Beleid inzake gegevensback-up

Versie: 20180502

1 Doel

Het beleid voor gegevensback-up biedt uitgebreide documentatie over de toepasselijke regelgeving in het bedrijf en de maatregelen die zijn genomen voor gegevensback-up. Het dient tevens als bewijs voor derden dat de juridisch vereiste beschikbaarheidscontrole correct wordt uitgevoerd.

2 Verantwoordelijkheden binnen de onderneming

Bedrijven moeten zorgen voor IT-beveiliging en gegevensback-up. De bedrijfsleiding is hiervoor rechtstreeks verantwoordelijk en is persoonlijk aansprakelijk in de gevallen waarin de aanvraag wordt ingediend.

3 Algemene wettelijke voorwaarden

De wet vereist bepaalde controles via technische en organisatorische maatregelen, zowel voor eigen gebruik als voor gegevensverwerking, waarbij met name een beschikbaarheidscontrole van toepassing is. Verificatie van de controles of technische en organisatorische maatregelen dient onder meer te worden verstrekt aan klanten in het kader van de gegevensverwerking.

4 Risico's

1. Menselijke fout: verkeerde werking/ongeval, sabotage, aanval
2. Technische storingen: technisch defect, hardware storing, storingen aan de lijn
3. Overmacht, ongevallen, rampen: water, brand, enz.
4. Significante tot existentiële dreigende gevolgen voor bedrijven mogelijk

5 procedures voor gegevensback-up' s, opties

1. Volledige back-up
2. Incrementele back-up
3. Differentiële back-up

6 Minimum technische en organisatorische voorschriften

1. **Algemene voorschriften:**
   - Back-up van gegevens moet op verantwoordelijke en bekwame wijze worden uitgevoerd.
   - Geen onopzettelijke omzeiling van autorisatiemodellen door gegevensback-upmaatregelen
   - Vertrouwelijkheid en verplichting tot gegevensbescherming
   - Benoeming van de verantwoordelijken voor elk taakgebied
   - De noodzaak van vertrouwelijkheid, integriteit en beschikbaarheid vaststellen

2. **Technische uitvoering:**
   - Back-upplan voor gegevens maken
   - Bepalen van de bewaartermijn en het aantal generaties
   - Coördinatie met het beleid ter voorkoming van noodsituaties
   - Voldoende documentatie en logboekbeheer: met name back-upgegevens, omvang van de back-up, back-up van parametrices
   - Regelen van de terugvorderingsprocedure
   - inventarislijst aanmaken
   - Zorgen voor de evaluatie van stammen
   - Beproevingen van reconstructie/restauratie van gegevens en noodoefeningen
   - De nodige controles instellen, met name toegangscontrole
   - De beschermingseisen voor vertrouwelijkheid, integriteit en beschikbaarheid ten uitvoer leggen
   - Specificeer en beveilig vervoerroutes
   - Capaciteiten toewijzen: doorvoer, volume, hoeveelheid en hoeveelheid apparaten voor gegevensopslag
   - Vereisten implementeren voor naadloze back-up (mobiele computers, PDA/MDA, databases, open bestanden, systeem gegevens, loggegevens, enz.
   - Met name zorgen voor toegangscontrole, transmissiecontrole, invoercontrole en scheidingscontrole, ook met betrekking tot gegevens back-up sets