



Back-up beleid gemeente Hoorn

Maart 2022

Versie 1.0

Zaaknummer: 1942892

Inhoudsopgave

Inhoud

1	Inleiding	3
1.1	Doel.....	3
1.2	Evaluatie	3
1.3	Afbakening	3
1.4	Kaders.....	3
1.5	Definities	3
2	Algemeen beleid	5
2.1	Uitgangspunten.....	5
2.1.1	Back-up en Restore	5
2.1.2	SAAS.....	6
2.1.3	Cloud	6
2.1.4	Content.....	6
2.1.5	Bewaartermijnen	6
3.	Organisatie, taken en verantwoordelijkheden	7
3.1	Teammanager GMB	7
3.2	Teammanager I&A.....	7
3.3	Coördinator informatiebeveiliging	7
3.4	Functionaris informatiebeveiliging	7
3.5	Leveranciers	7
3.6	Data- of applicatie eigenaar	7
3.7	Gebruikers	7

1 Inleiding

Back-up en recovery is een belangrijke beschikbaarheidsmaatregel die ervoor zorgt dat gecorrumpeerde, verloren of vernietigde bedrijfsinformatie hersteld kan worden. Niet alleen bedrijfsinformatie wordt meegenomen in een back-up, maar ook de system-states. Dit zijn machine instellingen en bijvoorbeeld de Active Directory (AD).

1.1 Doel

Het kunnen herstellen van gegevens en/of programmatuur bij verlies of beschadiging door bijvoorbeeld:

- Fouten in software
- Menselijke fouten, zoals bedienfouten
- Beschadiging van data of programmatuur
- Herstellen van dienst in geval van een incident of calamiteit

Het is nadrukkelijk niet de bedoeling dat bewust vernietigde informatie uit een back-up kan worden hersteld. Denk hierbij aan archiefvernietiging.

1.2 Evaluatie

Dit beleid wordt jaarlijks geëvalueerd en als dit nodig is geactualiseerd.

1.3 Afbakening

Dit beleid is van toepassing op alle informatiesystemen waar we bij de gemeente Hoorn direct en indirect gebruik van maken. Het geldt ook wanneer informatiesystemen technisch niet binnen de gemeente Hoorn draaien, bijvoorbeeld bij SaaS-applicaties. Dit beleid geldt voor iedereen die gebruik maakt van de informatiesystemen van de organisatie.

1.4 Kaders

Voor de gehele overheid is een normenkader voor informatiebeveiliging afgesproken waar elke organisatie aan moet voldoen. Dit is de Baseline

Informatiebeveiliging Overheid (BIO). Er is een Informatiebeveiligingsbeleid van de organisatie waarin de rollen, verantwoordelijkheden en maatregelen zijn opgenomen om gegevens te beschermen.

1.5 Definities

Recovery Point Objective (RPO)

Is de maximale termijn van gegevensregistratie die de organisatie bereid is kwijt te zijn naar aanleiding van een calamiteit of incident. Bij een RPO van vier uur betekent dit dat in het ergste geval alleen de data van de laatste vier uur verloren gaat.

Recovery Time Objective (RTO)

Is de maximale duur van de onderbreking van het computersysteem die de organisatie bereid is te accepteren in het geval van een calamiteit of incident. Bij een RTO van twee uur, is de applicatie in het ergste geval twee uur niet beschikbaar.

Recovery Granularity Objective (RGO)

Beschrijft het detailniveau waarop gegevens moeten kunnen worden hersteld. Als voorbeeld voor de mail omgeving, is dat per individuele mailbox of per mail.

CISO

De CISO (Chief Information Security Officer) is de functionaris informatiebeveiliging bij de gemeente Hoorn

Private Cloud

Een private Cloud of privé Cloud is een infrastructuur die een Clouddaanbieder levert aan één specifieke organisatie. Men beschikt hierbij over de middelen die horen bij Cloud computing, maar er wordt geen hard- of software met andere organisaties gedeeld.

Publieke Cloud

De publieke Cloud – of openbare Cloud - is een cloudoplossing waarbij men gebruik maakt van een gedeelde, online infrastructuur. De gemeentelijke applicaties en data bevinden zich in deze infrastructuur, die op een locatie van de Cloudaanbieder staat. Alle gerelateerde hardware, software en ondersteunende infrastructuur zijn eigendom van deze leverancier. De gemeentelijke data is alleen inzichtelijk voor medewerkers met een account van de gemeente Hoorn. Andere organisaties maken ook gebruik van de infrastructuur, zoals applicaties en servers.

Content

Content is de informatie-inhoud binnen een applicatie, database, website etc. Het is digitale informatie die bijvoorbeeld uit tekst, video of audio kan bestaan.

Bewaarperiode

Geeft aan hoe lang een back-up van de gegevens bewaard moet blijven.

2 Algemeen beleid

2.1 Uitgangspunten

De volgende beleidsuitgangspunten worden gehanteerd. Deze zijn ontleend aan de BIO, Archiefwet en aanvullend op het algemene beveiligingsbeleid van de gemeente. Het gaat hierbij om de back-up en herstelprocessen, nadrukkelijk niet over archivering.

2.1.1 Back-up en Restore

1. De back-up en recovery wordt gebruikt om de gevolgen van de uitval en/of het verlies van informatie te minimaliseren.
2. Het team Informatiemanagement en Automatisering (I&A) is belast met het uitvoeren van dit beleid. Zij kunnen dit uitbesteden aan een onderaannemer.
3. Het beleid wordt door de CISO getoetst.
4. De back-ups van alle gemeentelijke informatie, software, besturingssystemen en instellingen moeten worden bewaard op een wijze zodat 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.
5. Dataverlies wordt beperkt tot maximaal 28 uur (BIO 12.3.1.3)
Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident. (BIO 12.3.1.2)
6. De hersteltijd in geval van incidenten bedraagt:
 - o maximaal 2 uren voor bedrijf kritische applicaties (RTO)
 - o voor alle overige applicaties geldt 8 uur
 - o voor testsystemen is dit 24 uur.
 - o hersteltijd in geval van Incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen (BIO12.3.1.3)
7. De frequentie van back-ups wordt bepaald door de volatiliteit (beweeglijkheid, mate van verandering) van de gegevens.
8. De bewaartermijn voor reservekopieën wordt bepaald door de termijn waarbinnen de informatie hersteld moet kunnen worden.
9. De bewaartermijn kan worden beperkt door de toegestane bewaartermijn vanuit de archiefwet.
10. Minstens drie versies (3-2-1 methode) van een back-up moeten worden bewaard, op tenminste twee verschillende opslagmedia, waarvan er 1 op een andere fysieke (air-gap) plek bewaard moet worden.
11. Het back-up proces voorziet in opslag van de back-up op een door de CISO goedgekeurde locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere. (BIO12.3.1.4)
12. Alle gemeentelijke informatie welke staat op werkstations, laptops of andere draagbare apparaten moeten worden opgeslagen op een netwerk file server of Cloud opslag locatie (Office 365) om back-up mogelijk te maken.
13. Lokaal opgeslagen informatie wordt niet meegenomen in de back-up. Een uitzondering hierop is het bureaublad die met OneDrive wordt gesynchroniseerd.
14. Back-up documentatie omvat de identificatie van alle belangrijke gegevens, programma's, documentatie en support items die nodig zijn om het maken van back-ups goed uit te kunnen voeren.
15. De documentatie van het herstelproces moet aantoonbaar geteste procedures omvatten voor het herstel van server of applicatiestoringen.
16. De back-up en recovery procedures moeten actueel blijven. Bij veranderingen door applicatie- en organisatie wijzigingen en het gebruik van nieuwe technologie worden de procedures direct aangepast.
17. De back-ups dienen dagelijks gecontroleerd te worden op aanwezigheid en eventuele foutmeldingen.
18. De back-up en restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in

noodgevallen uitgevoerd moet worden. Dit wordt gedocumenteerd.
(BIO12.3.1.5)

19. Van back-up en recovery activiteiten en de verblijfplaats van de media wordt een logboek bijgehouden.
20. De back-up media worden vernietigd in overeenstemming met het beleid omtrent behandeling van digitale media van de organisatie en de hiervoor geldende bewaartermijn.
21. De back-up is op een dusdanige wijze van encryptie voorzien dat deze achteraf niet aan te passen of te wijzigen is.

2.1.2 SAAS

22. Bij SAAS systemen blijft de verantwoordelijkheid bij de organisatie.
23. Jaarlijks wordt bij de SAAS leverancier een overzicht van de controles op de back-up en restore test(en) opgevraagd. Dit wordt vastgelegd

2.1.3 Cloud

24. In de Private Cloud is het back-up beleid van de organisatie leidend.
25. In de Publieke Cloud, waaronder Office 365, zorgt de organisatie voor een aanvullende back-up voorziening als de standaard mogelijkheden tekort schieten.

2.1.4 Content

26. Voor alle door de organisatie gebruikte contentsystemen gelden de eisen uit dit document.

2.1.5 Bewaartermijnen

27. We bewaren de verslagen van het maken van back-up en restore conform de bewaartermijnen uit de archiefwet. In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar. (BIO 16.1.7.1)
28. Bij het vernietigen van een back-up volgen we de archiefvernietigingsprocedure volgens artikel 8 Archiefbesluit.

3. Organisatie, taken en verantwoordelijkheden

In dit hoofdstuk zijn de taken en verantwoordelijkheden beschreven.

3.1 Teammanager GMB

- Ziet toe op de uitvoering van de Archiefwet namens het college.
- Zorgt dat het back-up beleid word bijgesteld als de Archiefwet dat vereist.

3.2 Teammanager I&A

- Is eindverantwoordelijk voor de uitvoering van dit beleid.

3.3 Coördinator informatiebeveiliging

- Zorgt voor het opzetten, invoeren en monitoren van dit beleid.
- Zorgt ervoor dat er in samenwerking met de functionaris informatiebeveiliging een jaarlijkse evaluatie is van het back-up beleid en dat op basis van nieuwe wet- en regelgeving, mogelijkheden en risico's het beleid wordt bijgesteld.
- Controle op uitvoering van afgesproken werkzaamheden.

3.4 Functionaris informatiebeveiliging

- Houdt toezicht op de naleving van dit beleid en rapporteert hierover aan de directie.

3.5 Leveranciers

- SAAS leveranciers zijn verantwoordelijke voor de uitvoering van de back-up conform dit beleid.

- Een onderaannemer (RAM-IT) is verantwoordelijk voor de uitvoering van dit beleid op de systemen waar zij het beheer over voeren.

3.6 Data- of applicatie eigenaar

- De dataeigenaar is verantwoordelijk voor het juist laten back-uppen van de data.
- De applicatie-eigenaar voert regelmatig (jaarlijks) een restore uit en test deze.
- De applicatie eigenaar controleert regelmatig (maandelijks) de back-up en restore procedures.

3.7 Gebruikers

- Slaat data op in de door organisatie aangeboden informatiesystemen, zodat deze meegaan in de back-up oplossing van de organisatie.
- Zijn op de hoogte van het Digitaal toegangsbeleid.

Gemeente Hoorn

Nieuwe Steen 1

Postbus 603

1620 AR Hoorn

T 0229 25 22 00

www.hoorn.nl

