

Memo

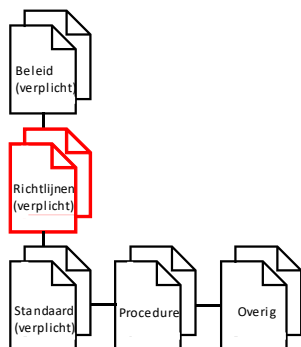
Backup PNB: maximaal dataverlies, bewaartermijnen backup sets, en hersteltijden

Inleiding

Regieorganisatie Dienstverlening ICT voert een project uit om de PNB backup in te richten, met de focus op de inrichting van backup voor de Office365 diensten (SharePoint Online, Teams, OneDrive, Exchange Online). Vanuit dit project is een voorstel uitgebracht hoe de backup voor PNB ingericht kan worden. Daarnaast wordt aangegeven dat PNB informatie moet aanleveren om het voorstel af te kunnen ronden, en de backup-oplossing te kunnen realiseren.

Deze memo is een aanvulling op de PNB beleidsstukken en richtlijnen in relatie tot backup, met name "IB Richtlijn Back-up en Recovery versie 1.5" (beschouwd als verplicht Beleid), en geeft antwoorden op vragen vanuit de Regieorganisatie Dienstverlening ICT op het gebied van maximaal dataverlies, bewaartermijnen van backup, en hersteltijden. De uitspraken in deze memo zijn richtlijnen voor de Regie-organisatie voor de uitwerking van de backup-oplossing zoals deze beschreven is in het document "PNB Inrichtingseisen Back-up en bewaartermijnen". Onderstaande figuur geeft de positie van deze memo weer in relatie tot haar omgeving.

Uitgangspunt is dat het beleid de minimale eisen weergeeft, en dat in specifieke gevallen (en contractueel geborgd) strengere eisen gelden. Daarom zijn ook de volgende PNB-OGD contractdocumenten in beschouwing genomen (als verplichte Richtlijnen): "E2_SLA TMO v1.1_get_20210305", "F6_Solution Document_v1.0 get 20200402", "F5_SLA FMO & dienstbeschrijving_v1.1 get 20210615" inclusief "Bijlage 1 : Backup Retentie PNB". Ook het document "PNB Back-up strategie versie 1.0" van de Regieorganisatie Dienstverlening ICT is meegenomen bij de totstandkoming van deze memo.



Onderlinge relatie tussen de documenten:

IB Richtlijn Back-up en Recovery versie 1.5

E2_SLA TMO v1.1_get_20210305

F6_Solution Document_v1.0 get 20200402

F5_SLA FMO & dienstbeschrijving_v1.1 get 20210615

PNB Back-up strategie versie 1.0

PNB Back-up en Bewaartermijnen (deze memo)

PNB Inrichtingseisen Back-up en bewaartermijnen (Overig)



Back-up is NIET bedoeld om te archiveren; een archief is een onafhankelijke functionaliteit (waar natuurlijk ook een back-up van gemaakt moet worden).

Acceptatie en Goedkeuring

Acceptatie en goedkeuring	Datum	

Overzicht maximaal data verlies en bewaartermijnen

Uitgangspunten bij het bepalen van het maximaal toegestane data verlies en bewaartermijnen backup:

1. Van elke informatieverzameling bestaan conform PNB beleid minstens drie versies ("PNB Back-up strategie versie 1.0").
2. Onderstaande tabel kent de informatieverzamelingen zoals Regieorganisatie Dienstverlening ICT deze onderscheid.
3. Er wordt op dit moment geen onderscheid gemaakt in bewaartermijnen afhankelijk van dataclassificatie binnen PNB.
4. De eigenaar van een informatieverzameling/data set kan af (laten) wijken van hier onder genoemde backup bewaartermijnen na goedkeuring van de CISO.
5. Retentietermijnen van data (informatie) in relatie tot privacy- en archiefwetten worden geborgd in die systemen waarin deze data wordt verwerkt, niet in de backup (b.v. conform archiefwet vernietigen van documenten of records).

Informatieverzameling	Maximaal data verlies (RPO) 2) / 3)	Locatie Productie	Bewaartermijn Eerste Backup kopie (Onsite)	Bewaartermijn Tweede Backup kopie (Offsite) 5)	Herstel granulariteit bestandsniveau
Bestandsshares (CIFS/NFS/DFS)	24 uur	PNB Private Cloud	1 maand	1 jaar	Ja
'Ruwe' R&D data (Dataplatforms, BI, etc)	24 uur	PNB Private Cloud	1 maand	1 jaar	Ja
SAP	PRD: 2 uur 3)	PNB Private Cloud	2 weken	1 jaar	Ja
	DEV: 2 uur 3)	PNB Private Cloud	2 weken	n.v.t	Ja
	QAS: 24 uur	PNB Private Cloud	1 maand	n.v.t	Ja
	Sandbox: 24 uur	PNB Private Cloud	2 weken	n.v.t	Ja
Databases Schema 1	2 uur 3)	PNB Private Cloud - Azure (Microsoft Public Cloud)	2 weken	1 maand	Ja 7)
Databases Schema 2	24 uur	PNB Private Cloud - Azure (Microsoft Public Cloud)	2 weken	1 maand	Ja 7)
Databases Schema 3	24 uur	PNB Private Cloud - Azure (Microsoft Public Cloud)	1 maand	1 jaar	Ja 7)
SaaS en PaaS data 1)	PRD: 24 uur	Public Cloud (Azure, Leverancier, etc)	1 maand	1 jaar	Ja 7)
	ACC: 24 uur		1 maand	1 maand	Ja 7)
	TST: 48 uur		2 weken	n.v.t.	Ja 7)
SharePoint Online	24 uur	Office365 4)	1 maand	1 jaar	Ja 8)
Teams (zie SharePoint)	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
Exchange Online (e-mail)	24 uur	Office365 4)	1 maand	1 jaar	Ja
OneDrive	24 uur	Office365 4)	1 maand	1 jaar	Ja
Power Platform	24 uur	MSFT SaaS	1 maand	1 jaar	Ja
MSFT Dynamics	24 uur	MSFT SaaS	1 maand	1 jaar	Ja
Systeemlogboeken (buiten SIEM)	24 uur	PNB Private Cloud	3 maanden	1 jaar 6)	Ja
Servers (VMs, Azure VMs)	PRD: 24 uur	PNB Private Cloud - Azure (Microsoft Public Cloud)	2 weken	1 maand	Ja 7)
	ACC: 24 uur		2 weken	1 maand	Ja 7)
	TST: 48 uur		2 weken	n.v.t.	Nee
	ONT: 48 uur		2 weken	n.v.t.	Nee
	Sandbox: 1 week		2 weken	n.v.t.	Nee
Servers (fysiek)	24 uur	PNB Private Cloud	2 weken	1 maand	Nee
Server images/templates	Laatste versie 3)	PNB Private Cloud	2 weken	2 weken	Nee
Azure storage (disks, blobs, files, queues etc.)	PRD: 24 uur	Azure (Microsoft Public Cloud)	1 maand	1 jaar	Ja 7)
	ACC: 24 uur		1 maand	1 jaar	Ja 7)

Informatieverzameling	Maximaal data verlies (RPO) 2) / 3)	Locatie Productie	Bewaartermijn Eerste Backup kopie (Onsite)	Bewaartermijn Tweede Backup kopie (Offsite) 5)	Herstel granulariteit bestandsniveau
	TST: 48 uur		2 weken	n.v.t.	Nee
	ONT: 48 uur		2 weken	n.v.t.	Nee
	Sandbox: 1 week		2 weken	n.v.t.	Nee
Apparaat configuraties	Laatste config 3)	PNB Private Cloud	1 maand	3 maanden	Ja
Systeemstatussen (system state)	24 uur	PNB Private Cloud	2 weken	1 maand	Ja
Active Directory	24 uur	PNB Private Cloud	1 maand	1 maand	Ja
Azure Active Directory (config)	24 uur	Azure (Microsoft Public Cloud)	1 maand	1 maand	Ja
Microsoft 365 Config	24 uur	Azure (Microsoft Public Cloud)	1 maand	1 maand	Ja
Azure Infra-as-a-Code (scripts, templates, repositories, etc)	24 uur	Azure (Microsoft Public Cloud)	1 maand	1 maand	Ja
Azure Governance (Subscriptions, policies, MGs, ec.)	24 uur	Azure (Microsoft Public Cloud)	1 maand	1 maand	Ja

Opmerkingen

- 1) Voor SaaS en andere extern gefaciliteerde IT diensten, moeten in de contracten afspraken zijn vastgelegd over backup en recovery in lijn met PNB beleid. Nog niet vastgesteld is of PNB zelf een eigen backup kopie van deze data wil hebben (en voor welke diensten dan).
- 2) Volgens PNB beleid is de RPO maximaal 24 uren. Minder mag: Raadpleeg hiervoor de bijbehorende contracten en SLA's via de contracteigenaar. Afhankelijk van het service level tot 1 uur voor Goud, 4 uren voor Zilver, 8 uren voor Brons (80% van de metingen).
- 3) De leverancier bepaalt hoe deze eis wordt ingevuld (denk aan een combinatie van kopiëren, incrementele en/of differentiele backups, transactielogboeken en system baselines).
- 4) Office365 kent retentie tijden ("bewaartermijnen") voor data die door de medewerkers verwijderd is zoals e-mails, SharePoint of OneDrive bestanden, en sites, teams en mail-boxen van medewerkers uit dienst, opgeheven teams etc. Na deze retentietijd wordt deze data automatisch verwijderd. Vanuit PNB zien we deze data kopiëren niet als backup kopie, omdat beheerder en/of medewerker data kan verwijderen zonder dat zo'n kopie bestaat.
- 5) De termijn voor de tweede backup is voor de meeste informatieverzamelingen op 1 jaar gezet conform PNB beleid. Dit biedt een goede balans tussen de risico's en impact van cyberaanvallen (b.v. ransomware) en privacy-, en archief wetgeving (zie ook de opmerking onder Hersteltijden). Randvoorwaarde hierbij is dat maatregelen genomen worden voor de tweede backup op het gebied van toegang (IAM) en voorkomen van aanpassingen van een backup (immutable of offline) nadat deze is gecreëerd. Voor databases is de termijn op een maand gezet vanwege de complexiteit een oudere backup consistent en integer te herstellen binnen het PNB applicatie- en data landschap. Er moet dan een andere oplossing gevonden worden. Voor Servers, configuraties en directories is de termijn korter gezet dan een jaar vanwege de complexiteit van het herstellen van doorgevoerde wijzigingen hierop als hiervoor langere termijnen worden gekozen.
- 6) Voor systeemlogboeken (eventlogs etc.) kunnen vanuit informatiebeveiliging, in het kader van forensisch onderzoek wellicht andere eisen worden gesteld, daar is hier niet van uit gegaan.
- 7) Indien mogelijk, afhankelijk van applicatie/software.
- 8) Betreft individuele bestanden, (sub-)sites, html-pagina's, etc.

Hersteltijden

De hersteltijd (Recovery Time Objective, RTO) in geval van incidenten bedraagt van PNB beleid maximaal 16 werkuren in 85% van de gevallen. Sneller mag: Raadpleeg hiervoor de bijbehorende contracten en SLA's via de contracteigenaar.

Opmerking:

Genoemde hersteltijden gelden in geval van normale (IT) operatie. En betreffen niet alleen de tijden om de data van een backup te restoren maar ook de vereiste controles en nabewerkingen door b.v. applicatiebeheerders die moeten worden uitgevoerd voordat het systeem, applicatie of informatie/data kan worden vrijgegeven voor gebruik. Denk hierbij aan het controleren van de consistentie en integriteit en het wederom vernietigen van data die op basis van archief- en/of privacy wet- en regelgeving in de productieomgeving reeds vernietigd is.

In geval het BCP in werking treedt, b.v. als gevolg van een calamiteit waardoor de totale IT dienstverlening vanuit een PNB data center uitvalt, dan worden systemen, applicaties, informatieverzamelingen/data sets herstelt in de prioriteitsvolgorde zoals vastgesteld in dit BCP.

Afkortingen en Begrippen

Afkortingen en Begrippen	Beschrijving
BCP	Business Continuity Plan
IAM	Identity & Access Management
Offsite	De term Offsite verwijst naar een datacenter locatie die verschillend is van de primaire PNB Data Centers. Deze wordt gebruikt voor opslag van backups zodat deze beschikbaar zijn voor herstel als de primaire PNB Data Centers worden getroffen door een calamiteit.
Onsite	Hiermee worden de primaire PNB datacenters bedoeld.
PNB Private Cloud	PNB Private Cloud, gehost in datacenters van PNB zelf (Den Bosch) en de Equinix datacenter in Amsterdam
Recovery	Recovery is het herstel van gegevens, een applicatie of omgeving naar de staat vóór het incident. Recovery is noodzakelijk na het verloren gaan van een applicatie of gegevens.
RPO	Recovery Point Objective. RPO is de maximale leeftijd van data die vanuit de back-up moeten worden hersteld om de normale werking te kunnen hervatten als een computer, systeem of netwerk uitvalt ten gevolge van een hardware-, programma- of communicatiefout.
RTO	Recovery Time Objective. RTO is de maximaal gewenste tijdsduur tussen een onverwachte storing of ramp en de hervatting van de normale activiteiten en dienstverleningsniveaus. De RTO bepaalt het tijdstip na een storing of ramp waarop de gevolgen van de onderbreking onaanvaardbaar worden.
PROD	Productie omgeving
ACC	Acceptatie omgeving
TST	Test omgeving
DEV	Development omgeving
ONT	Ontwikkel omgeving
QAS	Quality Assurance Omgeving