Bijlage J - Back-up en recovery beleid RID de Liemers

Ten behoeve van de beveiliging van informatie is er back-up en recovery beleid voor alle gemeentelijke voorzieningen. Het doel van dit beleid is te voorkomen dat, in geval van gedeeltelijk of geheel verlies of beschadiging van data en/of programmatuur, de dienstverlening van de gemeente of aangesloten GR geen hinder ondervindt.

RID de Liemers hanteert de onderstaande beleidsuitgangspunten en deze zijn ontleend aan de BIO en aanvullend op het algemene beveiligingsbeleid van de RID. Deze zijn van toepassing voor zowel RID de Liemers als derde partijen die data verwerken voor één of meer van de partijen die zijn aangesloten bij het samenwerkingsverband: Samenwerking de Liemers.

- Zowel de afdeling systeembeheer als derden partijen dienen aantoonbaar te voldoen aan de eisen beschreven in dit document;
- De back-ups van alle gemeentelijke informatie, software en besturingssystemen (en instellingen) moeten worden bewaard, zodat de computerbesturingssystemen, applicaties en informatie volledig hersteld kunnen worden in geval van een calamiteit;
- Dataverlies wordt beperkt tot maximaal 28 uur;
- De hersteltijd in geval van incidenten bedraagt maximaal 16 werkuren in 85% van de gevallen;
- 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;
- 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. Een off-site locatie dient een veilige ruimte in een apart gebouw van de gemeente of RID de Liemers te zijn of een locatie van een off-site storage-leverancier, waarbij deze off-site storage door de CISO van RID de Liemers dient te zijn goedgekeurd;
- Alle gemeentelijke informatie welke staat op werkstations, laptops of andere draagbare apparaten moeten worden opgeslagen op een netwerk file server om back-up mogelijk te maken;
- 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 rampscenario (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;
- Back-ups dienen dagelijks gecontroleerd te worden;
- Recovery procedures moeten minimaal op jaarbasis worden getest;
- Van back-up en recovery activiteiten en de verblijfplaats van de media wordt een logboek bijgehouden;
- Back-ups dienen beschermd te worden voor onbevoegde toegang door middel van versleuteling;
- Back-ups dienen alleen toegankelijk te zijn voor bevoegde personen;
- Alle back-ups dienen binnen de EU te worden opgeslagen;