GEMEENTE VELSEN

Beleid back-up en Recovery

Documentcode:	
Versie:	1.2
Versiedatum	30 april 2024
Gemaakt door:	Pieter Ouwerkerk, Marleen Peper
Goedgekeurd door:	College van Burgemeester en Wethouders
V-Classificatie:	Intern document / openbaar

Versiegegevens

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
02-04-2024	0.1	Pieter Ouwerkerk Marleen Peper	Concept basisdocument
03-04-2024	0.2	Pieter Ouwerkerk Marleen Peper	Opmerkingen verwerkt
04-04-2024	1.0	Pieter Ouwerkerk Marleen Peper	Versie 1 definitief gemaakt
29-04-2024	1.1	Pieter Ouwerkerk Marleen Peper	Opmerkingen DT en OGD verwerkt
30-04-2024	1.2	Pieter Ouwerkerk Marleen Peper	Besproken met manager Informatie

Inhoud

1. Aanleiding

Het bestaande beleid was geschreven vanuit een omgeving waarin de systemen in beheer waren van de gemeente Velsen en ook fysiek bij de gemeente Velsen stonden. Bij de overgang naar de nieuwe werkplek in de Cloud en de overgang naar SaaS-systemen moet back-up en herstel anders georganiseerd worden. Hierbij hoort een nieuw back-up en recovery beleid waarbij de gemeente meer gaat sturen en controleren en veel minder zelf gaat uitvoeren.

2. Doel

Het doel van back-up en recovery is te zorgen dat bij een calamiteit in onze systemen informatieverlies voorkomen wordt door de informatie te herstellen naar een moment waarvan we zeker weten dat de informatie op orde is.

3. Toelichting

De gemeente Velsen is steeds afhankelijker geworden van informatietechnologie. Daarom is het noodzakelijk dat de systemen en daarin opgeslagen informatie hersteld kunnen worden als door een incident systemen niet meer beschikbaar zijn. Hierbij moet niet alleen gekeken worden of de gegevens benaderbaar zijn, maar ook of ze veilig zijn. Naast inhoudelijke gegevens, vallen hieronder ook zaken als programmatuur en systeeminstellingen die nodig zijn om de gegevens te raadplegen.

4. Onderbouwing

Informatiesystemen zijn steeds complexer geworden. Door het uitbesteden van het beheer van deze systemen aan leveranciers, hoeft de gemeente minder technische kennis in huis te hebben en kan de gemeente gebruik maken van specifieke expertise van deze leveranciers. Tegelijkertijd betekent het ook dat de gemeente de gegevens niet meer zelf in huis heeft en meer moet sturen op beschikbaarheid en herstelbaarheid van gegevens, specifiek bij het niet meer beschikbaar zijn van systemen of gegevens. De oorzaak daarvan is minder relevant. Of er nu een brand in de serverruimte bij de leverancier is of dat systemen niet meer beschikbaar zijn door gijzelsoftware, de systemen en gegevens moeten hersteld kunnen worden, zodat de gemeente haar werkzaamheden kan blijven uitvoeren. Hierbij maken we wel onderscheid tussen kritieke systemen, die essentieel zijn voor onze dienstverlening aan de inwoner, en overige systemen die ondersteunend zijn maar minder – of niet kritiek en daarmee minder van belang zijn voor de continuïteit van onze dienstverlening. We sluiten hierbij aan op de systeemclassificatie zoals die ook in het informatiebeveiligingsbeleid wordt gebruikt.

4.1 Kritieke ketens

Systemen werken niet altijd volledig zelfstandig en kunnen gekoppeld zijn met andere systemen. Zo wordt het zaaksysteem gebruikt als documentopslag voor processen die in een ander systeem worden uitgevoerd. Voor de ketens die direct de dienstverlening aan onze inwoner raken, wordt aanvullend aan de reguliere testen (zie 5.5 Testen herstelprocedure) periodiek (minimaal eens per 3 jaar) een test gedaan waarbij wordt gecontroleerd of we de hele keten terug kunnen zetten naar een bepaald moment in het verleden.

5. Uitgangspunten

Een back-up is niet hetzelfde als een archief. Archieven moeten wel meegenomen worden in de back-up, maar een back-up is geen vervanger van een archief.

5.1 Tijdreizen

Bij het bewaren van back-ups wordt gewerkt met minimaal twee soorten termijnen. Voor systemen die kritieke processen ondersteunen, wordt een langere termijn gehanteerd dan voor andere systemen.

- Voor kritieke systemen worden de laatste twee geteste en goedgekeurde back-ups verplicht bewaard, samen met alle back-ups die na deze tests zijn gemaakt.
- Voor kritieke systemen moet er tot op de dag nauwkeurig een back-up teruggezet kunnen worden.
- Voor andere systemen wordt alleen de laatste geteste en goedgekeurde back-up bewaard, samen met alle back-ups die na deze test zijn gemaakt.

Het uitgangspunt is om altijd terug te kunnen vallen op een recente werkende back-up, terwijl ervoor wordt gezorgd dat er altijd een goede back-up beschikbaar is.

5.2 Onafhankelijk van locatie

De leverancier moet ervoor zorgen dat gegevens en systemen hersteld kunnen worden, ook als de primaire locatie waar deze zijn opgeslagen niet meer beschikbaar is.

5.3 Uitvoering van beleid:

Bij het aangaan van overeenkomsten worden afspraken en procedures vastgelegd bij het contract met de leveranciers. Deze worden vastgesteld bij het in beheer nemen van systemen. Nieuwe leveranciers moeten bij het sluiten van een overeenkomst deze afspraken en procedures naleven.

5.3.1 Restore vs AVG

- Back-up media die persoonsgegevens bevatten, moeten voldoen aan de AVG-wetgeving, wat betekent dat ze versleuteld moeten worden opgeslagen en dat verwijderverzoeken van gegevens moeten worden gerespecteerd. Indien nodig moet een verwijderverzoek opnieuw kunnen worden uitgevoerd, zelfs als oudere back-ups worden hersteld.

5.4 Hersteltijden

Gegevens moeten goed te restoren zijn binnen de afgesproken acceptabele tijd (conform BIO):

- Dataverlies bedraagt maximaal 28 uur;
- Hersteltijd na een incident is maximaal 16 uur in 85% van de gevallen.

5.5 Testen herstelprocedure

Testen moeten regelmatig gedaan worden. Minimaal eens per jaar maar ook na een grote wijziging waarbij de achterliggende gegevens bij systemen op een andere manier worden opgeslagen (conform BIO). De mate van betrouwbaarheid moet hoog zijn omdat er vanuit gegaan wordt dat het herstellen ook daadwerkelijk mogelijk is. Na de test moet bewezen kunnen worden dat er een geslaagde test heeft plaatsgevonden conform testprocedure en correcte verslaglegging.

5.6 Rollen en verantwoordelijkheden

Voor een correcte uitvoering moeten in ieder geval onderstaande rollen en verantwoordelijkheden worden belegd in de organisatie.

De manager verantwoordelijk voor team Informatie kan deze wijzigen door de bijlage[1] met rollen en verantwoordelijkheden aan te passen.

- Vaststellen back-up beleid;
- Toetsen uitvoering back-up beleid;
- Evalueren en voorstellen wijzigingen back-up beleid;
- Afspraken met leveranciers vastleggen;
- Monitoren uitvoering afspraken en beoordelen testverslagen;
- Steekproeven uitvoeren op restoretests?
- Signaleren (grote) wijzigingen bij leveranciers;

5.7 Overdragen verantwoordelijkheden

Zolang de gemeente Velsen verantwoordelijk is voor de door haar gebruikte systemen en de daarin opgeslagen informatie, blijft de gemeente eindverantwoordelijk voor het correct naleven van het back-up beleid.

Zodra informatie wordt overgedragen aan een daarvoor aangewezen organisatie, zoals het Noord-Hollands Archief, is deze organisatie verantwoordelijk voor een deugdelijk back-up beleid en een correcte uitvoering daarvan.

6. Monitoring

Jaarlijks wordt het back-up beleid geëvalueerd en getoetst aan veranderende richtlijnen, geldende wet- en regelgeving en de behoefte vanuit de organisatie. Mocht blijken dat uit deze evaluatie wijzigingen naar voren komen, dan wordt het beleid daarop aangepast.

Daarnaast wordt bekeken of het back-up beleid nog in lijn is met de samenhangende documentatie (zoals: informatiebeveiligingsbeleid, informatiebeheerplan, informatievisie, uitvoeringsplan Back-up & Recovery). Dit om consistentie te waarborgen in het bredere kader van informatiebeveiliging en operationele processen.

[1] Bijlage 1: Rollen en verantwoordelijkheden back-up beleid