					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P21S					Documenttitel: **Netwerkbeveiligingsbeleid - MKB**							
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	-
ISO/IEC 27002:2022	Beheersmaatregel 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
AVG	Artikel 32	-
EU NIS2	Artikelen 21(2)(d), (e)	-
EU DORA	Artikelen 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Doel

1.1. Het doel van dit beleid is te waarborgen dat alle interne en externe netwerkcommunicatie door duidelijk gedefinieerde beveiligingsmaatregelen wordt beschermd tegen ongeautoriseerde toegang, manipulatie, afluisteren en misbruik.

1.2. Dit beleid stelt regels vast voor het veilige ontwerp, gebruik en beheer van de netwerkinfrastructuur, waaronder routers, draadloze toegangspunten, externe toegangsverbindingen en gesegmenteerde netwerken.

1.3. Dit beleid heeft tot doel de blootstelling aan internetgerelateerde dreigingen te minimaliseren, de vertrouwelijkheid van gegevens die via interne en externe netwerken worden verzonden te waarborgen en de beschikbaarheid van kritieke diensten te handhaven.

1.4. Dit beleid ondersteunt certificering volgens ISO/IEC 27001:2022 en draagt rechtstreeks bij aan de naleving van wettelijke en reglementaire verplichtingen onder de AVG, NIS2 en DORA, en biedt tegelijkertijd technische assurance aan klanten en auditors.

2. Reikwijdte

2.1. Dit beleid is van toepassing op alle componenten van het IT-netwerk van de organisatie, waaronder:

2.1.1. Bekabelde en draadloze infrastructuur op kantoorlocaties

2.1.2. Routers, switches, toegangspunten, firewalls en gateways

2.1.3. Verbindingen voor externe toegang, waaronder VPN, beheer van mobiele apparaten, RDP en cloudtunnels

2.1.4. Cloudgebaseerde toepassingen die via interne of externe netwerken worden benaderd

2.1.5. Apparaten die door werknemers, opdrachtnemers of gasten met het netwerk zijn verbonden

2.2. Dit beleid is van toepassing op zowel fysieke als logische netwerksegmenten, waaronder gastzones, Internet of Things (IoT)-apparaten en backoffice-systemen.

2.3. Dit beleid geldt voor al het personeel met toegang tot het netwerk van de organisatie, waaronder:

2.3.1. Interne medewerkers

2.3.2. Medewerkers die op afstand werken en hybride medewerkers

2.3.3. Externe leveranciers, consultants en dienstverleners

2.3.4. Gasten die tijdelijk gebruikmaken van wifi-toegang

3. Doelstellingen

3.1. Waarborgen dat het netwerk van de organisatie is beschermd tegen ongeautoriseerde toegang en externe cyberdreigingen

3.2. Correcte segmentatie afdwingen tussen vertrouwde en niet-vertrouwde netwerken, zoals gastwifi en toegang door leveranciers

3.3. Veilige externe connectiviteit mogelijk maken zonder interne systemen in gevaar te brengen

3.4. De verspreiding van malware en data-exfiltratie via netwerkkanalen voorkomen

3.5. Monitoring, waarschuwingen en audits van netwerkactiviteit mogelijk maken ter ondersteuning van incidentdetectie, escalatie en naleving

3.6. Waarborgen dat uitsluitend goedgekeurde en beveiligde apparaten verbinding mogen maken met interne netwerken

3.7. Voldoen aan verplichtingen onder ISO 27001, de AVG en gerelateerde cybersecuritykaders

4. Rollen en verantwoordelijkheden

4.1. Algemeen directeur

4.1.1. Is eigenaar van dit beleid en zorgt ervoor dat passende middelen worden toegewezen voor een veilig netwerkontwerp en adequaat netwerkbeheer

4.1.2. Beoordeelt uitzonderingen op netwerkbeveiligingsmaatregelen en keurt overeenkomsten voor netwerktoegang door leveranciers goed

4.1.3. Beoordeelt incidenten of auditbevindingen met betrekking tot kwetsbaarheden in de netwerkbeveiliging

4.2. IT-dienstverlener / interne IT-verantwoordelijke

4.2.1. Implementeert, configureert en onderhoudt alle firewalls, routers, switches en draadloze controllers

4.2.2. Beheert de segmentatie tussen interne, gast- en externe netwerken

4.2.3. Beoordeelt logboeken en waarschuwingen op pogingen tot ongeautoriseerde toegang of netwerkanomalieën

4.2.4. Zorgt ervoor dat firmware- en configuratie-updates veilig en tijdig worden doorgevoerd

[... 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 ten minste jaarlijks worden beoordeeld door de algemeen directeur, samen met de IT-dienstverlener en de privacycoördinator.

9.2. Triggers voor tussentijdse beoordeling

9.2.1. Een beleidsbeoordeling moet ook worden gestart door:

9.2.1.1. Ingrijpende wijzigingen in de netwerkarchitectuur, zoals nieuwe VPN- of firewallsystemen

9.2.1.2. Een netwerkgerelateerd incident, zoals een inbraak, verspreiding van ransomware of data-exfiltratie

9.2.1.3. Wijzigingen in wetgeving, regelgeving of kaders die netwerkbescherming raken

9.2.1.4. Nieuwe leveranciersplatforms waarvoor alternatieve toegangsmethoden of protocollen nodig zijn

9.3. Versiebeheer en documentatie

9.3.1. Herzieningen van het beleid moeten worden geregistreerd met een versienummer, datum en samenvatting van de wijzigingen

9.3.2. Vorige versies moeten ten minste 3 jaar worden gearchiveerd

9.3.3. Updates moeten worden gecommuniceerd aan betrokken medewerkers, met verplichte beleidskennisname indien significante gedragswijzigingen worden ingevoerd

10. Gerelateerde beleidslijnen en samenhang

10.1. Dit beleid moet samen met de volgende mkb-beveiligingsbeleidslijnen worden geïmplementeerd:

10.1.1. P9S – Beleid inzake werken op afstand: stelt veilige methoden voor externe toegang, VPN-vereisten en endpointbeveiliging vast voor gebruikers buiten de locatie.

10.1.2. P12S – Beleid inzake bedrijfsmiddelenbeheer: waarborgt dat alle met het netwerk verbonden systemen worden geïdentificeerd, gecategoriseerd en gevolgd met een actuele beveiligingsstatus.

10.1.3. P17S – Beleid inzake gegevensbescherming en privacy: waarborgt dat netwerksegmentatie, toegangsbeheersmaatregelen en logging de privacy- en gegevensbeschermingsprincipes onder de AVG ondersteunen.

10.1.4. P22S – Logging- en monitoringbeleid: specificeert vereisten voor het vastleggen en beoordelen van logboeken van netwerkapparatuur, externe verbindingen en draadloze controllers.

10.1.5. P30S – Incidentresponsbeleid: definieert vereiste acties in reactie op netwerkinbreuken, pogingen tot ongeautoriseerde toegang of verspreiding van malware via interne netwerken.

11. Referentienormen en -kaders

11.1. ISO/IEC 27001

11.1.1. Clausule 8.1 – Vereist de implementatie van beheersmaatregelen om veilige en weerbare operationele processen, waaronder netwerken, te waarborgen.

11.2. ISO/IEC 27002

11.2.1. Beheersmaatregel 8.20 – Biedt technische en procedurele richtlijnen voor het beveiligen van netwerktoegang, segmentatie en monitoring.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Verplicht beheersing van informatiestromen binnen netwerken en tussen systemen.

11.3.2. SC-7 – Vereist grensbeveiliging, veilige routering en netwerksegmentatie om het risico op ongeautoriseerde toegang te verminderen.

11.4. AVG

11.4.1. Artikel 32 – Vereist passende technische en organisatorische maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid te waarborgen van netwerkgebonden systemen en diensten die persoonsgegevens verwerken.

11.5. EU NIS2-richtlijn

11.5.1. Artikel 21(2)(d) – Verplicht risicogebaseerde technische maatregelen, waaronder netwerkbeveiliging en toegangscontrole.

11.5.2. Artikel 21(2)(e) – Vereist systeemsegmentatie en isolatie om te voorkomen dat cyberincidenten zich verspreiden.

11.6. EU DORA

11.6.1. Artikel 9 – Vereist dat organisaties beheersmaatregelen voor ICT-risicobeheer implementeren, waaronder maatregelen voor veilige netwerken en communicatie.

11.6.2. Artikel 10 – Vereist dat strategieën voor digitale weerbaarheid bescherming van netwerkinfrastructuur en externe connectiviteit omvatten.

11.7. COBIT 2019

11.7.1. DSS05.02 – Vereist doeltreffende bescherming van IT-infrastructuur en netwerkomgevingen tegen interne en externe dreigingen.

11.7.2. APO13.01 – Vereist risicobeheerstrategieën die netwerksegmentatie en monitoring omvatten als onderdeel van dreigingsmitigatie.