					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P21S					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**

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Clause 8	-
ISO/IEC 27002:2022	Control 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
EU GDPR	Article 32	-
EU NIS2	Articles 21(2)(d), (e)	-
EU DORA	Articles 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Formål

1.1. Formålet med denne politik er at sikre, at al intern og ekstern netværkskommunikation beskyttes mod uautoriseret adgang, manipulation, aflytning og misbrug gennem klart definerede sikkerhedskontroller.

1.2. Politikken fastlægger krav til sikker design, anvendelse og styring af netværksinfrastruktur, herunder routere, trådløse adgangspunkter, fjernadgangsforbindelser og segmenterede netværk.

1.3. Politikken skal minimere eksponeringen for internetbaserede trusler, sikre fortroligheden af data, der overføres via interne og eksterne netværk, og opretholde tilgængeligheden af kritiske tjenester.

1.4. Denne politik understøtter certificering efter ISO/IEC 27001:2022 og bidrager direkte til opfyldelse af juridiske og regulatoriske forpligtelser efter GDPR, NIS2 og DORA samt dokumenterer et teknisk sikkerhedsniveau over for kunder og revisorer.

2. Omfang

2.1. Denne politik gælder for alle komponenter i organisationens IT-netværk, herunder:

2.1.1. Kablet og trådløs infrastruktur på kontorlokationer

2.1.2. Routere, switche, adgangspunkter, firewalls og gateways

2.1.3. Fjernadgangsforbindelser, herunder VPN, RDP og cloudtunneler

2.1.4. Cloudbaserede applikationer, der tilgås fra interne eller eksterne netværk

2.1.5. Enheder, der tilsluttes netværket af medarbejdere, kontrahenter eller gæster

2.2. Denne politik regulerer både fysiske og logiske netværkssegmenter, herunder gæstezoner, IoT-enheder og backoffice-systemer.

2.3. Politikken omfatter alt personale med adgang til organisationens netværk, herunder:

2.3.1. Interne medarbejdere

2.3.2. Fjernarbejdere og medarbejdere i hybride arbejdsformer

2.3.3. Eksterne leverandører, konsulenter og tjenesteudbydere

2.3.4. Gæster med midlertidig Wi-Fi-adgang

3. Mål

3.1. Sikre, at organisationens netværk er beskyttet mod uautoriseret adgang og eksterne cybertrusler

3.2. Håndhæve korrekt segmentering mellem betroede og ikke-betroede netværk (f.eks. gæste-Wi-Fi og leverandøradgang)

3.3. Muliggøre sikker fjernadgang uden at kompromittere interne systemer

3.4. Forebygge spredning af malware og dataeksfiltrering via netværkskanaler

3.5. Etablere overvågning, alarmering og revision af netværksaktivitet til understøttelse af hændelsesdetektion og efterlevelse

3.6. Sikre, at kun godkendte og sikrede enheder må tilsluttes interne netværk

3.7. Opfylde forpligtelser efter ISO 27001, GDPR og relaterede cybersikkerhedsrammeværk

4. Roller og ansvar

4.1. Direktør (GM)

4.1.1. Er ansvarlig for denne politik og sikrer, at der allokeres passende ressourcer til sikker design og styring af netværk

4.1.2. Gennemgår undtagelser fra netværkssikkerhedskontroller og godkender aftaler om leverandøradgang til netværk

4.1.3. Gennemgår hændelser eller revisionskonstateringer relateret til svagheder i netværkssikkerheden

4.2. IT-supportleverandør / intern IT-funktion

4.2.1. Implementerer, konfigurerer og vedligeholder alle firewalls, routere, switche og trådløse controllere

4.2.2. Styrer segmentering mellem interne, gæste- og eksterne netværk

4.2.3. Overvåger logfiler og alarmer vedrørende forsøg på uautoriseret adgang eller netværksanomalier

4.2.4. Sikrer, at firmware- og konfigurationsopdateringer implementeres sikkert og rettidigt

[... 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. Årlig gennemgang

9.1.1. Denne politik skal gennemgås mindst én gang årligt af direktøren sammen med IT-supportleverandøren og privatlivskoordinatoren.

9.2. Udløsende forhold for mellemliggende gennemgang

9.2.1. Gennemgang af politikken skal også udløses af:

9.2.1.1. Væsentlige ændringer i netværksarkitekturen (f.eks. nye VPN- eller firewallsystemer)

9.2.1.2. En netværksrelateret hændelse (f.eks. indtrængen, spredning af ransomware eller dataeksfiltrering)

9.2.1.3. Juridiske, regulatoriske eller rammeværksmæssige opdateringer, der påvirker netværksbeskyttelsen

9.2.1.4. Nye leverandørplatforme, der kræver alternative adgangsmetoder eller protokoller

9.3. Versionsstyring og dokumentation

9.3.1. Revisioner af politikken skal registreres med versionsnummer, dato og resumé af ændringer

9.3.2. Tidligere versioner skal arkiveres i mindst 3 år

9.3.3. Opdateringer skal kommunikeres til berørte medarbejdere med påkrævet bekræftelse, hvor der indføres væsentlige ændringer i adfærdskrav

10. Relaterede politikker og sammenhænge

10.1. Denne politik skal implementeres sammen med følgende SME-sikkerhedspolitikker:

10.1.1. P9S – Politik for fjernarbejde: Håndhæver sikre metoder til fjernadgang, VPN-krav og beskyttelse af endepunkter for brugere uden for organisationens lokationer.

10.1.2. P12S – Politik for styring af aktiver: Sikrer, at alle netværkstilsluttede systemer identificeres, kategoriseres og spores med opdateret sikkerhedsstatus.

10.1.3. P17S – Databeskyttelses- og privatlivspolitik: Sikrer, at netværkssegmentering, adgangskontroller og logning understøtter principper for databeskyttelse og privatliv efter GDPR.

10.1.4. P22S – Politik for logning og overvågning: Fastlægger krav til indsamling og gennemgang af logfiler fra netværksenheder, fjernforbindelser og trådløse controllere.

10.1.5. P30S – Politik for hændelseshåndtering: Definerer påkrævede handlinger ved netværksbrud, forsøg på uautoriseret adgang eller spredning af malware via interne netværk.

11. Referencestandarder og rammeværk

11.1. ISO/IEC 27001

11.1.1. Klausul 8.1 – Kræver implementering af kontroller, der sikrer sikker og robust drift, herunder netværk.

11.2. ISO/IEC 27002

11.2.1. Kontrol 8.20 – Giver teknisk og proceduremæssig vejledning om sikring af netværksadgang, segmentering og overvågning.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Kræver styring af informationsflow i netværk og mellem systemer.

11.3.2. SC-7 – Kræver beskyttelse af systemgrænser, sikker routing og netværkssegmentering for at reducere risikoen for uautoriseret adgang.

11.4. EU GDPR

11.4.1. Artikel 32 – Kræver passende tekniske og organisatoriske foranstaltninger til at sikre fortrolighed, integritet og tilgængelighed for netværksforbundne systemer og tjenester, der behandler personoplysninger.

11.5. EU NIS2-direktivet

11.5.1. Artikel 21(2)(d) – Kræver risikobaserede tekniske foranstaltninger, herunder netværkssikkerhed og adgangsstyring.

11.5.2. Artikel 21(2)(e) – Kræver systemsegmentering og isolering for at forhindre spredning af cyberhændelser.

11.6. EU DORA

11.6.1. Artikel 9 – Kræver, at virksomheder implementerer kontroller for styring af IKT-risiko, herunder kontroller for sikre netværk og kommunikation.

11.6.2. Artikel 10 – Kræver, at strategier for digital robusthed omfatter beskyttelse af netværksinfrastruktur og fjernforbindelser.

11.7. COBIT 2019

11.7.1. DSS05.02 – Kræver effektiv beskyttelse af IT-infrastruktur og netværksmiljøer mod interne og eksterne trusler.

11.7.2. APO13.01 – Kræver risikostyringsstrategier, der omfatter netværkssegmentering og overvågning som led i trusselsreduktion.