| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Voer hier de naam van de geregistreerde rechtspersoon in | | | | | | | |
| Documentnummer:<br>P03S | | | | | Documenttitel:<br>**Beleid inzake aanvaardbaar gebruik** | | | | | | | |
| 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 | Clausule 5 | Relevant voor de algemene reikwijdte en implementatie van het beleid |
| ISO/IEC 27002:2022 | 5.10, 5.11, 5 | Richtlijnen voor vereisten en beheersmaatregelen inzake aanvaardbaar gebruik |
| NIST SP 800-53 Rev.5 | AC-19, AC-20, AT-2 | Omvat systeem-/apparaatgebruik, monitoring en gebruikerstraining |
| AVG | Artikelen 5(1)(f), 32 | Integriteit en vertrouwelijkheid van gegevens en beveiligingsmaatregelen |
| NIS2-richtlijn | Artikel 21(2)(b) | Vereist passende beveiligingsbeleidslijnen, waaronder regels voor aanvaardbaar gebruik |
| DORA | Artikel 9 | Beleid voor ICT-risicobeheer, beheersmaatregelen en handhaving |
| COBIT 2019 | DSS05, BAI08 | Beveiligingsdiensten en kennisbeheer |

**1. Doel**

1.1. Dit beleid definieert het aanvaardbare, verantwoorde en veilige gebruik van door de onderneming verstrekte systemen, apparaten, internettoegang, e-mail, clouddiensten en alle privéapparaten die voor zakelijke doeleinden worden gebruikt.

1.2. Dit beleid waarborgt dat personen hun verplichtingen begrijpen bij het gebruik van IT-middelen van de organisatie, ter bescherming van gegevensintegriteit, privacy en operationele continuïteit.

1.3. Dit beleid ondersteunt de naleving van ISO/IEC 27001:2022 door duidelijke normen voor gebruikersgedrag af te dwingen, in lijn met wettelijke, contractuele en reglementaire vereisten.

**2. Reikwijdte**

**2.1. Dit beleid is van toepassing op alle personen die toegang hebben tot, beheer uitvoeren over of gebruikmaken van bedrijfssystemen of -gegevens, waaronder:**

2.1.1. werknemers en opdrachtnemers

2.1.2. tijdelijke medewerkers of stagiairs

2.1.3. externe IT-dienstverleners

**2.2. Dit beleid heeft betrekking op:**

2.2.1. computers, telefoons en tablets die eigendom zijn van de onderneming

2.2.2. privéapparaten die zijn goedgekeurd voor zakelijk gebruik (BYOD)

2.2.3. bedrijfsnetwerken, cloudplatforms en softwarediensten

2.2.4. internettoegang, e-mailsystemen, gedeelde opslag en zakelijke toepassingen

2.3. Dit beleid is van toepassing op alle werkomgevingen — op locatie, op afstand en hybride — en gedurende alle werkuren.

## 3. Doelstellingen

### 3.1. Vaststellen wat geldt als aanvaardbaar en onaanvaardbaar gebruik van IT-systemen.

3.1.1. Beveiligingsrisico's beperken die voortvloeien uit misbruik, ongeautoriseerde toegang of de introductie van malware.

3.1.2. Bedrijfsgegevens, klantinformatie en de reputatie van de onderneming beschermen.

3.1.3. Afdwingbare regels vaststellen en verantwoording door alle gebruikers mogelijk maken.

3.1.4. Monitoring en naleving ondersteunen om overtredingen vroegtijdig te detecteren en corrigerende maatregelen te nemen.

## 4. Rollen en verantwoordelijkheden

### 4.1. Algemeen directeur

4.1.1. Keurt dit beleid goed en is ervoor verantwoordelijk te waarborgen dat middelen en bevoegdheden voor handhaving beschikbaar zijn.

4.1.2. Beoordeelt en autoriseert eventuele uitzonderingen op dit beleid.

### 4.2. IT-manager of externe IT-dienstverlener

4.2.1. Beheert inventarissen van goedgekeurde software en hardware.

4.2.2. Configureert apparaten zodanig dat regels voor aanvaardbaar gebruik worden afgedwongen, bijvoorbeeld door middel van contentfiltering en toegangslogregistratie.

4.2.3. Monitort gebruik op mogelijke overtredingen en onderzoekt incidenten.

4.2.4. Waarborgt dat privéapparaten (BYOD) geautoriseerd en beveiligd zijn wanneer deze zakelijk worden gebruikt.

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

## 9. Vereisten voor herziening en actualisering

### 9.1. Jaarlijkse beoordeling

9.1.1. Dit beleid moet jaarlijks worden beoordeeld door de IT-manager, met definitieve goedkeuring door de algemeen directeur, om te waarborgen dat het in lijn blijft met patronen in technologiegebruik, opkomende risico's en nalevingsverplichtingen.

### 9.2. Triggers voor tussentijdse beoordeling

9.2.1. Beoordelingen moeten ook worden uitgevoerd naar aanleiding van:

9.2.2. nieuwe systemen of technologieën, zoals een nieuwe clouddienst of endpointplatform

9.2.3. significante beleidsovertredingen

9.2.4. gewijzigde wet- en regelgeving of contractvoorwaarden die van invloed zijn op IT-gebruik

### 9.3. Documentatie van wijzigingen

**9.3.1. Alle actualisaties moeten worden vastgelegd in een versielogboek dat ten minste het volgende bevat:**

9.3.1.1. versienummer

9.3.1.2. datum van beoordeling

9.3.1.3. samenvatting van wijzigingen

9.3.1.4. goedkeurende autoriteit

### 9.4. Beleidscommunicatie

9.4.1. Herziene versies van dit beleid moeten worden gedeeld met alle betrokken gebruikers. Werknemers moeten als onderdeel van hun verplichtingen inzake beveiligingsbewustzijn kennisnemen van ontvangst en begrip.

## 10. Gerelateerde beleidslijnen en samenhang

### 10.1. Dit beleid hangt samen met verschillende andere SME-beleidslijnen om volledige afdekking van beveiligingsverantwoordelijkheden te waarborgen:

10.1.1. P4S – Beleid inzake toegangsbeheersing: definieert de technische en procedurele afdwinging van toegestaan gebruik en accountbeperkingen.

10.1.2. P8S – Beleid inzake informatiebeveiligingsbewustzijn en opleiding: biedt gebruikersvoorlichting over grenzen van aanvaardbaar gebruik en meldverplichtingen.

10.1.3. P9S – Beleid inzake werken op afstand: reguleert het gebruik van bedrijfssystemen buiten de bedrijfslocatie of in de thuisomgeving.

10.1.4. P17S – Beleid inzake gegevensbescherming en privacy: handhaaft regels voor de verwerking van persoonsgegevens die samenhangen met monitoring van aanvaardbaar gebruik en BYOD.

10.1.5. P30S – Incidentresponsbeleid: regelt procedures voor het onderzoeken van en reageren op misbruik of overtredingen van regels voor aanvaardbaar gebruik.

## 11. Referentienormen en -kaders

### 11.1. ISO/IEC 27001

11.1.1. Clausule 5.10 – Vereist dat organisaties aanvaardbaar gebruik van informatie-activa definiëren en afdwingen.

### 11.2. ISO/IEC 27002

11.2.1. Beheersmaatregel 5.10 – Geeft richtlijnen voor aanvaardbaar gebruik van systemen, waaronder toegestane en verboden gedragingen.

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

11.3.1. AC-19 – Behandelt beheersing van systeemgebruik, waaronder privéapparaten.

11.3.2. AC-20 – Vereist autorisatie en monitoring van externe systemen.

11.3.3. AT-2 – Benadrukt het trainen van gebruikers in praktijken voor aanvaardbaar gebruik.

### 11.4. AVG

11.4.1. Artikel 5(1)(f) – Vereist integriteit en vertrouwelijkheid van persoonsgegevens, die in het gedrang kunnen komen door misbruik door gebruikers.

11.4.2. Artikel 32 – Verplicht de implementatie van technische en organisatorische maatregelen om systemen en gegevens te beveiligen.

### 11.5. NIS2-richtlijn

11.5.1. Artikel 21(2)(b) – Vereist passende beveiligingsbeleidslijnen, waaronder regels inzake aanvaardbaar gebruik, om cyberdreigingen te beperken.

### 11.6. DORA

11.6.1. Artikel 9 – Vereist beleidslijnen voor ICT-risicobeheer, waaronder gebruiksbeheersmaatregelen en handhavingsmechanismen.

### 11.7. COBIT 2019

11.7.1. DSS05 – Manage Security Services: benadrukt op beleid gebaseerde beheersing van gebruikersgedrag.

11.7.2. BAI08 – Manage Knowledge: behandelt bewustzijn van beleidsverantwoordelijkheden en voorlichting over aanvaardbaar gebruik.