					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P21					Documenttitel: **Netwerkbeveiligingsbeleid**							
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 8	N.v.t.
ISO/IEC 27002:2022	Beheersmaatregelen 8.20-8.22	N.v.t.
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N.v.t.
AVG	Artikel 32	N.v.t.
EU NIS2	Artikel 21(2)(d)	N.v.t.
EU DORA	Artikel 9	N.v.t.
COBIT 2019	DSS01.03, DSS05.01, MEA03	N.v.t.

1. Doel

1.1 Het doel van dit beleid is het vaststellen van de vereisten van de organisatie voor de bescherming van haar interne en externe netwerken tegen ongeautoriseerde toegang, verstoring van dienstverlening, onderschepping van gegevens en misbruik.

1.2 Dit beleid waarborgt dat alle netwerkinfrastructuur, waaronder fysieke, virtuele, cloudgehoste en hybride omgevingen, wordt beschermd door gelaagde beheersmaatregelen zoals segmentatie, firewallafdwinging, veilige routering en gecentraliseerde monitoring.

1.3 Dit beleid geeft uitvoering aan ISO/IEC 27001, clausule 8.1, en bijlage A-beheersmaatregelen 8.20 tot en met 8.22, en borgt naleving van toepasselijke wettelijke en regelgevende verplichtingen op grond van de AVG, artikel 32, NIS2, artikel 21, en DORA, artikel 9.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle netwerken en gerelateerde infrastructuurcomponenten, waaronder:

2.1.1 routers, switches, draadloze toegangspunten en firewalls

2.1.2 virtuele cloudnetwerken (bijvoorbeeld AWS VPC en Azure VNet), VPN-concentrators en SD-WAN-systemen

2.1.3 interne LAN's, gedemilitariseerde zones (DMZ's), voorzieningen voor externe toegang en verbindingen tussen locaties of met derden

2.1.4 ondersteunende systemen zoals DNS, DHCP, proxyservers en monitoringsystemen

2.2 Dit beleid is bindend voor alle medewerkers en externe dienstverleners die netwerken van de organisatie beheren, configureren, monitoren of daarmee koppelen, ongeacht of deze zich on-premises of in de cloud bevinden.

2.3 Alle systemen en toepassingen die zijn verbonden met de netwerken van de organisatie, ongeacht locatie of eigenaarschap, moeten voldoen aan deze vereisten inzake netwerkbeveiliging.

3. Doelstellingen

3.1 De vertrouwelijkheid, integriteit en beschikbaarheid (CIA) van gegevens die via netwerken worden verzonden waarborgen door middel van sterke toegangscontroles, veilige routering en monitoring.

3.2 Ongeautoriseerde toegang, laterale verplaatsing en misbruik van netwerkgebonden middelen voorkomen door segmentatie, zonering en grensbeveiliging af te dwingen.

3.3 Consistente netwerkconfiguraties handhaven op basis van industrienormen en threat intelligence om bescherming te bieden tegen zich ontwikkelende cyberdreigingen.

3.4 Externe communicatie, cloudconnectiviteit en externe toegang (VPN, beheer van mobiele apparaten) beveiligen met versleutelde kanalen, strikte authenticatie en validatie van eindpunten.

3.5 Zicht bieden op netwerkactiviteit door middel van gecentraliseerde logging, realtime inspectie van netwerkverkeer en geautomatiseerde waarschuwingen.

3.6 Naleving van regelgeving waarborgen door alle netwerkactiviteiten af te stemmen op de vereisten van ISO/IEC 27001:2022, de AVG, NIS2, DORA en COBIT 2019.

4. Rollen en verantwoordelijkheden

4.1 Chief Information Security Officer (CISO)

4.1.1 Is eigenaar van dit beleid en waarborgt dat het wordt herzien en afgestemd op de bredere cyberbeveiligingsstrategie van de organisatie.

4.1.2 Keurt netwerksegmentatiemodellen, firewallregelsets voor gevoelige systemen en uitzonderingsverzoeken goed.

4.2 Manager Netwerkbeveiliging / Verantwoordelijke Infrastructuurbeveiliging

4.2.1 Beheert de architectuur voor netwerkverdediging, waaronder firewalls, systemen voor inbraakdetectie en -preventie (IDS/IPS), VPN's en veilige routering.

4.2.2 Houdt toezicht op netwerksegmentatie, VLAN-toewijzingen, verkeerszonering en externe connectiviteit.

4.2.3 Waarborgt de doorlopende beoordeling van filtering van inkomend en uitgaand verkeer en de afdwinging van zero-trustprincipes over alle netwerksegmenten heen.

[... 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 jaarlijks worden herzien door de Manager Netwerkbeveiliging in samenwerking met de CISO en worden bijgewerkt op basis van:

9.1.1 opkomende dreigingen (zoals nieuwe aanvalstechnieken en protocolkwetsbaarheden)

9.1.2 wijzigingen in de infrastructuur (zoals migraties naar cloudgehoste systemen en uitrol van SD-WAN)

9.1.3 wijzigingen in wet- en regelgeving of normen die van invloed zijn op netwerkbeveiliging

9.1.4 auditbevindingen, incidenttrends of prestatievermindering veroorzaakt door beheersmaatregelen

9.2 Herzieningen moeten ook worden getriggerd door:

9.2.1 majeure wijzigingen in de netwerkarchitectuur

9.2.2 implementatie van nieuwe firewall-, VPN- of cloudnetwerkplatforms

9.2.3 buitengebruikstelling van kritieke activa of vertrouwde zones

9.3 Bijwerkingen moeten worden vastgelegd in het ISMS-documentbeheerregister en worden gecommuniceerd aan:

9.3.1 infrastructuur- en netwerkoperatie

9.3.2 SOC- en security-engineeringteams

9.3.3 applicatieteams met systeemafhankelijkheden van netwerkstromen

9.3.4 alle externe leveranciers met actieve interconnectiviteit

9.4 Alle eerdere versies van dit beleid moeten veilig worden gearchiveerd met annotaties van de wijzigingshistorie om auditeerbaarheid en traceerbaarheid van wijzigingen te behouden.

10. Gerelateerde beleidslijnen en samenhang

10.1 P1 - Informatiebeveiligingsbeleid. Stelt de fundamentele beveiligingsprincipes vast en schrijft gelaagde bescherming voor, waaronder netwerkgebaseerde toegangs- en dreigingsbeheersmaatregelen.

10.2 P4 - Beleid inzake toegangscontrole. Waarborgt dat netwerksegmentatie wordt afgedwongen in overeenstemming met gebruikersrollen, het beginsel van minimale bevoegdheden en regels voor toekenning van toegangsrechten.

10.3 P5 - Wijzigingsbeheerbeleid. Regelt firewallwijzigingen, aanpassingen van VPN-regels en routeringswijzigingen via een gedocumenteerd en auditeerbaar proces.

10.4 P12 - Beleid inzake beheer van bedrijfsmiddelen. Ondersteunt de identificatie en classificatie van systemen die met het netwerk zijn verbonden en waarborgt dat alle verbonden bedrijfsmiddelen worden beheerd binnen de beleidsmatig vastgestelde reikwijdte.

10.5 P22 - Logging- en monitoringbeleid. Regelt de verzameling, correlatie en bewaring van netwerklogboeken, waaronder firewallgebeurtenissen, toegangspogingen en gedetecteerde afwijkingen.

10.6 P30 - Incidentresponsbeleid. Beschrijft de procedures voor escalatie, indamming en uitroeiing in reactie op netwerkgedragen dreigingen of inbreuken, zoals DDoS, laterale verplaatsing of ongeautoriseerde toegang.

11. Referentienormen en -raamwerken

11.1 Dit beleid is afgestemd op internationale normen en regelgevende verplichtingen die veilige netwerkoperaties, segmentatie, perimeterbeveiliging en veilige externe toegang voorschrijven.

11.2 ISO/IEC 27001

11.2.1 Clausule 8.1 - Operationele planning en beheersing: vereist dat technische beheersmaatregelen, waaronder maatregelen voor netwerkbeveiliging, in operationele processen zijn ingebed.

11.3 ISO/IEC 27002:2022

11.3.1 Beheersmaatregelen 8.20-8.22: bieden richtsnoeren voor het beschermen van netwerken, het segmenteren van diensten en het beveiligen van netwerkdiensten door middel van toegangscontroles en monitoring.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Grensbeveiliging: vereist perimeterbeheersmaatregelen, segmentatie en veilige interconnecties.

11.4.2 AC-4 - Afdwinging van informatiestromen: ondersteunt zonering en op regels gebaseerde beperkingen op netwerkverkeer.

11.4.3 SC-32 - Partitionering van informatiesystemen: bevordert logische scheiding van informatiesystemen.

11.5 AVG

11.5.1 Artikel 32 - Beveiliging van de verwerking: vereist technische maatregelen, zoals firewalls en segmentatie, ter bescherming van persoonsgegevens.

11.6 EU NIS2-richtlijn (2022/2555)

11.6.1 Artikel 21(2)(d): vereist doeltreffende beveiliging van netwerk- en informatiesystemen, perimeterbeveiliging, veilige configuratie en scheidingsmaatregelen.

11.7 EU DORA (2022/2554)

11.7.1 Artikel 9 - ICT-risicobeheer: verplicht financiële entiteiten om netwerken en interconnecties te beschermen tegen ongeautoriseerde toegang, datalekken en operationele verstoringen.

11.8 COBIT 2019

11.8.1 DSS01.03 - Infrastructuur monitoren: vereist proactieve beheersing van de gezondheid en connectiviteit van het netwerk.

11.8.2 DSS05.01 - Beschermen tegen malware: omvat segmentatie en grensbeheersing om verspreiding te minimaliseren.

11.8.3 MEA03 - Naleving monitoren, evalueren en beoordelen: versterkt de handhaving van netwerkbeleid en nalevingsbeoordelingen.