

Styrdokument
Dokumenttyp: Regler
Beslutat av: Kommunstyrelsen
Fastställersedatum inkl. dnr: 2026-01-14 §10, KS.2025.206
Gäller för: Gislaveds kommuns organisation
Ansvarig: Avdelningschef verksamhetsstyrning och it
Revideras: vid behov eller vart fjärde år
Följs upp: It-enheten

Regler för anslutning till kommunens nätverk

2025-11-26

Innehållsförteckning

I	Syfte	3
2	Omfattning	3
3	Ansvar	3
4	Grundregler för anslutning	3
5	Utrustning som får anslutas	4
6	Trådbundet nätverk	4
7	Trådlöst nätverk	4
8	Extern utrustning och leverantör	4
9	VPN och fjärråtkomst	4
10	Utrustning som inte uppfyller kraven	5
11	Avbrott, isolering och incidenter	5

I Syfte

Reglerna säkerställer att all nätverksanslutning till kommunens nätverk sker kontrollerat och med tillräcklig säkerhet för att skydda kommunens information, tjänster och driftmiljö.

2 Omfattning

Reglerna gäller för:

- alla nätverksanslutningar, trådbundna och trådlösa
- alla enheter som ansluts till nätverket
- interna och externa användare som får tillgång till kommunens nät

Reglerna gäller oavsett om utrustning ägs av kommunen, hyrts in eller tillhör en leverantör.

3 Ansvar

- Verksamheter säkerställer att behov och förutsättningar kommuniceras så att IT-enheten kan planera anslutning och förändringar, samt ansvarar för att säkerställa att anslutna enheter och tjänster följer dessa regler.
- Chefer ansvarar för att medarbetare och konsulter använder nätverket enligt gällande krav.
- IT-enheten, i samverkan med verksamheten, ansvarar för nätverksdesign, segmentering, säkerhet och övervakning.
- Informationssäkerhetsfunktionen stödjer vid risk- och säkerhetsbedömningar.

Brott mot reglerna kan leda till indragen åtkomst, isolering av utrustning, blockering av trafik eller incidentutredning.

4 Grundregler för anslutning

- Endast godkända och säkra enheter får anslutas.
- Nätverkets zonindelning ska följas. Placering i zoner styrs av informationens klassning och tekniska risker.
- Aktivitet på nätverket loggas och kan följas upp enligt kommunens rutiner för logghantering och incidenthantering.

IT-enheten beslutar om:

- vilka nät som finns
- vilka enheter som får anslutas
- vilken säkerhetsnivå respektive nät har

5 Utrustning som får anslutas

Endast utrustning som uppfyller kommunens säkerhetskrav får anslutas. Det inkluderar:

- kommunens klienter, servrar och driftutrustning
- kommunens godkända mobila enheter
- utrustning som genomgått teknisk kontroll och säkerhetsbedömning

IT-enheten avgör i enlighet med gällande rutiner om utrustning uppfyller kraven för anslutning.

6 Trådbundet nätverk

- Endast av IT-enheten godkända enheter får anslutas till nätverksuttag.
- Uttag får inte byggas ut, flyttas eller modifieras av verksamheten utan samråd med IT-enheten.

7 Trådlöst nätverk

- Kommunens trådlösa nät är uppdelat i interna nät och gästnät.
- Endast tjänstenheter eller annan godkänd utrustning får anslutas till interna nät.
- Gästnät får endast användas av privata enheter.
- Egna eller externa trådlösa nät får inte etableras inom kommunens lokaler.

8 Extern utrustning och leverantör

Leverantörer och externa aktörer får endast ansluta utrustning som är godkänd av IT-enheten. Detta gäller även:

- styr- och driftutrustning
- IoT- och sensorenheter
- kamera- och säkerhetssystem
- telefoni- och kommunikationsutrustning

All extern åtkomst ska vara tidsbegränsad, spårbar och följa kommunens krav för leverantörssäkerhet.

9 VPN och fjärråtkomst

VPN och fjärranslutning är endast tillåten via kommunens godkända lösningar. Krav:

- stark autentisering (MFA)
- enheten måste vara godkänd och uppfylla säkerhetskrav
- åtkomst kan tidsbegränsas eller isoleras vid behov

Fjärrstyrningsprogram som inte godkänts av IT-enheten får inte användas.

I 0 Utrustning som inte uppfyller kraven

Utrustning som saknar säkerhetsstöd eller uppdateringar får inte anslutas.

IT-enheten kan besluta att:

- isolera eller ta bort enheter från nätverket
- kräva uppgradering eller att utrustningen byts ut

I 1 Avbrott, isolering och incidenter

IT-enheten får när som helst avbryta anslutning, isolera utrustning eller blockera trafik vid misstanke om säkerhetsrisk, skadlig aktivitet, felkonfiguration eller policybrott.

Incidenter hanteras enligt kommunens incidentrutin.