn

- De bewaartermijnen dienen te voldoen aan wet- en regelgeving;
- Daar waar wet- en/of regelgeving geen (eenduidige) aanwijzingen geven over bewaartermijnen geldt dat back-ups maximaal 1 jaar worden bewaard;
- Het wissen van back-ups na het verlopen van de bewaartermijn gebeurt zo veel mogelijk automatisch;
- Het tijdig wissen van back-ups moet aantoonbaar zijn.

3.6. Documentatie en procedures

- 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 recoveryproces 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 procedures 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;
- Van back-up en recovery activiteiten en de verblijfplaats van de bijbehorende media wordt een logboek bijgehouden.

4. RELATIE VAN DE RICHTLIJN MET ANDERE DOCUMENTEN

Document	Relatie
NEN-ISO 27001	Kader stellend
NEN-ISO 27002	Kader stellend
BIO versie 1.04	Kader stellend
DOC-B-01 Beleid Informatiebeveiliging	Kader stellend

5. RELATIE VAN DE RICHTLIJN MET VERSCHILLENDE WET EN REGELGEVING

Wet & Regelgeving	Verwijzing
NEN-ISO 27001	Hoofdstuk A.12.3
NEN-ISO 27002	Hoofdstuk 12.3
BIO versie 1.04	Hoofdstuk 12.3
Forum Standaardisatie	Register verplichte standaarden

6. VERANTWOORDELIJKHEDEN

Rol	Verantwoordelijkheid
Directie Provincie Noord-Brabant	- Eigenaar van dit document.
Chief Information Security Officer (CISO)	- Opstellen en onderhouden van deze richtlijn. - Laat op regelmatige basis IB maatregelen controleren dat de regelgeving correct wordt toegepast. - Inrichten, advisering en toezien op de naleving van de technische en organisatorische beveiligingsregels met betrekking tot back-up en herstel van de bedrijfsinformatie.
Information Security Officer (CISO)	- Ondersteuning bij de implementatie van deze richtlijn.
Team leveranciersmanagement	- Opstellen contract, SLA, DAP en Verwerkersovereenkomst met cloud leverancier, indien van toepassing.
Programma Manager Dienstverlening ICT	- Zorgdragen voor de implementatie van deze regels opgesteld in deze richtlijn. - Het regelmatig controleren dat de vereisten voor back-up voldoen aan de maatregelen. - Het beoordelen of het back-up plan is afgestemd op de klassen van informatie. - Het ontwerpen van een architectuur voor back-up. - De elementen binnen deze architectuur afstemmen op het herstelplan. - De vereisten voor back-up en herstel laten opnemen in het lastenboek of contract met een leverancier.