					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P21					Dokumenttitel: **Politik for netværkssikkerhed**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Juridisk meddelelse (ophavsret og brugsbegrænsninger)

(C) 2025 Clarysec LLC. All rights reserved.

Dette dokument er Clarysec LLC's intellektuelle ejendom. Ingen del af dette dokument må kopieres, genbruges, distribueres eller ændres til kommercielle eller implementeringsmæssige formål uden udtrykkelig skriftlig tilladelse.
Uautoriseret brug er strengt forbudt og kan medføre retslige skridt.
For licensiering kontakt: info@clarysec.com

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	N/A
ISO/IEC 27002:2022	Kontroller 8.20-8.22	N/A
NIST SP 800-53 Rev.5	SC-7, AC-4, SC-32	N/A
EU GDPR	Artikel 32	N/A
EU NIS2	Artikel 21(2)(d)	N/A
EU DORA	Artikel 9	N/A
COBIT 2019	DSS01.03, DSS05.01, MEA03	N/A

1. Formål

1.1 Formålet med denne politik er at fastlægge organisationens krav til beskyttelse af interne og eksterne netværk mod uautoriseret adgang, driftsafbrydelser, aflytning af data og misbrug.

1.2 Politikken skal sikre, at al netværksinfrastruktur, herunder fysisk, virtuel, cloudbaseret og hybrid infrastruktur, beskyttes gennem lagdelte kontroller såsom netværkssegmentering, håndhævelse af firewallregler, sikker routing og centraliseret overvågning.

1.3 Denne politik understøtter ISO/IEC 27001 klausul 8.1 og Annex A-kontrollerne 8.20 til 8.22 samt sikrer overholdelse af gældende juridiske og regulatoriske forpligtelser i henhold til GDPR artikel 32, NIS2 artikel 21 og DORA artikel 9.

2. Omfang

2.1 Denne politik gælder for alle netværk og tilknyttede infrastrukturkomponenter, herunder:

2.1.1 Routere, switche, trådløse adgangspunkter og firewalls

2.1.2 Cloudbaserede virtuelle netværk (f.eks. AWS VPC, Azure VNet), VPN-koncentratorer og SD-WAN-løsninger

2.1.3 Interne LAN, DMZ'er, fjernadgangsveje samt forbindelser mellem lokationer eller til tredjeparter

2.1.4 Understøttende systemer såsom DNS, DHCP, proxyservere og overvågningsenheder

2.2 Politikken er bindende for alle medarbejdere og tredjepartsleverandører, der administrerer, konfigurerer, overvåger eller på anden måde interagerer med organisationens netværk, uanset om dette sker på lokal infrastruktur eller i cloudmiljøer.

2.3 Alle systemer og applikationer, der er forbundet til organisationens netværk, skal uanset placering eller ejerskab efterleve disse krav til netværkssikkerhed.

3. Mål

3.1 Sikre fortrolighed, integritet og tilgængelighed for data, der transmitteres over netværk, gennem stærk adgangsstyring, sikker routing og overvågning.

3.2 Forebygge uautoriseret adgang, lateral bevægelse og udnyttelse af netværkstilsluttede ressourcer ved at håndhæve netværkssegmentering, zoneopdeling og beskyttelse af systemgrænser.

3.3 Opretholde ensartede netværkskonfigurationer baseret på branchestandarder og trusselsintelligens for at beskytte mod cybertrusler under udvikling.

3.4 Sikre ekstern kommunikation, cloudforbundet kommunikation og fjernadgang ved hjælp af krypterede forbindelser, stærk brugergodkendelse og validering af endepunkter.

3.5 Etablere synlighed i netværksaktivitet gennem centraliseret logning af adgang, inspektion af netværkstrafik i realtid og automatiske alarmer.

3.6 Sikre overholdelse af regulatoriske krav ved at tilpasse alle netværksaktiviteter til kravene i ISO/IEC 27001:2022, GDPR, NIS2, DORA og COBIT 2019.

4. Roller og ansvar

4.1 Chief Information Security Officer (CISO)

4.1.1 Er ansvarlig for denne politik og skal sikre, at den gennemgås og er tilpasset organisationens overordnede cybersikkerhedsstrategi.

4.1.2 Godkender modeller for netværkssegmentering, firewallregelsæt for følsomme systemer og anmodninger om undtagelser.

4.2 Leder af netværkssikkerhed / ansvarlig for infrastruktursikkerhed

4.2.1 Forvalter netværksforsvarsarkitekturen, herunder firewalls, systemer til registrering og forebyggelse af indtrængen (IDS/IPS), VPN-løsninger og sikker routing.

4.2.2 Fører tilsyn med netværkssegmentering, tildeling af VLAN'er, zoneopdeling af trafik og ekstern konnektivitet.

4.2.3 Sikrer løbende gennemgang af filtrering af indgående og udgående trafik samt håndhævelse af Zero Trust på tværs af netværkslag.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Denne politik skal gennemgås årligt af lederen af netværkssikkerhed i samarbejde med CISO og opdateres på baggrund af:

9.1.1 Nye risici (f.eks. nye angrebsteknikker og protokolsårbarheder)

9.1.2 Ændringer i infrastrukturen (f.eks. cloudmigreringer og udrulning af SD-WAN)

9.1.3 Opdateringer af regler eller standarder, der påvirker netværksbeskyttelsen

9.1.4 Revisionskonstateringer, hændelsestendenser eller forringet ydeevne som følge af kontroller

9.2 Gennemgange skal også udløses af:

9.2.1 Væsentlige ændringer i netværksarkitekturen

9.2.2 Implementering af nye firewall-, VPN- eller cloudnetværksplatforme

9.2.3 Udfasning af nøgleaktiver eller betroede zoner

9.3 Opdateringer skal registreres i ISMS-dokumentstyringsregisteret og formidles til:

9.3.1 Infrastruktur- og netværksdrift

9.3.2 SOC og sikkerhedstekniske teams

9.3.3 Applikationsteams med systemafhængigheder til netværksflows

9.3.4 Alle tredjepartsleverandører med aktiv interkonnektivitet

9.4 Alle tidligere versioner af politikken skal arkiveres sikkert med annoteringer om ændringshistorik for at bevare revisionsspor og sporbarhed af ændringer.

10. Relaterede politikker og sammenhænge

10.1 P1 - Informationssikkerhedspolitik. Fastlægger grundlæggende sikkerhedsprincipper og kræver lagdelte beskyttelsesforanstaltninger, herunder netværksbaseret adgangsstyring og trusselskontroller.

10.2 P4 - Politik for adgangskontrol. Sikrer, at netværkssegmentering håndhæves i overensstemmelse med brugerroller, princippet om mindst privilegium og regler for tildeling af adgang.

10.3 P5 - Politik for ændringsstyring. Regulerer ændringer af firewalls, justeringer af VPN-regler og routingændringer gennem en dokumenteret og revisionsbar proces.

10.4 P12 - Politik for styring af aktiver. Understøtter identifikation og klassificering af netværkstilsluttede systemer og sikrer, at alle tilsluttede aktiver forvaltes inden for det omfang, som politikkerne fastsætter.

10.5 P22 - Lognings- og overvågningspolitik. Regulerer indsamling, korrelation og opbevaring af netværkslogfiler, herunder firewallhændelser, adgangsforsøg og anomalidetektioner.

10.6 P30 - Politik for hændelseshåndtering. Definerer eskalerings-, inddæmnings- og elimineringsprocedurer som reaktion på netværksbårne trusler eller indtrængen, såsom DDoS, lateral bevægelse eller uautoriseret adgang.

11. Referencestandarder og rammeværker

11.1 Denne politik er tilpasset internationale standarder og regulatoriske krav, der fastsætter krav til sikker netværksdrift, netværkssegmentering, perimeterbeskyttelse og sikker fjernadgang.

11.2 ISO/IEC 27001

11.2.1 Klausul 8.1 - Operationel planlægning og styring: Kræver, at teknologiske kontroller, herunder netværkssikkerhedsforanstaltninger, integreres i operationelle processer.

11.3 ISO/IEC 27002:2022

11.3.1 Kontroller 8.20-8.22: Giver vejledning om beskyttelse af netværk, segmentering af tjenester og sikring af netværkstjenester gennem adgangsstyring og overvågning.

11.4 NIST SP 800-53 Rev.5

11.4.1 SC-7 - Beskyttelse af systemgrænser: Kræver perimeterkontroller, netværkssegmentering og sikre sammenkoblinger.

11.4.2 AC-4 - Håndhævelse af informationsflow: Understøtter zoneopdeling og regelbaserede begrænsninger på netværkstrafik.

11.4.3 SC-32 - Partitionering af informationssystemer: Fremmer logisk adskillelse af informationssystemer.

11.5 EU GDPR (2016/679)

11.5.1 Artikel 32 - Behandlingssikkerhed: Kræver tekniske foranstaltninger såsom firewalls og netværkssegmentering til beskyttelse af personoplysninger.

11.6 EU NIS2-direktivet (2022/2555)

11.6.1 Artikel 21(2)(d): Kræver effektiv sikkerhed for netværks- og informationssystemer, perimeterbeskyttelse, sikker konfiguration og kontroller for adskillelse.

11.7 EU DORA (2022/2554)

11.7.1 Artikel 9 - Styring af IKT-risiko: Pålægger finansielle enheder at beskytte netværk og sammenkoblinger mod uautoriseret adgang, datalækage og driftsforstyrrelser.

11.8 COBIT 2019

11.8.1 DSS01.03 - Overvågning af infrastruktur: Kræver proaktiv kontrol med netværkssundhed og konnektivitet.

11.8.2 DSS05.01 - Beskyttelse mod malware: Omfatter netværkssegmentering og beskyttelse af systemgrænser for at minimere spredning.

11.8.3 MEA03 - Overvågning, evaluering og vurdering af efterlevelse: Understøtter håndhævelse af netværkspolitikken og vurdering af efterlevelse.