



PNB Back-up strategie

Auteur: Peter van de Bree
Versie: 0.9
Creatie datum: 10-06-2022
Revisie datum: 06-10-2022

Voorblad

Onderwerp	Omschrijving
Documentnaam:	PNB Back-up Strategie
Aantal pagina's:	3
Opsteller:	Peter van de Bree
Status:	0.9 Concept
Datum	06-10-2022
Classificatie:	Bedrijfsvertrouwelijk

Specifieke besluiten

Acceptatie en goedkeuring	Datum	
Akkoord gevraagd op de Back-up Strategie		
Akkoord gevraagd op het inregelen van de back-up oplossing op basis van de back-up strategie en processen.		

Vervolg

Vervolgstappen	Datum	
Op basis van deze vastgestelde Back-up strategie wordt een traject gestart voor de keuze van een back-up oplossing		

Back-up Strategie: van ambitie naar principes, met een schaalbaar, wendbaar en betrouwbaar platform voor Informatieveiligheid

Informatie veilig stellen met een verantwoordelijkheid om informatie gegevens te beveiligen tegen:

- ✓ (On)opzettelijke verwijdering
- ✓ Bestands corruptie
- ✓ Cyberaanvallen en ransomware
- ✓ Uitval / calamiteiten op Datacenter / Cloud omgevingen

Informatieveiligheid wordt ingezet vanuit **focus** op de beveiliging van primaire processen, vanuit **expertise** op het gebied van veiligheid en **eenduidig** binnen de afdelingen en over de organisatie.

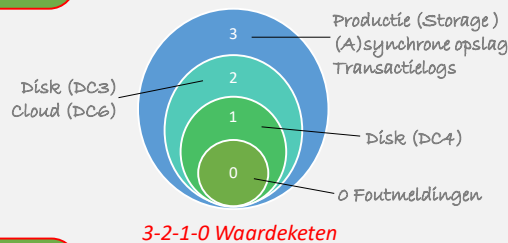
Paradigmashift

De rol van informatiebeveiliging verschuift van “**zorgen voor**” naar “**zorgen dat**”, de data - die zich ontwikkelt met 21-eeuwse eisen en vaardigheden – is beschermd, de Back-up anticipeert.

Provincie Noord-Brabant

Data steeds belangrijker

Formele en informele informatieoverdracht binnen de organisatie, met collega's, partners en hun wettelijk vertegenwoordigers en met ketenpartners is steeds belangrijker



Processen verder verbeteren

Technologie wordt steeds professioneler en breder toepasbaar: remote werken, apps, portalen, self service, sociale media, eLearning, etc. Druk op budgetten blijft bestaan.

Data overal en altijd

Alle medewerkers en klanten willen toegang hebben tot data. Plaats --, tijd en apparaat onafhankelijk. Veiligheid, beschikbaarheid en betrouwbaarheid van data is essentieel. Schaalbaarheid is tevens belangrijk.

Doelstellingen

- ★ **Back-up voor borging van beschikbaarheid en continuïteit van data.**
Bieden van beveiliging vanuit ICT door het waarborgen van de beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van data, zodat de continuïteit van primaire processen ten allen tijden gegarandeerd zijn (ook bij uitval van primaire ICT systemen).
- ★ **We hanteren de 3-2-1-0 regel voor de waardeketen.** Voor alle data hebben we 3 verschillende versies, 2 opslagmedia, 1 off-site back-up en een herstelplan die 0 fouten bevat.
 - SAN Storage (Productie, (a)synchrone, snapshots)
 - Disk Storage en Cloud
 - Off-site back-up (geografisch elders dan waar de bron data zich bevindt)
- ★ **Er is een wendbare en hybride back-up inrichting.**
We maken gebruik van technische componenten die hieraan kunnen voldoen en verzorgen in voorspelbare kwaliteit en kosten. proces, beheer en technologie van de back-up voorzien in data opslag van zowel traditionele (On Prem) als nieuwe vormen van IT diensten (Cloud based)
- ★ **Back-up is betrouwbaar en hoog beschikbaar.**
Voldoet aan IB beleid, BIO, wet & regelgeving* en 'best practices. data is veilig, integer en betrouwbaar. Er is een geïsoleerde DR back-up omgeving die voldoet aan cyber security eisen en maatregelen.
- ★ **Borgen van (langdurige) beschikbaarheid van data.**
Er is een aparte 'IAM ingang' voor een geïsoleerde DR back-up. PNB wil zich maximaal verzekeren tegen corruptie, ongewenste versleuteling of verwijdering van de brondata op de operationele ICT omgeving. Door gebruik te maken van het WORM (Write Once Read Many) concept.

Uitgangspunten

- ★ Er vindt controle plaats op de back-up en op informatie corruptie middels monitoring, via dashboards en logboeken en regelmatige recovery-tests.
- ★ Informatieveiligheid van al onze data, ongeacht Cloud of OnPrem, wordt bepaald door de informatie eigenaar, die bepaald de RPO van maximaal dataverlies vanuit de 3-2-1-0 waardeketen. BIO richtlijn schrijft voor te voldoen aan een RPO van hooguit 24u aan dataverlies.
- ★ Informatieveiligheid sluit aan op de **Cloud Strategie**. De huidige OnPrem voorziening alleen voor OnPrem back-up. Voor Cloud (SaaS, PaaS, IaaS) een **Cloud-Native back-up voorziening**.
- ★ DVL-ICT is belast met het uitvoeren van dit beleid en verzorgt registratie van alle back-up media en (Cloud)locaties waar back-ups zich bevinden.
- ★ We kiezen **product leadership** voor onderscheidende Informatiebeveiliging en voor informatie beschikbaarheid (buiten de operationele ICT omgeving)
- ★ **Uitbesteden** doen we waar dit verantwoord kan en vanuit een beheersbare situatie.

Principes

- ★ Wij weten te allen tijde waar onze data zich bevindt (locatie) en zijn ons hiervan bewust. Data binnen EER (Europese Economische Ruimte; BIO).
- ★ Gebruik eigen private **encryptiesleutels**, zodat we zelf de back-upgegevens beheren en niet de leverancier.
- ★ Back-up van persoons- of bedrijfsdata in de Cloud zijn voorzien van encryptie conform beleid. Zowel in opslag als tijdens **transport**.
- ★ De back-up applicatie is voor admins alleen bereikbaar vanaf een steppingstone en netwerk-segmenten door middel van een firewall.
- ★ Back-up moet **ransomware-proof** zijn.
- ★ Gebruik verschillende opslagproviders voor **off-site back-up**, om risico's te beperken. Bij Cloud letten we op bandbreedte of andere extra kosten voor gegevensoverdracht en transport.
- ★ Maken van back-ups mag **geen performance impact** hebben op de operationele processen van PNB.
- ★ Compliant met BIO en AVG inzake persoonsgegevens in de back-up.
- ★ Back-up jobs worden **binnen 24u afgerond**. Gebruikmakend van de verschillende methoden van back-up; differential, Incremental en Full.
- ★ We maken gebruik van **Least Privilege Access** concept en hebben een extra beschermingslaag met MFA.
- ★ De back-up recovery granularity objective (**RGO**) is waar nodig op detail niveau (item-level), voorbeeld; email berichten, Sharepoint items.
- ★ **Voorkomen** is beter dan genezen. We vertrouwen niet alleen op back-ups. We hanteren een combinatie van endpoint protection, e-mail security en cybersecurity awareness trainingen om de risico's van een ransomware aanval zo klein mogelijk te maken.
- ★ Back-up in lijn met **retentie beleid** met data classificatie en de service level agreement (sla). Back-up oplossing is vertrouwelijk geclassificeerd.
- ★ **Data management** is op orde (waaronder data eigenaarschap, eenduidigheid, één bron, datakwaliteit)

Wensen

- ★ Back-up heeft **Self service** mogelijkheden voor gebruikers en servicedesk.
- ★ Back-up beheer middels één cockpit, **Single-pane-of-glass** concept.
- ★ Back-up is doorzoekbaar en is vindbaar middels **eDiscovery** concepten.