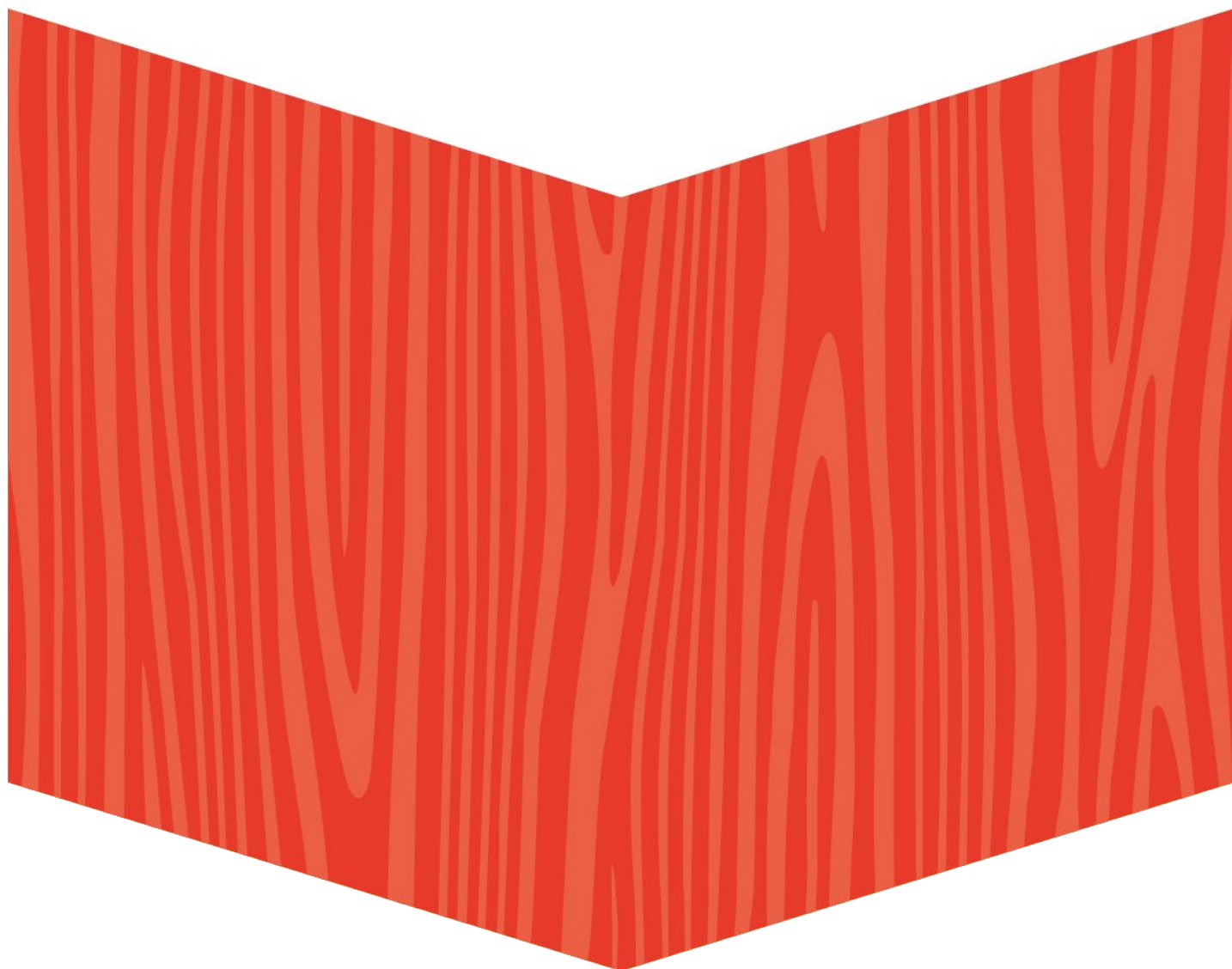




Riktlinjer för cybersäkerhet

Kommunstyrelsen

Flik 8.41





Dokumenttyp	Riktlinjer
Dokumentnamn	Riktlinjer för cybersäkerhet
Fastställd	2026-02-09
Beslutande	Kommunstyrelsen
Giltighetstid	2026-02-09 – tills vidare
Processägare	Kommundirektör
Senast reviderad	
Detta dokument gäller för	Vingåkers kommun

Innehållsförteckning

1. Syfte och Omfattning	4
2. Principer och Mål	4
3. Ledningens Ansvar.....	4
4. Obligatoriska cybersäkerhetsåtgärder	4
5.1 Uppföljning och revision.....	5

1. Syfte och Omfattning

Syftet med dessa riktlinjer är att utifrån den av kommunfullmäktige beslutade policyn för cybersäkerhet säkerställa en hög gemensam nivå av nätverks- och informationssäkerhet samt att skydda kommunens medborgare, verksamheter och tillgångar mot cyberhot, störningar och incidenter.

Riktlinjerna konkretiserar innehållet i den policy som fullmäktige har beslutat när det gäller ledningens åtagande att uppfylla de krav som ställs i Lag (2025:1506) om cybersäkerhet (som genomför EU:s NIS 2-direktiv), samt andra relevanta lagkrav (t.ex. GDPR, OSL).

Riktlinjerna omfattar precis som policyn alla kommunala nämnder, förvaltningar, kommunala bolag (där lagen så kräver), anställda, inhyrd personal samt system och tjänster som behandlar kommunens information.

2. Principer och Mål

Fullmäktige har i policyn lagt fast att kommunens cybersäkerhetsarbete ska bygga på följande principer:

- Riskbaserat arbetssätt: Cybersäkerheten ska utgå från kontinuerlig riskanalys och anpassas till de hot och sårbarheter som är relevanta för respektive verksamhet.
- Systematiskt och förebyggande: Arbetet ska vara systematiskt, dokumenterat och integrerat i kommunens befintliga ledningssystem.
- Kontinuitet och robusthet: Säkerhetsåtgärder ska säkerställa att kritiska kommunala tjänster kan upprätthållas även vid allvarliga cyberincidenter.

Det övergripande målet är enligt fullmäktiges policy att kommunen minst ska uppnå och bibehålla den grundläggande säkerhetsnivå som krävs av den nya cybersäkerhetslagen för att minimera risken för betydande incidenter i samhällsviktiga tjänster.

3. Ledningens Ansvar

Kommunfullmäktige har ålagt Kommunstyrelsen ansvar för genomförandet, uppföljning och tillsyn av denna policy samt det övergripande cybersäkerhetsarbetet. I det ingår bland annat att Kommunstyrelsen ska säkerställa:

- Styrning: En organisation och tydliga roller finns för att hantera och övervaka cybersäkerhetsarbetet.
- Utbildning: Ledningen och samtliga medarbetare genomgår regelbunden och obligatorisk utbildning i cybersäkerhet för att uppnå nödvändig kompetens (1 § Lag om cybersäkerhet).
- Resurser: Tillräckliga ekonomiska och personella resurser avsätts för att uppfylla lagkraven och de åtgärder som krävs för en hög säkerhetsnivå.

4. Obligatoriska cybersäkerhetsåtgärder

Nedan återges de åtgärder som fullmäktige beslutat i policyn, och därutöver anges vilka enheter som under fullmäktige och styrelse har ansvaret för att verkställa åtgärderna.

A. Incidenthantering: Kommunikations- och IT-enheten ansvarar

Etablera processer för snabb detektion, analys och hantering av incidenter, samt säkerställa efterlevnad av tidsfristerna för incidentrapportering till tillsynsmyndigheter vid allvarliga incidenter.

B. Kontinuitetshantering: Kommunikations- och IT-enheten ansvarar

Utveckla och testa planer för kontinuitet och återställning (återhämtning efter incidenter) för alla kritiska system och tjänster.

C. Säkerhet i leveranskedjan: Kanslienheten ansvarar

Ställa tydliga cybersäkerhetskrav på externa leverantörer och tjänsteleverantörer, särskilt de som tillhandahåller kritiska IT-system och molntjänster inklusive riskklassning av leverantörer.

D. Säkerhet vid utveckling: Kommunikations- och IT-enheten ansvarar

Införa rutiner för säkerhetsmässig utvärdering och testning vid anskaffning och utveckling av nya system (säkerhet genom design).

E. Kryptografi och fysisk säkerhet: Kommunikations- och IT-enheten ansvarar

Använda kryptografiska lösningar för att skydda känslig data samt säkerställa adekvat fysisk säkerhet för nätverks- och informationssystem.

F. Åtkomstkontroll och tillgångsförvaltning: Kommunikations- och IT-enheten ansvarar

Införa strikta policyer för åtkomstkontroll baserat på principen om minsta behörighet, inklusive flerfaktorsautentisering (MFA) för all fjärråtkomst till nätverk och kritiska system. Säkerställa att rutiner efterlevs för att tilldela och återta behörigheter vid anställning, förflyttning och avslut. Samt när så krävs genomföra adekvat personalkontroll.

G. Cyberhygien: Kommunikations- och IT-enheten ansvarar

Genomföra regelbunden uppdatering av system, skydd mot skadlig kod samt införa processer för patch management, sårbarhetshantering och säker konfigurering av nätverk.

H. Kriskommunikation: Kommunikations- och IT-enheten ansvarar

Säkerställa att alternativa kommunikationsvägar finns tillgängliga och kan utnyttjas i händelse av cyberangrepp.

5. Uppföljning och revision

Kommunstyrelsen har i uppdrag från fullmäktige att årligen följa upp att policyn för cybersäkerhet efterlevs och att säkerhetsnivån är adekvat. En central del i det är uppföljning av de uppdrag som ges genom dessa riktlinjer.

Revision: Fullmäktige har i policyn angett att revision av cybersäkerhetsarbetet ska genomföras regelbundet av internrevisor eller extern specialist. Kommunstyrelsen kommer därför att ta initiativ till att sådana revisioner genomförs.

Rapportering: Fullmäktige har beslutat att en rapport om cybersäkerhetsläget och efterlevnaden av lagkraven ska lämnas till fullmäktige minst en gång per mandatperiod. Kommunstyrelsen har i uppdrag att se till att det görs.