

**KUNTA
LIITTO**

*Onneksi on
KUNNAT!*

Digital säkerhet i kommunen

**På vilket sätt kan du som kommunal
beslutsfattare fungera som en stark
länk i din kommuns digitala säkerhet?**

Iakttagelser till stöd för arbetet för kommunens förtroendevalda 26.5.2025
Martti Setälä, specialsakkunnig, digitalisering och informationssamhället



Inledning

- Digitaliseringen gör det möjligt för kommunen att ordna tjänsterna på ett bättre och effektivare sätt. Målen kan dock inte nås utan att informationssäkerheten, cybersäkerheten och dataskyddet – dvs. *den digitala säkerheten* – för de digitala tjänsterna har säkerställts. Den behöver också ses över kontinuerligt, eftersom både hoten och lösningarna utvecklas snabbt.
- Kommuninvånarnas förtroende för förvaltningen beror dessutom till en del på hur pålitliga de digitala tjänsterna är. Som förtroendevald har också du ansvar för att säkerställa tjänsternas säkerhet, oberoende av om du verkar i fullmäktige, kommunstyrelsen, nämnderna eller i ett kommunägt bolags styrelse.
- Den här presentationen ger en introduktion i ämnet genom att lyfta fram centrala synpunkter på ditt ansvar och dina möjligheter att påverka samt länkar till fördjupat material.
- Som förtroendevald i kommunen kommer du att få riktlinjer och skyldigheter inom digital säkerhet. Det är bra att studera dem och ta sig an dem först.
- Vi rekommenderar att du sedan går igenom den här presentationen (längd ca 10–15 minuter) samt, i mån av tid och möjlighet, utbildningen som Myndigheten för digitalisering och befolkningsdata erbjuder: [Digital säkerhet för kommunernas förtroendevalda](#) (längd 30–60 minuter). Fler materialrekommendationer finns i slutet av dokumentet.



Den digitala säkerheten utvecklas genom långsiktigt grundarbete och genom gemensamt arbete 1/2

- Grunderna för den digitala säkerheten i kommunen ska byggas upp långsiktigt och systematiskt.
 - Utvecklingen ska basera sig på kunskap och förståelse för kommunens interna och externa digitala verksamhetsmiljö.
 - Kommunen ska på ett ändamålsenligt sätt organisera ansvaret, anvisningarna, utbildningarna, arbetsredskapen och övervakningen inom den digitala säkerheten.
 - Fastställandet av effektiva digitala säkerhetsåtgärder kräver klassificering av information, identifiering av kritiska tjänster och material samt riskbedömning och riskhantering under hela databehandlingens livscykel.
 - För att säkerställa den digitala säkerheten behövs ändamålsenliga tekniska och administrativa lösningar.
 - En kontrollerad publicering av information är en viktig del av den digitala säkerheten.
- Upphandlingsprocessen är väsentlig för att säkerställa den digitala säkerheten.
 - I upphandlingsvillkoren och avtalen ska kraven på digital säkerhet beaktas i tillräcklig mån och preciseras hur tjänsternas överensstämmelse med kraven övervakas.
- Kommunen ska också ha beredskap och kontinuitetshantering, dvs. förmåga att hantera och återhämta sig från störningssituationer inom den digitala säkerheten.
 - Dessa behöver övas regelbundet.

Den digitala säkerheten utvecklas genom långsiktigt grundarbete och genom gemensamt arbete 2/2

- Ledningens roll betonas när det gäller att säkerställa den digitala säkerheten.
 - Till ledningen hör bl.a. hantering av strategiska digitala säkerhetsrisker, godkännande av modellen för hantering av digitalt skydd, hantering av kvarstående risker samt övervakning av helheten av digitalt skydd.
 - Ledningens yttersta ansvar – inklusive den digitala säkerheten – kan inte delegeras även om det operativa ansvaret har lagts ut på en tjänsteproducent utanför kommunen.
 - Det är viktigt att ledningen förbinder sig till att upprätthålla och utveckla den digitala säkerheten och tydligt visar detta för personalen, intressentgrupperna och samarbetspartnerna.
- Digitaliseringens roll i kommunernas tjänsteproduktion och verksamhet ökar – samtidigt ökar behovet av satsningar på digital säkerhet
 - Produktiviteten och genomslaget hos åtgärderna för digital säkerhet bör kontinuerligt utvärderas och utvecklas.
 - Gamla verksamhetsmodeller och praxis bör vid behov ändras så att satsningar kan göras på ett produktivt och högklassigt sätt.
 - Betydelsen av och behovet av samarbete med berörda parter ökar på alla nivåer.
 - Samarbetet mellan och inom kommunerna (mellan funktioner och sektorer) står i centrum.
 - Styrning på nationell nivå, utvecklingsfinansiering, lösningar för digitala säkerhet och stöd behövs.
 - Tjänsteproducenter som är engagerade och som förstår kommunerna har också en viktig roll.



Inom sektorerna bör särskilda frågor om dataskydd och informationssäkerhet beaktas 1/2

- **Inom bildningsväsendet** ansvarar kommunen för en stor mängd personuppgifter om elever och föräldrar. Skyddet av personuppgifter är viktigt och beror både på kommunens egna verksamhetsmodeller och på hur säkra tjänsteleverantörernas informationssystem är.
- Artificiell intelligens och andra digitala lösningar ska införas i undervisningen med försiktighet, både för att kunna skydda personuppgifterna och för att kunna hänvisa användarna på förhand till en trygg användning av lösningarna.
- I planläggnings-, byggnadstillsyns-, vatten- och infrastrukturutvecklingsuppgifter inom **sektorn för den byggda miljön, dvs. den tekniska sektorn**, produceras, hanteras och publiceras beslutsuppgifter, planer, visualiseringar, kartor och maskinläsbara geografiska data i anslutning till infrastrukturen.
- Kommunerna publicerar information om den byggda miljön bland annat på webbsidor, i informationstjänsterna och i dokumenthandeln samt delar data som uppkommer i kommunens uppgifter via laddningstjänster och tekniska gränssnitt.
- Kommunerna ska systematiskt identifiera känsliga delar av kritisk infrastruktur samt sekretessbelägga och skydda kritiska uppgifter i anslutning till dem. Delning av data ska genomföras omsorgsfullt och kontrollerat



Inom sektorerna bör särskilda frågor om dataskydd och informationssäkerhet beaktas 2/2

- **Kommunen ska bättre än tidigare identifiera och skydda sekretessbelagda uppgifter och betydande personuppgiftsregister som kommunen ansvarar för.**
- Sekretesskraven och skyddet av personuppgifter ska beaktas också i kommunens upphandlings- och ekonomidokumentation (anbudsförfrågningar, kontrakt, fakturor och ekonomiska rapporter), i beslutsdokumentationen och i andra handlingar som publiceras.
- Till exempel ska detaljerade uppgifter om kommunens säkerhets- och beredskapsarrangemang och därmed eventuella sårbarheter identifieras och sekretessbeläggas.
- Balansgången mellan behovet av att skydda uppgifterna och iakttagandet av offentlighetsprincipen kräver kontinuerligt noggrant övervägande. Öppenhet ska vidhållas så långt det är möjligt samtidigt som eventuella sårbarheter systematiskt bör identifieras och sekretessbeläggas.

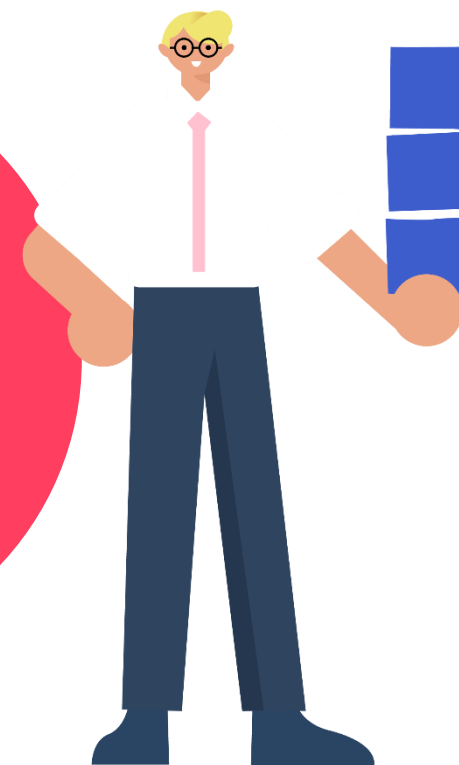


Den förtroendevaldas tre roller i säkerställandet av den digitala säkerheten i kommunen

Den förtroendevalda som godkännare och övervakare av kommunens/det kommunägda bolagets strategi och styrsystem samt budget

Den förtroendevalda som nationell och internationell politisk påverkare

Den förtroendevalda som "arbetstagare" i kommunorganisationen



Roll 1: Den förtroendevalda som godkännare och övervakare 1/3

Den förtroendevalda som godkännare och övervakare av kommunens/det kommunägda bolagets strategi och styrsystem samt budget

Den förtroendevalda som nationell och internationell politisk påverkare

Den förtroendevalda som "arbetstagare" i kommunorganisationen

- I **kommunstyrelsen** kan du säkerställa att
 - lägesrapporten om digital säkerhet behandlas regelbundet i kommunstyrelsen
 - betydande digitala säkerhetsrisker beaktas i kommunens övergripande riskhantering
 - helhetsförståelsen av läget samt riskhanteringen och tillsynen i fråga om den digitala säkerheten är tillräcklig
- Som **kommunfullmäktigeledamot** kan du säkerställa att
 - lägesrapporten om digital säkerhet behandlas regelbundet i kommunfullmäktige
 - kommunen har de resurser som behövs för att säkerställa den digitala säkerheten
 - kommunen samarbetar med andra kommuner för att säkerställa tillräckliga förmågor och resurser (bl.a. upphandling, ägarstyrning av anknutna enheter, kontakt med tjänsteleverantörer)
- Som ledamot i en **kommunal nämnd** kan du säkerställa att
 - lägesrapporten om digital säkerhet behandlas regelbundet i nämnden
 - nämnden har en tillräcklig helhetsförståelse av läget samt riskhanteringen och tillsynen i fråga om den digitala säkerheten – nämnden kan ha väsentliga personregister som den ansvar för



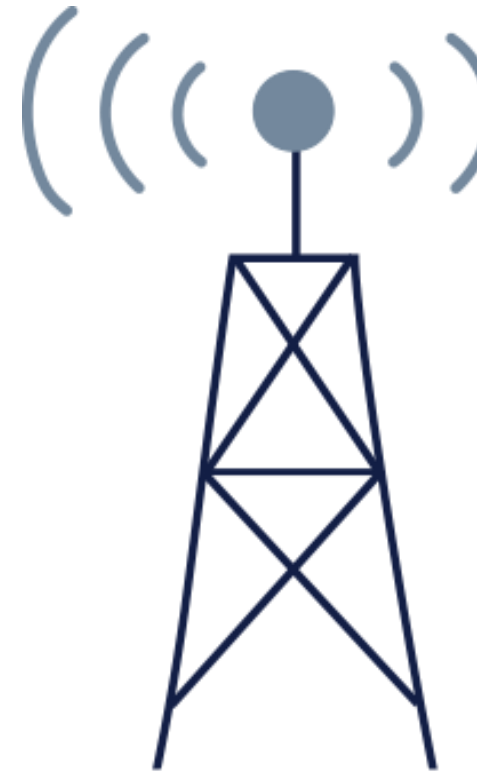
Roll 1: Den förtroendevalda som godkännare och övervakare 2/3

Den förtroendevalda som godkännare och övervakare av kommunens/det kommunägda bolagets strategi och styrsystem samt budget

Den förtroendevalda som nationell och internationell politisk påverkare

Den förtroendevalda som "arbetstagare" i kommun-organisationen

- När du är verksam i **styrelsen för ett kommunägt bolag med kritisk infrastruktur** (såsom energi-, vatten- eller avfallshantering) kan du säkerställa att
 - lägesrapporten om digital säkerhet behandlas regelbundet i bolagets styrelse
 - helhetsförståelsen av läget samt riskhanteringen och tillsynen i fråga om den digitala säkerheten är tillräcklig i bolaget
 - den expert som ansvarar för informationssäkerheten i din kommun berättar för dig huruvida kommunens infrastrukturbolag omfattas av tillämpningsområdet för EU:s NIS2-direktiv (så är fallet endast i ett fåtal av de största kommunerna) och om så är fallet, be om lämplig utbildning för ledningen i enlighet med direktivet.
- Som ledamot i **kommunens revisionsnämnd** kan du säkerställa att
 - den digitala säkerheten på ett ändamålsenligt sätt beaktas vid intern kontroll och intern revision (att fokusera på kontroll av informationssäkerheten eller dataskyddet kan vara ett nyttigt utvecklingsinstrument för kommunen)
 - uppgifterna om digitala säkerhetsarrangemang sekretessbeläggs på ett ändamålsenligt sätt i internrevisionens och den interna kontrollens rapporter



Roll 1: Den förtroendevalda som godkännare och övervakare 3/3

Den förtroendevalda som godkännare och övervakare av kommunens/det kommunägda bolagets strategi och styrsystem samt budget

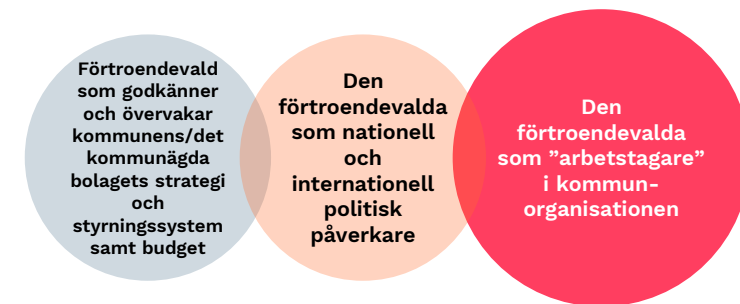
Den förtroendevalda som nationell och internationell politisk påverkare

Den förtroendevalda som "arbetstagare" i kommunorganisationen

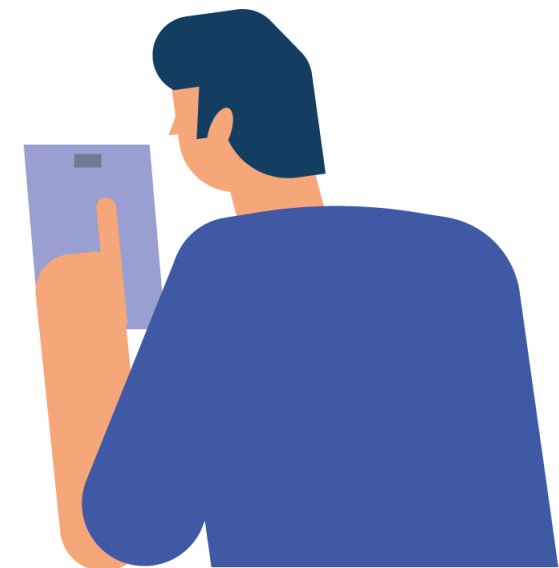
- Intervallen för översikterna över den digitala säkerheten som lämnas till organet beror på kommunen och organet.
 - torde ligga mellan en gång per fullmäktigeperiod till en gång per halvår
 - också en granskning från fall till fall kan komma i fråga t.ex. om den digitala verksamhetsmiljön förändras avsevärt, kommunen stöter på en allvarlig kränkning av informationssäkerheten eller dataskyddet eller behandlar internrevisionens rapport om informationssäkerheten eller dataskyddet.
- Innehållet i översikterna över den digitala säkerheten som ges till organet beror på organet och ärendets natur.
 - Den översikt som ges kommunstyrelsen eller nämnden kan vara mer detaljerad än den översikt som riktats till kommunfullmäktige.
 - Om det i kommunen pågår ett betydande projekt för utveckling av den digitala säkerheten, kan det vara ändamålsenligt att granska hur projektet framskrider, antingen i kommunstyrelsen eller inom det verksamhetsområde som är föremål för utveckling.
 - Behandling av sekretessbelagda uppgifter ska undvikas. Det behövs knappast heller.
 - De förtroendevalda bör koncentrera sig på tillsynsnivån i fråga om digital säkerhet, medan tjänsteinnehavarna ansvarar för praktiska operativa frågor.
 - Myndigheten för digitalisering och befolkningsdata (DVV) och Traficom Cybersäkerhetscenter erbjuder kommunerna stöd och avgiftsfria verktyg för att utveckla den digitala säkerheten och skapa en lägesbild.



Roll 2: Den förtroendevalda som kommunens ”arbetstagare”



- Som förtroendevald kan du säkerställa att
 - du känner till din egen verksamhets betydelse när det gäller att säkerställa kommunens informationssäkerhet och dataskydd
 - du har gått igenom det utbildningsmaterial som finns om kommunens digitala säkerhet
 - du vet hur du kan använda enheter och hantera data på ett säkert sätt för att garantera integritet och sekretess
 - du kan utan dröjsmål underrätta de aktörer som ansvarar för informationssäkerheten och dataskyddet i kommunen om sådana kränkningar av informationssäkerheten och dataskyddet som du observerat eller om situationer där det kan finnas en stor risk för kränkning.
 - OBS! Oaktsam användning av egna enheter, såsom laptop eller mobiltelefon, och behandling av kommunens uppgifter kan leda till att en brottslig aktör eller en aktör för en fientlig stat kan bryta sig in i kommunens informationssystem eller annars få tillgång till sekretessbelagt informationsmaterial som kommunen bör skydda.



Roll 3: Den förtroendevalda som nationell och internationell politisk påverkare



- Om du är förtroendevald i kommunen och samtidigt deltar i det nationella eller internationella politiska beslutsfattandet, kan du säkerställa att
 - finansieringen och resurserna för upprätthållandet och utvecklandet av kommunernas digitala säkerhet säkerställs samt att kommunernas särdrag och behov beaktas
 - kommunernas självstyrelse respekteras
 - inga nya krav ställs på lätta grunder
 - och om sådana införs, kompenseras kommunerna för kostnaderna för dem
 - gemensamma lösningar utarbetas på nationell nivå eller EU-nivå på ett ändamålsenligt sätt för att säkerställa den digitala säkerheten
 - man eftersträvar att minska kommunernas obefogade administrativa börda
 - kommunerna ges mångsidiga förutsättningar och lösningar för kommunalt samarbete, såsom olika sätt att ordna tjänster.
 - du identifierar hybridpåverkan som ett fenomen som också kan beröra kommunernas verksamhet. (Se materialet i slutet av dokumentet.)

Mer information och material 1/2

Kommunförbundet

- [Kommunala beslutsfattarens materialbank](#)
 - [Handbok i kommunalt beslutsfattande](#). (information om datasäkerhet och dataskydd i kommunens beslutsprocesser)
- Innehåll som är riktat till kommunala sakkunniga och som står till kommunala beslutsfattarens förfogande
 - [Digital säkerhet och cybersäkerhet](#)
 - [Dataskydd](#)
 - [Kartläggning av kommunernas digitalisering 2024](#)
 - Del 8: Digital säkerhet, innehåller bl.a. uppgifter om nuläget i fråga om digitala säkerhetsgranskningar i kommunernas olika organ
 - [Blogginlägg: Digital säkerhet i kommunen - iakttagelser för ledningen, informationsförvaltningen och sektorerna samt för intressentgrupper](#)
 - [Blogginlägg: Kommunerna som föremål för hybridpåverkan \(på finska\)](#)

FCG:s tjänst för kommunala beslutsfattare

- Grundkurs för förtroendevalda
 - De förtroendevaldas digitala färdigheter
- God förvaltning
 - Informationshantering, dataskydd och informationssäkerhet
- Sammanträdespraxis
 - Digitalt sammanträde

FCG:s dokumentation finns tillgänglig på webben om din kommun har skaffat licensen.



Mer information och material 2/2

Viktig lagstiftning

- Bekanta dig med följande: *Kommunförbundet: Innehåll riktat till kommunala sakkunniga och som finns till kommunala beslutsfattares förfogande*, samt DVV:s och FCG:s material

Myndigheten för digitalisering och befolkningsdata (DVV)

- [Webbutbildningen digital säkerhet för kommunernas förtroendevalda](#)

Cybersäkerhetscentret vid Transport- och kommunikationsverket Traficom

- [Guiden cybersäkerhet och företagsstyrelsens ansvar](#)
- [Stärkande av cybersäkerheten i finländska organisationer – anvisningar till ledningen och sakkunniga](#)

Annat material

- [Inrikesministeriet: Hybridhot och hybridpåverkan](#)
- [Valtiolla.fi: Näin hybridivaikuttaminen uhkaa yhteiskunnan resilienssiä](#)
- [Statsrådets kansli: Översikt över informationspåverkan](#)

Kontakt

Digital säkerhet och cybersäkerhet

Martti Setälä
Specialsakkunnig
Strategienheten,
Digitalisering och informationssamhället
+358 9 771 2282, +358 40 536 6350
martti.setala@kommunforbundet.fi



www.kommunforbundet.fi

***Onneksi on
KUNNAT!***

KUNTA
LIITTO