Informatiebeveiligingsbeleid

BLD-002

Voorbeeld IT B.V.

Waarom en hoe wij informatie beschermen. Vastgesteld door de directie.

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de ISO 27001 Toolkit · alle 56 documenten: www.maasiso.nl/toolkits/iso-27001/

Documentinformatie

DOCUMENTTITEL	Informatiebeveiligingsbeleid
DOCUMENTNUMMER	BLD-002
VERSIE	1.0
DATUM	19 oktober 2026
AUTEUR	Sanne de Vries
GOEDGEKEURD DOOR	Sanne de Vries
ORGANISATIE	Voorbeeld IT B.V.
CLASSIFICATIE	Intern

Versiehistorie

Versie	Datum	Auteur	Wijzigingen
1.0	19 oktober 2026	Sanne de Vries	Initiële versie

CLAUSULE 5.2 · A.5.1

1. Waarom dit beleid

Voorbeeld IT B.V. werkt elke dag met informatie van klanten, medewerkers en de eigen organisatie. Klanten vertrouwen ons die informatie toe. Als die informatie uitlekt, verloren gaat of niet beschikbaar is wanneer het nodig is, schaadt dat hen en ons.

Met dit beleid leggen wij vast hoe wij informatie beschermen. Het geldt voor iedereen die voor of namens Voorbeeld IT B.V. werkt.

Wij beheren de IT van ruim zestig MKB-klanten en hosten hun applicaties. Wij hebben daarvoor toegang tot hun systemen en gegevens. Een beveiligingsincident bij ons kan dus direct gevolgen hebben voor onze klanten.

2. Wat wij beschermen

Wij beschermen drie eigenschappen van informatie:

Eigenschap	Wat het betekent	Voorbeeld van een inbreuk
Vertrouwelijkheid	Alleen wie de informatie nodig heeft, kan erbij.	Een medewerker stuurt een klantbestand naar het verkeerde e-mailadres.
Integriteit	De informatie is juist en volledig en wordt niet ongemerkt gewijzigd.	Een aanvaller past bankrekeningnummers in facturen aan.
Beschikbaarheid	De informatie is er wanneer het nodig is.	Ransomware maakt alle bestanden onbruikbaar.

Het beleid geldt binnen het toepassingsgebied dat is vastgelegd in SCP-001 Toepassingsgebied.

3. Onze doelen

Het doel van informatiebeveiliging is dat Voorbeeld IT B.V. en haar klanten kunnen rekenen op betrouwbare informatie. Concreet streven wij naar:

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de ISO 27001 Toolkit · alle 56 documenten: www.maasiso.nl/toolkits/iso-27001/

- geen incidenten waardoor klanten schade lijden;
- snelle ontdekking en afhandeling als er toch iets misgaat;
- medewerkers die weten wat er van hen verwacht wordt en die problemen zonder aarzelen melden;
- aantoonbare naleving van wet- en regelgeving en van afspraken met klanten.

Deze doelen werken wij elk jaar uit in meetbare doelstellingen in DST-002 Doelstellingen informatiebeveiliging.

4. Onze verbintenissen

De directie van Voorbeeld IT B.V. verbindt zich ertoe:

1. te voldoen aan de eisen die gelden voor onze informatiebeveiliging: wetten, regels, contracten met klanten en de eisen van ISO/IEC 27001;
2. het managementsysteem voor informatiebeveiliging continu te verbeteren;
3. voldoende tijd, geld en kennis beschikbaar te stellen om dit beleid uit te voeren;
4. dit beleid elk jaar te beoordelen en eerder als er iets belangrijks verandert.

5. Zo pakken wij het aan

Wij werken risicogestuurd. Wij brengen in kaart wat er mis kan gaan, hoe waarschijnlijk dat is en wat de gevolgen zijn. Op basis daarvan kiezen wij maatregelen. Hoe wij dat doen, staat in ISB-P01 Procedure risicomanagement. De risico's staan in RSK-002 Risicoregister en behandelplan, de gekozen maatregelen in ISB-001 Verklaring van toepasselijkheid.

Restrisico's accepteren wij alleen bewust en volgens vaste regels: de risico-eigenaar mag lage en middelgrote risico's accepteren, alleen de directie mag hoge risico's accepteren en kritieke risico's accepteren wij niet.

Wat wij niet goed doen, leggen wij vast en verbeteren wij volgens AFW-P01 Procedure afwijkingen en verbetering.

6. Beleidsregels per onderwerp

Dit beleid geeft de richting. De concrete regels staan in beleidsregels per onderwerp. Die gelden net zo goed als dit beleid. Enkele onderwerpen staan samen in één document; de tabel laat zien waar elk onderwerp geregeld is.

Onderwerp	Waar de regels staan
Aanvaardbaar gebruik, werken op afstand, opgeruimd bureau en scherm	GBR-001 Regels voor medewerkers
Medewerkers: screening, geheimhouding, vertrek en disciplinaire maatregelen	HRM-P01 Procedure HR-beveiliging
Toegang tot systemen en informatie	ISB-P02 Toegangsbeheer
Incidenten melden en afhandelen	ISB-P03 Incidenten melden en afhandelen
Bedrijfscontinuïteit	ISB-P04 Bedrijfscontinuïteit
Leveranciers en clouddiensten	ISB-P05 Leveranciers en clouddiensten
Classificatie, labelen en uitwisselen van informatie	ISB-P06 Classificatie en uitwisseling van informatie
Werkplekken, malware, kwetsbaarheden en opslagmedia	ISB-P14 Werkplekken, malware en kwetsbaarheden
Privacy en persoonsgegevens	GBR-001 Regels voor medewerkers en REG-002 Wet- en regelgeving en contracten

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de ISO 27001 Toolkit · alle 56 documenten: www.maasiso.nl/toolkits/iso-27001/

Onderwerp	Waar de regels staan
Documenten en registraties beheren en bewaren	DOC-P01 Procedure documentbeheer
Back-up	ISB-P11 Back-up en herstel
Versleuteling	ISB-P09 Versleuteling
Logging en monitoring	ISB-P10 Logging en monitoring
Netwerk en cloud	ISB-P12 Netwerkbeveiliging
Wijzigingen aan systemen	ISB-P08 Wijzigingen in systemen en projecten
Fysieke beveiliging	ISB-P07 Fysieke beveiliging
Veilige softwareontwikkeling	ISB-P13 Veilige softwareontwikkeling

7. Wie waarvoor verantwoordelijk is

Rol	Verantwoordelijkheid
Directie	Stelt dit beleid vast, stelt middelen beschikbaar, accepteert hoge restrisico's en beoordeelt het managementsysteem minimaal elk jaar.
ISMS-coördinator	Zorgt dat het managementsysteem werkt, coördineert risicobeoordeling, audits en incidenten en rapporteert aan de directie.
Leidinggevende	Zorgt dat de eigen medewerkers de regels kennen en volgen.
Medewerker	Volgt de regels, gaat zorgvuldig om met informatie en meldt incidenten direct, uiterlijk binnen één uur na ontdekking.

Rol	Naam
Directie	Mark Jansen
ISMS-coördinator	Sanne de Vries

8. Bekendmaking

Wij maken dit beleid bekend:

- aan alle medewerkers bij indiensttreding en na elke wijziging, met een bevestiging dat zij het hebben gelezen; die bevestiging leggen wij vast in CMP-001 Competenties, training en bewustzijn;
- aan klanten, leveranciers en andere belanghebbenden die erom vragen; de beleidsverklaring hieronder mag openbaar worden gemaakt.

9. Gevolgen bij overtreding

Wie de regels van dit beleid bewust of herhaaldelijk overtreedt, kan disciplinaire maatregelen krijgen volgens de arbeidsvoorwaarden. Bij inhuurkrachten en leveranciers gelden de afspraken in het contract.

10. Beleidsverklaring

Voorbeeld IT B.V. beschermt de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie die klanten, medewerkers en partners ons toevertrouwen. Wij werken risicogestuurd, voldoen aan de eisen die op ons van toepassing zijn en verbeteren ons managementsysteem voor informatiebeveiliging voortdurend. Iedereen die voor ons werkt, draagt hieraan bij.

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de ISO 27001 Toolkit · alle 56 documenten: www.maasiso.nl/toolkits/iso-27001/

Naam	Functie	Datum	Handtekening
Mark Jansen	Algemeen directeur	1 november 2026	

11. Verwante documenten

Document	Titel
SCP-001	Toepassingsgebied
ISB-P01	Procedure risicomanagement
RSK-002	Risicoregister en behandelplan
ISB-001	Verklaring van toepasselijkheid
DST-002	Doelstellingen informatiebeveiliging
AFW-P01	Procedure afwijkingen en verbetering

© 2026 MaasISO — licentie [Licentienummer] voor [Licentiehouder] | maasiso.nl

Voorbeeld uit de ISO 27001 Toolkit · alle 56 documenten: www.maasiso.nl/toolkits/iso-27001/

VOORBEELD UIT DE TOOLKIT

Dit is 1 van de 56 documenten uit de ISO 27001 Toolkit

U hebt een echt document uit de toolkit bekeken, ingevuld voor een voorbeeldorganisatie. In de toolkit zit de volledige set, in Word en Excel, klaar om aan te passen aan uw organisatie.

Wat zit er verder in

Algemeen	5
Context van de organisatie	4
Leiderschap en beleid	2
Planning, risico's en doelstellingen	5
Ondersteuning	4
Uitvoering	19
Evaluatie	4
Verbetering	2
Formulieren	11

Prijs

- € 595 excl. btw (€ 719,95 incl. btw), eenmalig
- 12 maanden updates bij wijzigingen in de norm of wet
- 30 dagen geld terug, zonder opgaaf van reden
- Op naam van uw organisatie geleverd, direct na betaling te downloaden

Direct bestellen

Bekijk alle documenten en voorbeeldpagina's
www.maasiso.nl/toolkits/iso-27001/

Vragen over de inhoud? Mail info@maasiso.nl.