



***DISASTER RECOVERY PLAN
KLAAR?
CONTROLEER HET!***



CHECKLIST



Moderne back-up strategie

Checklist

Immutable back-up



- Is je back-up immutable? Dus niet te wissen of aan te passen door eigen medewerkers of hackers?
- Breng afhankelijkheden en koppelingen in beeld

Risicoanalyse & impact



- Bepaal dreigingen (cyberaanval, brand, stroomuitval)
- Analyseer impact op bedrijfsprocessen
- Stel RTO (hersteltijd) en RPO (dataverliesgrens) vast

Back-upstrategie controleren



- Zijn er automatische back-ups ingesteld?
- Worden (online) back-ups regelmatig getest?
- Is alle data gescheiden en veilig opgeslagen (cloud, offline)?

Herstelprocedures definiëren



- Beschrijf per systeem hoe herstel plaatsvindt
- Test regelmatig de procedures
- Maak stappen begrijpelijk voor niet-technische medewerkers

Rollen & verantwoordelijkheden



- Stel een recovery-team samen
- Wijs per onderdeel verantwoordelijken aan
- Zorg voor vervanging bij afwezigheid

Helder communicatieplan



- Stel interne- en externe communicatieprotocollen op
- Gebruik templates en vooraf gedefinieerde boodschappen
- Zorg voor alternatieve kanalen bij uitval (zoals sms, telefoon)



Disaster Recovery Plan

Checklist

Testen & simulaties



- Plan (minimaal) jaarlijkse Disaster Recovery tests in
- Organiseer crisissimulaties
- Documenteer verbeterpunten na elke test

Versiebeheer & documentatie



- Werk met duidelijke versienummers
- Leg wijzigingen vast in een changelog
- Maak het Disaster Recovery Plan centraal en makkelijk toegankelijk

Wet- en regelgeving



- Check of het plan voldoet aan AVG/GDPR
- Stem herstelafspraken af met leveranciers (SLA's)
- Houd rekening met auditverplichtingen

Post-incident evaluatie



- Voer na elk incident een evaluatie uit
- Bespreek wat goed en fout ging
- Werk het DRP bij op basis van inzichten



 *Volg jij ons al?*