| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Voer hier de naam van de geregistreerde rechtspersoon in | | | | | | | |
| Documentnummer:<br>P15 | | | | | Documenttitel:<br>**Beleid inzake back-up en herstel** | | | | | | | |
| Versie:<br>1.0 | | Ingangsdatum:<br>01.01.2025 | | | Documenteigenaar: | | | | | | | |
| X | Beleid | | Standaard | | Procedure | | Formulier | | Register | | Overig | |

| **Revisiegeschiedenis** | | | | |
|---|---|---|---|---|
| **Revisienummer** | **Revisiedatum** | **Wijzigingen** | **Beoordeeld door** | **Proceseigenaar** |
| | | | | |
| | | | | |

| **Goedkeuringen** | | | |
|---|---|---|---|
| **Naam** | **Functie** | **Datum** | **Handtekening** |
| | | | |
| | | | |

Afgestemd op normen en regelgeving

| Norm/regelgeving | Clausule/artikel | Opmerking |
|---|---|---|
| ISO/IEC 27001:2022 | Clausules 6.1.3, 8.1 | Risicobehandeling, planning en operationele beheersmaatregelen voor back-up |
| ISO/IEC 27002:2022 | Beheersmaatregelen 8.13, 5.28, 5.29 | Back-upbeheer, veilige afvoer en weerbaarheid |
| NIST SP 800-53 Rev.5 | CP-9, CP-10, SI-12, MP-6 | Vereisten voor systeemback-up, herstel en mediasanering |
| AVG | Artikel 32, overweging 49 | Herstel en beschikbaarheid van persoonsgegevens, bedrijfscontinuïteit |
| EU NIS2 | Artikel 21(2)(c-e) | Beheersmaatregelen voor back-up en continuïteit ter ondersteuning van weerbaarheid |
| EU DORA | Artikelen 10, 11 | Vereisten voor back-up, herstel en testen in de financiële sector |
| COBIT 2019 | DSS01, DSS04, MEA03 | Back-upactiviteiten, continuïteit en continue nalevingsmonitoring |

## 1. Doel

1.1 Het doel van dit beleid is het vaststellen van verplichte eisen voor de back-up en het herstel van gegevens, systemen en applicaties ter ondersteuning van operationele weerbaarheid, gegevensintegriteit en bedrijfscontinuïteit.

**1.2 Dit beleid stelt een gestandaardiseerd kader vast om:**

1.2.1 Gegevens van de organisatie te beschermen tegen verlies als gevolg van verwijdering, corruptie, uitval of cyberaanvallen

1.2.2 Herstelverwachtingen vast te leggen met duidelijke parameters voor RTO (Recovery Time Objective) en RPO (Recovery Point Objective)

1.2.3 Back-upactiviteiten te integreren met het bredere ISMS en de bedrijfscontinuïteitsplannen

1.2.4 Naleving van toepasselijke wet- en regelgeving en sectorspecifieke voorschriften inzake beschikbaarheid en herstelbaarheid te waarborgen

1.3 Dit beleid geeft invulling aan beheersmaatregelen uit ISO/IEC 27001:2022 met betrekking tot veilige afvoer van gegevens (5.28), weerbaarheid (5.29) en operationeel herstel (8.13), en sluit aan op best practices uit ISO/IEC 27002:2022, NIST SP 800-53 Rev.5, de AVG, DORA en NIS2.

## 2. Reikwijdte

**2.1 Dit beleid is van toepassing op:**

2.1.1 Alle bedrijfskritische en operationele systemen binnen de reikwijdte van het ISMS

2.1.2 Alle gestructureerde en ongestructureerde bedrijfsgegevens, waaronder databases, bestanden, e-mails en configuraties

2.1.3 Alle omgevingen — on-premises, in de cloud gehost, hybride en externe/opslag buiten de locatie

2.1.4 Alle medewerkers die verantwoordelijk zijn voor het beheren, uitvoeren, verifiëren of herstellen van back-upprocessen

**2.2 Dit beleid is tevens van toepassing op:**

2.2.1 Back-upmedia en -infrastructuur, waaronder fysieke tapes, virtuele appliances, schijfsnapshots en cloudgebaseerde back-upoplossingen

2.2.2 Externe dienstverleners die zijn gecontracteerd om back-ups van de organisatie te hosten, beheren of verwerken

2.2.3 Back-ups van logbestanden, configuraties, audittrails en operationele documentatie die kritiek zijn voor continuïteit

2.3 Systemen die expliciet van back-up zijn uitgesloten, moeten worden gedocumenteerd, risicobeoordeeld en formeel geaccepteerd door de ISMS-manager en de systeemeigenaar.

## 3. Doelstellingen

3.1 Waarborgen dat van alle kritieke systemen en gegevens op betrouwbare wijze back-ups worden gemaakt met voldoende frequentie, redundantie en beveiligingsmaatregelen.

3.2 Herstelmechanismen bieden die voldoen aan vastgestelde RTO- en RPO-doelstellingen, in lijn met business impact analyses.

3.3 Volledige documentatie onderhouden van back-upprocedures, bewaarschema's, rollen en technologieën.

3.4 De doeltreffendheid van back-upactiviteiten valideren door systematische hersteltesten, logging van uitval en opvolging van corrigerende maatregelen.

3.5 Back-upgegevens gedurende de volledige levenscyclus beschermen tegen ongeautoriseerde toegang, wijziging of vernietiging.

**3.6 Naleving mogelijk maken van:**

3.6.1 operationele en continuïteitsvereisten uit ISO/IEC 27001

3.6.2 de NIST SP 800-53 CP- en MP-families voor back-up en sanering

3.6.3 AVG artikel 32 en overweging 49 voor herstel van toegang tot persoonsgegevens

3.6.4 DORA artikel 10 en NIS2 artikel 21 voor ICT-continuïteit en weerbaarheid

3.7 Waarborgen dat back-updiensten van derden voldoen aan contractuele en wettelijke beveiligingsverplichtingen, waaronder encryptie, afvoer en meldingsprotocollen.

## 4. Rollen en verantwoordelijkheden

### 4.1 Topmanagement

4.1.1 Bekrachtigt dit beleid en waarborgt dat bedrijfskritische systemen afdoende worden beschermd door goedgekeurde back-up- en herstelpraktijken.

4.1.2 Draagt de eindverantwoordelijkheid voor het waarborgen dat back-upactiviteiten over voldoende middelen beschikken en periodiek worden beoordeeld op naleving van wet- en regelgeving.

### 4.2 Chief Information Security Officer (CISO)

4.2.1 Is eigenaar van dit beleid en waarborgt afstemming met bredere kaders voor informatiebeveiliging, risico en continuïteit.

4.2.2 Houdt toezicht op de integratie van back-upprocedures in bedrijfscontinuïteitsplannen, incidentrespons en weerbaarheidsplanning.

4.2.3 Beoordeelt back-upuitzonderingen en evalueert voorstellen voor acceptatie van restrisico bij uitsluiting van kritieke systemen.

[ ... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ... ]

**9. Eisen voor herziening en actualisering**

**9.1 Dit beleid moet ten minste eenmaal per jaar worden beoordeeld, of eerder indien getriggerd door:**

9.1.1 Wijzigingen in de strategie voor bedrijfscontinuïteit of disaster recovery

9.1.2 Nieuwe wettelijke of juridische verplichtingen die invloed hebben op back-upfrequentie of gegevensbewaring

9.1.3 Wijzigingen in systeemarchitectuur, back-uptools of dienstverleners

9.1.4 Significante incidenten of auditbevindingen met betrekking tot gegevensverlies of herstelfouten

**9.2 De beoordeling moet worden gecoördineerd door de CISO in samenwerking met:**

9.2.1 IT-infrastructuur en IT-operatie

9.2.2 de interne audit- en compliancefunctie

9.2.3 de Functionaris voor gegevensbescherming (FG)

9.2.4 teams voor bedrijfscontinuïteit en disaster recovery

**9.3 Back-upschema's, lijsten met opgenomen systemen, hersteldocumentatie en uitzonderingslogboeken moeten gelijktijdig worden beoordeeld om te waarborgen:**

9.3.1 Juistheid van de back-updekking voor alle kritieke activa

9.3.2 Naleving van RTO/RPO- en bewaartermijnvereisten

9.3.3 Volledigheid van testlogbestanden en incidentrapportages

9.3.4 Correctie van eerder geïdentificeerde beheersingshiaten

**9.4 Alle actualisaties moeten:**

9.4.1 Onder versiebeheer worden geplaatst en worden bewaard in het ISMS-documentregister

9.4.2 Een samenvatting van wijzigingen en onderbouwing bevatten

9.4.3 Worden goedgekeurd door topmanagement

9.4.4 Worden gecommuniceerd aan alle betrokken technische en zakelijke medewerkers

**10. Gerelateerde beleidslijnen en samenhang**

**10.1 Dit beleid ondersteunt rechtstreeks en hangt samen met de volgende gerelateerde documenten:**

10.1.1 P6 - Beleid inzake risicobeheer: identificeert risicogebaseerde prioritering van back-upbescherming voor systemen en diensten.

10.1.2 P12 - Beleid inzake assetmanagement: waarborgt dat systemen die voor back-up in aanmerking komen zijn opgenomen in de inventaris en gekoppeld zijn aan levenscyclusbeheer en classificatie.

10.1.3 P13 - Beleid inzake gegevensclassificatie en etikettering: geeft richting aan welke gegevenscategorieën een back-up vereisen, inclusief classificatiemetadata voor prioritering.

10.1.4 P14 - Beleid inzake gegevensbewaring en afvoer: stemt bewaartermijnen van back-ups af op wettelijke bewaartermijnen en correcte afvoer van verlopen media.

10.1.5 P16 - Beleid inzake gegevensmaskering en pseudonimisering: ondersteunt gegevensminimalisatie tijdens back-up van gevoelige datasets.

10.1.6 P30 - Incidentresponsbeleid (P30): wordt geactiveerd bij back-upuitval, herstelproblemen of compromittering van back-updatarepositories.

10.2 Deze onderling samenhangende beleidslijnen vormen een consistent kader dat waarborgt dat back-upgovernance is ingebed in het bredere ISMS en de strategie voor operationele weerbaarheid van de organisatie.

## 11. Referentienormen en -raamwerken

### 11.1 ISO/IEC 27001:

11.1.1 Clausule 6.1.3 - risicobehandelingsplan: ondersteunt risicogebaseerde prioritering van back-ups en herstelplanning.

11.1.2 Clausule 8.1 - operationele planning en beheersing: integreert beheersmaatregelen voor herstel en continuïteit als onderdeel van operationele waarborgen.

11.1.3 Bijlage A beheersmaatregel 5.28 - veilige afvoer of hergebruik van apparatuur: behandelt veilige sanering van back-upmedia.

11.1.4 Bijlage A beheersmaatregel 5.29 - informatiebeveiliging tijdens verstoringen: waarborgt herstelmogelijkheden tijdens incidenten of rampen.

11.1.5 Bijlage A beheersmaatregel 8.13 - informatieback-up: wordt rechtstreeks afgedekt via geplande, geteste en beveiligde back-upactiviteiten.

11.2 ISO/IEC 27002:2022 - beheersmaatregelen 8.13, 5.28, 5.29: deze beheersmaatregelen versterken de eis voor regelmatige back-ups, integriteitsvalidatie en herstelplanning in alle IT-omgevingen.

### 11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-9 - systeemback-up: stelt uitgebreide back-upprocedures vast, waaronder opslag buiten de locatie en hersteltesten.

11.3.2 CP-10 - systeemherstel en -restauratie: vereist gevalideerde procedures voor volledig of gedeeltelijk herstel in lijn met hersteldoelstellingen.

11.3.3 MP-6 - mediasanering: waarborgt veilige omgang met verouderde back-upmedia.

11.3.4 SI-12 - procedures voor informatieverwerking: versterkt verantwoordelijkheden voor back-up en herstel van gevoelige gegevens.

### 11.4 AVG (2016/679):

11.4.1 Artikel 32 - beveiliging van verwerking: verplicht herstelmogelijkheden en waarborgen voor gegevensbeschikbaarheid, in het bijzonder voor persoonsgegevens.

11.4.2 Overweging 49: ondersteunt maatregelen voor bedrijfscontinuïteit en herstel na verstoringen, waaronder veilige back-up als onderdeel van organisatorische weerbaarheid.

### 11.5 EU NIS2-richtlijn (2022/2555):

11.5.1 Artikel 21(2)(c-e): vereist technische en organisatorische maatregelen, waaronder beheersmaatregelen voor back-up en continuïteit, om de weerbaarheid van diensten te waarborgen.

### 11.6 EU DORA (2022/2554):

11.6.1 Artikel 10 - ICT-bedrijfscontinuïteit: vereist dat financiële entiteiten beschikken over volledige gegevensback-up, herstel en continuïteitsplanning.

11.6.2 Artikel 11 - testen van ICT-bedrijfscontinuïteitsplannen: benadrukt validatie van herstelcapaciteit door middel van regelmatige tests.

### 11.7 COBIT 2019:

11.7.1 DSS01 - beheerde operaties: ondersteunt betrouwbare dienstverlening door beschermde beschikbaarheid van gegevens.

11.7.2 DSS04 - beheerde continuïteit: definieert strategische en operationele beheersmaatregelen voor continuïteit, waaronder geverifieerde back-ups.

11.7.3 MEA03 - Monitoren, evalueren en beoordelen van naleving: verplicht periodieke beoordeling van continuïteitsmaatregelen, waaronder de doeltreffendheid van back-upbeheersmaatregelen.