					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P03					Documenttitel: **Beleid inzake aanvaardbaar gebruik**							
Versie: 1.0		Ingangsdatum: 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	Stelt gedragsnormen en vereisten vast voor het Beleid inzake aanvaardbaar gebruik
ISO/IEC 27002:2022	Beheersmaatregelen 6.1, 6.2, 8.1, 8.12	Geeft richting aan verantwoordelijkheden voor informatiebeveiliging, bewustwording en governance van apparaten en gegevens
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Toegangscontrole en bewustwordings- en gedragsmaatregelen die relevant zijn voor het gebruik van IT-bedrijfsmiddelen
AVG	Artikelen 5(1)(f), 32; overweging 39	Borgt vertrouwelijkheid en integriteit, verplicht technische en organisatorische maatregelen en vereist rechtsgronden voor rechtmatig gebruik
NIS2-richtlijn	Artikel 21(2)(a–d)	Verplicht operationele beleidslijnen en training inzake veilig gebruik
DORA	Artikel 5	Ondersteunt ICT-risicobeheer door gebruikersgedrag te reguleren
COBIT 2019	APO07, BAI05, DSS05, MEA01	Human resources, wijzigingsbeheer, beheerde beveiliging, monitoring van naleving en prestaties

1. Doel

1.1 Dit beleid definieert het aanvaardbare en niet-aanvaardbare gebruik van de informatiesystemen, IT-middelen, communicatiemiddelen en gegevensverwerkingspraktijken van de organisatie.

1.2 Het waarborgt dat alle gebruikers hun verantwoordelijkheden begrijpen bij het gebruik van IT-bedrijfsmiddelen en dat hun handelingen de vertrouwelijkheid, integriteit, beschikbaarheid en rechtmatige verwerking van informatie ondersteunen.

1.3 Dit beleid voldoet aan ISO/IEC 27001:2022, clausule 5.10, door gedragsnormen vast te stellen voor systeemgebruik en technische en procedurele waarborgen toe te passen om het risico op misbruik, nalatigheid of oneigenlijk gebruik te beperken.

1.4 Het beleid ondersteunt tevens onderzoeks- en handhavingsactiviteiten, waaronder incidentrespons en disciplinaire maatregelen bij overtredingen.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle personen en entiteiten aan wie toegang is verleend tot de informatiesystemen en bedrijfsmiddelen van de organisatie, met inbegrip van maar niet beperkt tot:

2.1.1 werknemers, opdrachtnemers, consultants, stagiairs en uitzendkrachten

2.1.2 externe leveranciers met systeemtoegang of gedelegeerde beheerdersrollen

2.1.3 gasten of partners die gebruikmaken van IT-infrastructuur die eigendom is van of geautoriseerd is door de organisatie

2.2 De reikwijdte omvat alle technologische middelen en gegevensactiva van de organisatie, waaronder:

2.2.1 werkplekken, laptops, mobiele apparaten en servers

2.2.2 netwerkinfrastructuur en in de cloud gehoste diensten

2.2.3 e-mail, berichtendiensten, bestandsopslag, samenwerkingsplatforms en VPN-verbindingen

2.2.4 gegevens in rust, tijdens transport of in verwerking, ongeacht formaat of locatie

2.2.5 elk persoonlijk apparaat dat wordt gebruikt onder een Bring Your Own Device (BYOD)-regeling en verbinding maakt met systemen van de organisatie

2.3 Dit beleid is afdwingbaar in alle werkomgevingen, waaronder:

2.3.1 bedrijfskantoren en productielocaties

2.3.2 locaties voor thuiswerken of hybride werkvormen

2.3.3 veldoperaties of locaties die door derden worden beheerd

2.4 Alle gebruikers moeten kennisnemen van en handelen in overeenstemming met dit beleid als voorwaarde voor toegang tot bedrijfssystemen of verwerking van bedrijfsgegevens.

3. Doelstellingen

3.1 Het definiëren en handhaven van regels voor het aanvaardbare gebruik van de IT-middelen van de organisatie.

3.2 Het voorkomen van ongeautoriseerde toegang, datalekken of schade als gevolg van nalatig of kwaadwillig gebruik.

3.3 Het beschermen van bedrijfsnetwerken, bedrijfsmiddelen en gegevens tegen dreigingen die via gebruikersgedrag worden geïntroduceerd.

3.4 Het ondersteunen van wettelijke en contractuele verplichtingen door zorgvuldigheid aan te tonen in de governance van IT-middelen.

3.5 Het waarborgen van consistentie en duidelijkheid bij de toepassing van disciplinaire maatregelen en processen voor uitzonderingsbeheer.

3.6 Het bevorderen van een cultuur van ethisch, veilig en verantwoord gebruik van digitale en fysieke computermiddelen.

4. Rollen en verantwoordelijkheden

4.1 Directie

4.1.1 Keurt het Beleid inzake aanvaardbaar gebruik (AUP) goed en zorgt ervoor dat het in lijn is met bedrijfsdoelstellingen, wettelijke en regelgevende vereisten en organisatiewaarden.

4.1.2 Wijst middelen toe voor handhaving, training, monitoring en beleidsevaluatie.

4.1.3 Beoordeelt de nalevingsstatus en disciplinaire maatregelen die samenhangen met beleidsovertredingen als onderdeel van de ISMS-governance.

4.2 IT- en informatiebeveiligingsteams

4.2.1 Implementeren technische waarborgen om dit beleid af te dwingen, waaronder:

4.2.2 contentfiltering, malwarebescherming, endpointbeveiliging en netwerkmonitoringtools

4.2.3 e-mailbeveiligingsconfiguraties en oplossingen voor preventie van gegevensverlies (DLP)

4.2.4 blokkeerlijsten en toelatingslijsten voor software, hardware en websites

4.2.5 Houden een inventaris bij van goedgekeurde en verboden software, apparaten en diensten.

4.2.6 Onderzoeken vermoedelijke overtredingen van het Beleid inzake aanvaardbaar gebruik (AUP), verzamelen forensisch bewijsmateriaal en ondersteunen waar passend disciplinaire of juridische maatregelen.

4.2.7 Werken samen met HR en Juridische Zaken en Compliance op het gebied van incidentafhandeling, escalatie en meldingsverplichtingen.

[... 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 actualisatie

9.1 Herzieningstriggers en frequentie

9.1.1 Dit beleid moet worden herzien:

9.1.1.1 ten minste jaarlijks

9.1.1.2 na significante wijzigingen in technologie of infrastructuur

9.1.1.3 na incidenten of auditbevindingen die hiaten in de handhaving aantonen

9.1.1.4 als reactie op wijzigingen in toepasselijke wet- en regelgeving of contracten

9.2 Eigenaarschap en goedkeuring

9.2.1 De CISO of aangewezen ISMS-manager is verantwoordelijk voor het herzieningsproces.

9.2.2 Actualisaties moeten door de directie worden goedgekeurd en organisatiebreed worden gecommuniceerd.

9.2.3 Kennisname van bijgewerkte bepalingen moet opnieuw worden vastgelegd bij heruitgifte van het beleid.

9.3 Documentbeheer

9.3.1 Het beleid moet de volgende metadata en versiegegevens bevatten:

9.3.1.1 titel, ID en classificatieniveau

9.3.1.2 beleidseigenaar en documentbeheerder

9.3.1.3 wijzigingshistorie en motivering voor actualisaties

9.3.1.4 datum van herziening en volgende geplande actualisatiedatum

9.3.1.5 verwijzingen naar distributie- en kennisnamelogboeken

9.3.2 Het masterexemplaar moet onder versiebeheer worden bewaard in de documentrepository van het ISMS.

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid moet worden geïnterpreteerd in samenhang met de volgende beleidslijnen:

10.1.1 P1 – Informatiebeveiligingsbeleid: Stelt de basisverwachtingen voor gedrag en de betrokkenheid van de directie bij aanvaardbaar gebruik vast.

10.1.2 P4 – Beleid inzake toegangscontrole: Definieert machtigingen en rechten die samenhangen met toegang van gebruikers, systemen en gegevens en handhaaft daarmee rechtstreeks de grenzen van aanvaardbaar gebruik.

10.1.3 P6 – Risicobeheerbeleid: Behandelt gedragsgerelateerde risico's en ondersteunt monitoring- en beheersactiviteiten die verband houden met door gebruikers veroorzaakte dreigingen.

10.1.4 P7 – Onboarding- en offboardingbeleid: Zorgt ervoor dat voorwaarden voor aanvaardbaar gebruik bij indiensttreding worden bevestigd en bij uitdiensttreding worden ingetrokken.

10.1.5 P9 – Beleid inzake werken op afstand: Breidt bepalingen voor aanvaardbaar gebruik uit naar werkomgevingen op afstand en hybride werkomgevingen.

10.2 Deze gerelateerde beleidslijnen vormen samen een gelaagd verdedigingsmodel voor gedragsmatige, technische en contractuele governance.

11. Referentienormen en -raamwerken

11.1 Dit Beleid inzake aanvaardbaar gebruik (AUP) is afgestemd op internationaal erkende normen en juridische kaders om afdwingbare, auditeerbare en risicogebaseerde gedragsmaatregelen te waarborgen voor elk gebruik van digitale en fysieke informatiesystemen.

11.2 ISO/IEC 27001:2022

11.2.1 Clausule 5.10 – Aanvaardbaar gebruik van informatie en andere gerelateerde activa: Dit beleid voldoet rechtstreeks aan de eis om regels te definiëren, te communiceren en te handhaven voor passend gebruik van IT-middelen.

11.2.2 Bijlage A, beheersmaatregel 6.1 – Verantwoordelijkheid voor informatiebeveiliging: Wijst duidelijke verantwoordelijkheden toe voor gebruikersgedrag en toezicht op naleving.

11.2.3 Bijlage A, beheersmaatregel 6.2 – Bewustwording, opleiding en training op het gebied van informatiebeveiliging: Ingebedde trainings- en beleidskennisnameprocessen maken deel uit van de handhaving van het Beleid inzake aanvaardbaar gebruik (AUP).

11.2.4 Bijlage A, beheersmaatregel 8.1 – Eindgebruikersapparaten en 8.12 – Preventie van gegevensverlies (DLP): Behandelt aanvaardbaar gedrag op gebruikersapparaten en stuurt activiteiten aan die kunnen leiden tot blootstelling of lekkage van gegevens.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (Toegangscontrole voor mobiele apparaten) en AC-20 (Gebruik van externe informatiesystemen): Dit beleid definieert verplichtingen en beperkingen voor gebruikers ten aanzien van BYOD en toegang tot systemen van derden.

11.3.2 PL-4 (Gedragsregels): Biedt gedetailleerde vereisten voor aanvaardbaar gebruik die in overeenstemming zijn met dit beleid.

11.3.3 AT-2 (Beveiligingsbewustzijnstraining): Ondersteund door gebruikerstraining en gedocumenteerde beleidskennisname.

11.3.4 AU-2 (Auditgebeurtenissen) en AU-12 (Auditgeneratie): Handhaving is afhankelijk van het monitoren van gebruikershandelingen en het genereren van waarschuwingen bij overtredingen.

11.4 AVG (Verordening (EU) 2016/679):

11.4.1 Artikel 5(1)(f): Vereist de beveiliging en integriteit van persoonsgegevens; dit beleid beperkt risico's die voortkomen uit menselijk gedrag en ongeautoriseerd gebruik.

11.4.2 Artikel 32: Verplicht technische en organisatorische maatregelen, zoals gedragsmaatregelen en gebruiksbeperkingen, ter bescherming van persoonsgegevens.

11.4.3 Overweging 39: Benadrukt de noodzaak om te waarborgen dat alleen noodzakelijke toegang en rechtmatig gebruik van gegevens plaatsvinden door geautoriseerde personen.

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

11.5.1 Artikel 21(2)(a–d): Vereist operationele beleidslijnen en training voor veilig systeemgebruik, waarin dit Beleid inzake aanvaardbaar gebruik (AUP) voorziet door gedrag, monitoring en handhavingsprocessen te definiëren.

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

11.6.1 Artikel 5: Dit beleid ondersteunt het ICT-risicobeheerkader door regels vast te stellen voor de interactie tussen mens en systeem en de aan gedrag gerelateerde blootstelling aan cyberrisico's te beperken.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources: Borgt gebruikersverantwoordelijkheden en bewustwording gedurende de gehele levenscyclus van werknemers.

11.7.2 BAI05 – Managed Organizational Change: Verankert governance voor aanvaardbaar gebruik in wijzigingsprocessen die van invloed zijn op gebruikersgedrag.

11.7.3 DSS05 – Managed Security Services: Ondersteunt monitoring van gebruikersactiviteiten, gedragswaarschuwingen en geautomatiseerde responsmechanismen.

11.7.4 MEA01 – Monitor, Evaluate, and Assess Performance and Conformance: Het beleid definieert meetpunten en mechanismen om te valideren of gebruikers voldoen aan gedragsverwachtingen.