					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P21S					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	-
ISO/IEC 27002:2022	Kontroll 8	-
NIST SP 800-53 Rev.5	AC-4, SC-7	-
EU:s dataskyddsförordning (GDPR)	Artikel 32	-
EU:s NIS2-direktiv	Artiklarna 21.2 d och e	-
EU:s DORA-förordning	Artiklarna 9, 10	-
COBIT 2019	DSS05.02, APO13	-

1. Syfte

1.1. Syftet med denna policy är att säkerställa att all intern och extern nätverkskommunikation skyddas mot obehörig åtkomst, manipulation, avlyssning och missbruk genom tydligt definierade säkerhetskontroller.

1.2. Policyn fastställer krav för säker utformning, användning och hantering av nätverksinfrastruktur, inklusive routrar, trådlösa åtkomstpunkter, fjärråtkomstanslutningar och segmenterade nätverk.

1.3. Policyn ska minimera exponeringen för internetbaserade hot, säkerställa konfidentialiteten för data som överförs via interna och externa nätverk samt upprätthålla tillgängligheten för kritiska tjänster.

1.4. Denna policy stödjer certifiering enligt ISO/IEC 27001:2022 och bidrar direkt till att uppfylla rättsliga och regulatoriska skyldigheter enligt GDPR, NIS2 och DORA samt ger kunder och revisorer säkerhet avseende tekniska skyddsåtgärder.

2. Omfattning

2.1. Denna policy gäller för alla komponenter i organisationens IT-nätverk, inklusive:

2.1.1. Trådbunden och trådlös infrastruktur i kontorslokaler

2.1.2. Routrar, switchar, åtkomstpunkter, brandväggar och gateways

2.1.3. Fjärråtkomstanslutningar, inklusive VPN, RDP och molntunnlar

2.1.4. Molnbaserade applikationer som nås från interna eller externa nätverk

2.1.5. Enheter som ansluts till nätverket av anställda, entreprenörer eller gäster

2.2. Denna policy omfattar både fysiska och logiska nätverkssegment, inklusive gästzoner, IoT-enheter och backoffice-system.

2.3. Policyn gäller all personal med åtkomst till organisationens nätverk, inklusive:

2.3.1. Internanställda

2.3.2. Distansarbetande och hybridarbetande personal

2.3.3. Externa leverantörer, konsulter och tjänsteleverantörer

2.3.4. Gäster som använder tillfällig Wi-Fi-åtkomst

3. Mål

3.1. Säkerställa att organisationens nätverk är skyddat mot obehörig åtkomst och externa cyberhot

3.2. Säkerställa korrekt segmentering mellan betrodda och icke-betrodda nätverk (t.ex. gäst-Wi-Fi och leverantörsåtkomst)

3.3. Möjliggöra säker fjärranslutning utan att kompromettera interna system

3.4. Förhindra spridning av skadlig kod och dataexfiltration via nätverkskanaler

3.5. Tillhandahålla övervakning, larm och granskning av nätverksaktivitet för att stödja incidentdetektering och efterlevnad

3.6. Säkerställa att endast godkända och skyddade enheter tillåts ansluta till interna nätverk

3.7. Uppfylla krav enligt ISO/IEC 27001, GDPR och relaterade cybersäkerhetsramverk

4. Roller och ansvar

4.1. Verkställande chef (GM)

4.1.1. Är policyägare för denna policy och säkerställer att lämpliga resurser avsätts för säker utformning och hantering av nätverk

4.1.2. Granskar undantag från nätverkssäkerhetskontroller och godkänner avtal om nätverksåtkomst för leverantörer

4.1.3. Granskar incidenter eller revisionsiakttagelser relaterade till brister i nätverkssäkerheten

4.2. IT-supportleverantör/intern IT-funktion

4.2.1. Implementerar, konfigurerar och underhåller samtliga brandväggar, routrar, switchar och trådlösa styrenheter

4.2.2. Hanterar segmentering mellan interna, externa och gästnätverk

4.2.3. Övervakar loggar och larm avseende försök till obehörig åtkomst eller nätverksavvikelser

4.2.4. Säkerställer att firmware- och konfigurationsuppdateringar genomförs säkert och i rätt tid

[... 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. Årlig granskning

9.1.1. Denna policy ska granskas minst en gång per år av den verkställande chefen tillsammans med IT-supportleverantören och integritetssamordnaren.

9.2. Utlösande faktorer för mellanliggande granskning

9.2.1. Granskning av policyn ska även utlösas av:

9.2.1.1. Större förändringar i nätverksarkitekturen (t.ex. nya VPN- eller brandväggssystem)

9.2.1.2. En nätverksrelaterad incident (t.ex. intrång, spridning av ransomware eller dataexfiltration)

9.2.1.3. Uppdateringar av rättsliga krav, regulatoriska krav eller ramverk som påverkar nätverksskyddet

9.2.1.4. Nya leverantörsplattformar som kräver alternativa åtkomstmetoder eller protokoll

9.3. Versionshantering och dokumentation

9.3.1. Revideringar av policyn ska registreras med versionsnummer, datum och ändringssammanfattning

9.3.2. Tidigare versioner ska arkiveras i minst tre år

9.3.3. Uppdateringar ska kommuniceras till berörda anställda, med krav på bekräftelse när betydande förändringar i förväntat beteende införs

10. Relaterade policyer och kopplingar

10.1. Denna policy ska tillämpas tillsammans med följande säkerhetspolicyer för SME:

10.1.1. P9S – Policy för distansarbete: Fastställer säkra metoder för fjärråtkomst, krav på VPN och endpointskydd för användare utanför arbetsplatsen.

10.1.2. P12S – Policy för tillgångshantering: Säkerställer att alla system som är anslutna till nätverket identifieras, klassificeras och spåras med uppdaterad säkerhetsstatus.

10.1.3. P17S – Policy för dataskydd och integritet: Säkerställer att nätverkssegmentering, åtkomstkontroller och loggning stöder principer för integritet och dataskydd enligt GDPR.

10.1.4. P22S – Policy för loggning och övervakning: Anger krav för insamling och granskning av loggar från nätverksenheter, fjärranslutningar och trådlösa styrenheter.

10.1.5. P30S – Policy för incidenthantering: Definierar nödvändiga åtgärder vid nätverksintrång, försök till obehörig åtkomst eller spridning av skadlig kod via interna nätverk.

11. Referensstandarder och ramverk

11.1. ISO/IEC 27001

11.1.1. Klausul 8.1 – Kräver införande av kontroller för att säkerställa säker och motståndskraftig drift, inklusive nätverk.

11.2. ISO/IEC 27002

11.2.1. Kontroll 8.20 – Ger teknisk och processrelaterad vägledning för att skydda nätverksåtkomst, segmentering och övervakning.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-4 – Kräver styrning av informationsflöden inom nätverk och mellan system.

11.3.2. SC-7 – Kräver gränsskydd, säker routning och nätverkssegmentering för att minska risken för obehörig åtkomst.

11.4. EU:s dataskyddsförordning (GDPR)

11.4.1. Artikel 32 – Kräver lämpliga tekniska och organisatoriska åtgärder för att säkerställa konfidentialitet, riktighet och tillgänglighet i nätverksanslutna system och tjänster som behandlar personuppgifter.

11.5. EU:s NIS2-direktiv

11.5.1. Artikel 21.2 d – Kräver riskbaserade tekniska åtgärder, inklusive nätverkssäkerhet och åtkomstkontroll.

11.5.2. Artikel 21.2 e – Kräver systemsegmentering och isolering för att förhindra spridning av cyberincidenter.

11.6. EU:s DORA-förordning

11.6.1. Artikel 9 – Kräver att organisationer inför kontroller för IKT-riskhantering, inklusive kontroller för säkra nätverk och säker kommunikation.

11.6.2. Artikel 10 – Kräver att strategier för digital operativ motståndskraft omfattar skydd för nätverksinfrastruktur och fjärranslutning.

11.7. COBIT 2019

11.7.1. DSS05.02 – Kräver ett effektivt skydd av IT-infrastruktur och nätverksmiljöer mot interna och externa hot.

11.7.2. APO13.01 – Kräver riskhanteringsstrategier som omfattar nätverkssegmentering och övervakning som en del av riskreducering.