					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P21					Dokumenttitel: **Nätverkssäkerhetspolicy**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Anpassning till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Ej tillämpligt
ISO/IEC 27002:2022	Kontroller 8.20–8.22	Ej tillämpligt
NIST SP 800-53 Rev. 5	SC-7, AC-4, SC-32	Ej tillämpligt
EU:s dataskyddsförordning (GDPR)	Artikel 32	Ej tillämpligt
EU:s NIS2-direktiv	Artikel 21.2 d	Ej tillämpligt
EU:s DORA-förordning	Artikel 9	Ej tillämpligt
COBIT 2019	DSS01.03, DSS05.01, MEA	Ej tillämpligt

1. Syfte

1.1 Syftet med denna policy är att fastställa organisationens krav för att skydda interna och externa nätverk mot obehörig åtkomst, tjänsteavbrott, avlyssning av data och missbruk.

1.2 Policyn säkerställer att all nätverksinfrastruktur, inklusive fysisk, virtuell, molnbaserad och hybrid infrastruktur, skyddas genom lagerindelade säkerhetskontroller såsom segmentering, brandväggsstyrning, säker routning och centraliserad övervakning.

1.3 Denna policy omsätter kraven i ISO/IEC 27001 klausul 8.1 och Annex A-kontrollerna 8.20 till 8.22 samt säkerställer efterlevnad av tillämpliga rättsliga och regulatoriska skyldigheter enligt artikel 32 i EU:s dataskyddsförordning (GDPR), artikel 21 i EU:s NIS2-direktiv och artikel 9 i EU:s DORA-förordning.

2. Omfattning

2.1 Denna policy gäller för alla nätverk och tillhörande infrastrukturkomponenter, inklusive:

2.1.1 Routrar, switchar, trådlösa accesspunkter och brandväggar

2.1.2 Virtuella molnnätverk (t.ex. AWS VPC, Azure VNET), VPN-koncentratorer och SD-WAN-system

2.1.3 Interna LAN, demilitariserade zoner (DMZ), fjärråtkomstvägar samt förbindelser mellan platser eller med tredje part

2.1.4 Stödsystem såsom DNS, DHCP, proxyservrar och övervakningsutrustning

2.2 Policyn är bindande för all personal och tredjepartsleverantörer som hanterar, konfigurerar, övervakar eller ansluter till organisationens nätverk, oavsett om detta sker lokalt eller i molnmiljö.

2.3 Alla system och applikationer som är anslutna till organisationens nätverk, oavsett plats eller ägarskap, ska uppfylla dessa krav på nätverkssäkerhet.

3. Mål

3.1 Säkerställa konfidentialitet, riktighet och tillgänglighet för data som överförs över nätverk genom starka åtkomstkontroller, säker routning och övervakning.

3.2 Förhindra obehörig åtkomst, lateral förflyttning och utnyttjande av nätverksanslutna resurser genom att upprätthålla segmentering, zonindelning och gränsskydd.

3.3 Upprätthålla enhetliga nätverkskonfigurationer baserade på vedertagen branschpraxis och hotinformation för att skydda mot föränderliga cyberhot.

3.4 Skydda extern kommunikation, molnsammankopplingar och fjärråtkomst med krypterade kanaler, stark autentisering och validering av slutpunkter.

3.5 Ge insyn i nätverksaktivitet genom centraliserad loggning, trafikinspektion i realtid och automatiserade larm.

3.6 Säkerställa regelefterlevnad genom att anpassa all nätverksdrift till kraven i ISO/IEC 27001:2022, EU:s dataskyddsförordning (GDPR), EU:s NIS2-direktiv, EU:s DORA-förordning och COBIT 2019.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 Är policyägare för denna policy och säkerställer att den granskas och är anpassad till organisationens övergripande cybersäkerhetsstrategi.

4.1.2 Godkänner modeller för nätverkssegmentering, brandväggsregelverk för känsliga system och undantagsbegäranden.

4.2 Chef för nätverkssäkerhet/infrastruktursäkerhetsansvarig

4.2.1 Ansvarar för arkitekturen för nätverksförsvar, inklusive brandväggar, system för intrångsdetektering och intrångsskydd (IDS/IPS), VPN och säker routning.

4.2.2 Ansvarar för nätverkssegmentering, tilldelning av VLAN, trafikzonindelning och extern anslutning.

4.2.3 Säkerställer löpande granskning av filtrering för inkommande och utgående trafik samt tillämpning av zero trust över nätverkets olika lager.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1 Denna policy ska granskas årligen av chef för nätverkssäkerhet i samarbete med informationssäkerhetschef (CISO) och uppdateras baserat på:

9.1.1 Framväxande hot, exempelvis nya angreppstekniker och protokollsårbarheter

9.1.2 Förändringar i infrastrukturen, exempelvis migrering till molnmiljö och införande av SD-WAN

9.1.3 Regulatoriska uppdateringar eller ändringar i standarder som påverkar skyddet av nätverk

9.1.4 Revisionsiakttagelser, incidenttrender eller prestandaförsämringar som orsakas av kontroller

9.2 Granskningar ska även utlösas av:

9.2.1 Större förändringar i nätverksarkitekturen

9.2.2 Införande av nya plattformar för brandväggar, VPN eller molnnätverk

9.2.3 Avveckling av centrala tillgångar eller betrodda zoner

9.3 Uppdateringar ska loggas i ISMS-dokumentregistret för styrning och kommuniceras till:

9.3.1 Infrastruktur- och nätverksdrift

9.3.2 SOC och säkerhetsarkitekturteam

9.3.3 Applikationsteam med systemberoenden till nätverksflöden

9.3.4 Alla tredjepartsleverantörer med aktiv sammankoppling

9.4 Alla tidigare versioner av policyn ska arkiveras säkert med ändringshistorik för att bevara revisionsbarhet och spårbarhet.

10. Relaterade policyer och kopplingar

10.1 P1 - Informationssäkerhetspolicy. Fastställer grundläggande säkerhetsprinciper och kräver lagerindelade skyddsåtgärder, inklusive nätverksbaserade kontroller för åtkomst och hot.

10.2 P4 - Åtkomstkontrollpolicy. Säkerställer att nätverkssegmentering upprätthålls i linje med användarroller, principen om minsta privilegium och regler för åtkomsttilldelning.

10.3 P5 - Ändringshanteringspolicy. Reglerar ändringar i brandväggar, justeringar av VPN-regler och routningsändringar genom en dokumenterad och granskningsbar process.

10.4 P12 - Policy för tillgångshantering. Stödjer identifiering och klassificering av nätverksanslutna system och säkerställer att alla anslutna tillgångar hanteras inom policydefinierade ramar.

10.5 P22 - Loggnings- och övervakningspolicy. Reglerar insamling, korrelation och bevarande av nätverksloggar, inklusive brandväggshändelser, åtkomstförsök och avvikelsedetektering.

10.6 P30 - Policy för incidenthantering. Definierar rutiner för eskalering, begränsning och eliminering som svar på nätverksburna hot eller intrång, såsom DDoS, lateral förflyttning eller obehörig åtkomst.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till internationella standarder och regulatoriska krav som definierar säker nätverksdrift, segmentering, perimeterskydd och säker fjärråtkomst.

11.2 ISO/IEC 27001

11.2.1 Klausul 8.1 - Operativ planering och styrning: Kräver att tekniska kontroller, inklusive skyddsåtgärder för nätverk, integreras i operativa processer.

11.3 ISO/IEC 27002:2022

11.3.1 Kontroller 8.20–8.22: Ger vägledning om skydd av nätverk, segmentering av tjänster och skydd av nätverkstjänster genom åtkomstkontroller och övervakning.

11.4 NIST SP 800-53 Rev. 5

11.4.1 SC-7 - Boundary Protection: Kräver perimeterkontroller, segmentering och säkra sammankopplingar.

11.4.2 AC-4 - Information Flow Enforcement: Stödjer zonindelning och regelbaserade trafikbegränsningar.

11.4.3 SC-32 - Information System Partitioning: Främjar logisk separation av informationssystem.

11.5 EU:s dataskyddsförordning (GDPR) (2016/679)

11.5.1 Artikel 32 - Säkerhet i behandlingen: Kräver tekniska åtgärder, såsom brandväggar och segmentering, för att skydda personuppgifter.

11.6 EU:s NIS2-direktiv (2022/2555)

11.6.1 Artikel 21.2 d: Kräver effektiv säkerhet för nätverks- och informationssystem, perimeterskydd, säker konfiguration och separationskontroller.

11.7 EU:s DORA-förordning (2022/2554)

11.7.1 Artikel 9 - IKT-riskhantering: Ålägger finansiella entiteter att skydda nätverk och sammankopplingar mot obehörig åtkomst, dataläckage och operativa störningar.

11.8 COBIT 2019

11.8.1 DSS01.03 - Övervaka infrastruktur: Kräver proaktiv kontroll över nätverkshälsa och anslutningsförmåga.

11.8.2 DSS05.01 - Skydda mot skadlig kod: Innefattar segmentering och gränsskydd för att minimera spridning.

11.8.3 MEA03 - Övervaka, utvärdera och bedöm efterlevnad: Förstärker tillämpningen av nätverkspolicyn och bedömningar av efterlevnad.