



MALÅ KOMMUN
Målågen kommunvdrna

Malå kommun

Anvisning

– Informationssäkerhet för användare

Antagen av: Administrativ chef, 2026-06-04

Sida 0 av 10

Innehållsförteckning

1 Inledning	2
2 Syfte	2
3 Omfattning och ansvar	2
4 Säkerhetsmedvetenhet och ansvar	2
4.1 Rapportera incidenter	3
4.2 Utbildning	3
5 Hanteringsregler	3
5. Övergripande regler	3
5.3 Allmänna handlingar	6
5.1 Pappersdokument	6
5.2 Muntlig information och möten	6
5.4 E-post	6
5.5 Teams	6
5.6 Internet och sociala medier	7
5.7 Säkerhetskopiering	7
6 Mobila enheter	7
7 Lösenordshantering	8
8 Skadlig kod (virus)	8
9 Spårbarhet och loggning	8
10 Användning av Artificiell Intelligens (AI)	9
10 Fysisk säkerhet	9
10.1 Tillträde till våra lokaler	9
10.1.1 Besökare	9
10.1.2 Säkerhetszoner	10
10.2 Nycklar och passerkort	10
10.3 Din arbetsplats	10
11 Distansarbete	10

1 Inledning

Information är kommunens viktigaste tillgång och har ett stort värde för alla våra verksamheter i det dagliga arbetet. Informationen kan röra till exempel skola och barnomsorg, socialtjänst, stadsplanering, hemsjukvård eller bygglov. Vi hanterar dagligen information i olika former, från muntlig, skriftlig till digital. Information kan antingen vara tillgänglig för allmänheten att få ta del av, eller känslig och får då endast vara tillgänglig för behöriga användare.

Denna anvisning är avsedd för användare och syftar till att säkerställa att all information hanteras på ett säkert och ansvarsfullt sätt oavsett i vilken form den förekommer. Alla användare, inklusive anställda, konsulter och förtroendevalda har en viktig uppgift i att skydda både vår och våra medborgares information och förtroende.

Informationssäkerhet innebär att vi måste hantera vår information på ett säkert sätt för att:

- förhindra obehörig åtkomst till informationen
- förhindra att informationen förvanskas eller förstörs
- se till att informationen är tillgänglig när den behövs

2 Syfte

Denna anvisning är tänkt att tillföra en medvetenhet till medarbetare inom Malå kommun att hantera vår information på ett säkert sätt. Allt från att komma ihåg att logga ut då vi lämnar datorn till hur och vart vi pratar om vårt arbete.

3 Omfattning och ansvar

Denna anvisning avser alla som hanterar Malå kommuns information. Det innebär alla medarbetare, men även de externa aktörer som på ett eller annat sätt handhar information som ägs av organisationen.

Ansaret för att denna anvisning efterlevs ligger ytterst på Kommunstyrelsen. Inom våra olika verksamheter ligger ansvaret på ansvarig chef. Till stöd för detta arbete finns Informationssäkerhetssamordnare, säkerhetschef, men även IT-chef eller tekniker kan också bistå med stöd.

4 Säkerhetsmedvetenhet och ansvar

Säkerhetsmedvetenhet är ett viktigt begrepp inom informationssäkerhet som handlar om att förstå potentiella risker och vara medveten om hur man på bästa sätt skyddar information. Det innebär att alla användare, oavsett roll, måste vara väl informerade

om hur information ska hanteras på ett säkert sätt för att utföra sina uppgifter. Dessutom krävs det en förståelse för vad som utgör en informationssäkerhetsincident och hur man rapporterar upptäckta risker eller brister.

Användare av kommunens informationssystem behöver ta del av och följa kommunens policy och riktlinjer för informationssäkerhet. För att agera säkerhetsmedvetet behöver användare ha förståelse för till exempel vilka konsekvenser det kan få för en enskild individ om personens sekretessbelagda information skulle komma i orätta händer, förstöras eller bli otillgänglig. I vissa fall kan vara så allvarligt att det handlar om liv eller död.

Genom att vara medveten om hur hotbilden kan se ut, kan användare aktivt bidra till att minimera riskerna för intrång och förlust av information. Säkerhetsmedvetenhet handlar också om att vara uppmärksam på vem det är vi släpper in i våra lokaler och hur vi som medarbetare fortsätter att skydda information när vi inte längre befinner oss på arbetsplatsen. Det är en gemensam uppgift för alla att upprätthålla informationssäkerheten och säkerställa att kommunens information hanteras på ett säkert och ansvarsfullt sätt.

4.1 Rapportera incidenter

Alla medarbetare har skyldighet att rapportera incidenter eller brister som misstänks kunna medföra negativ påverkan på kommunens information.

- IT-angrepp
- Skadlig kod
- Oskyddad eller röjd information
- Obehöriga i våra lokaler
- Brister i efterlevnad av denna anvisning

Alla incidenter, du kan läsa mer om hur du rapporterar i Anvisning – Incidenthantering för användare, ska rapporteras i KIA. Vid akuta, pågående IT-angrepp kontakta alltid IT-enheten omedelbart. Meddela också din närmaste chef om det inträffade.

4.2 Utbildning

Att upprätthålla informationssäkerheten i Malå kommun är av stor vikt och är något som alla anställda behöver hjälpas åt att upprätthålla. Detta gör vi genom att delta och genomföra de utbildningsinsatser som kontinuerligt kommer att skickas ut till alla verksamheter. Ansvar för att hålla sig uppdaterad ligger på den anställda.

5 Hanteringsregler

För att hantera information på ett säkert sätt behöver våra hanteringsregler följas.

5. Övergripande regler

Grundregeln är att verksamhetsinformation ska sparas i ett för ändamålet avsett verksamhetssystem.

Öppen och Intern information

- Kan sparas i M365 (Teams eller Onedrive) under tiden den handläggs, men om informationen hör till ett ärende ska den diarieföras eller hanteras i ett verksamhetssystem.

Konfidentiell och Strikt konfidentiell information

- Ska hanteras i specifika och godkända verksamhetssystem.
- Vid behov av mellanlagring (t.ex. om information behöver hanteras temporärt eller om ett verksamhetssystem inte kan vara första steget) kan information lagras under H:
- Ansökan om tillgång till H: görs till din närmsta chef som vid godkännande av din förfrågan lägger en beställning till IT.

Nedan tabell beskriver våra hanteringsregler och används som hjälp för anställda att hantera information rätt.

Information	Förklaring	Exempel på information	Lagra information	Dela information
Öppen	Information som kan delas fritt internt och externt	- Information på vår hemsida - Information i våra sociala medier	- Lagra på din Onedrive eller i Teams - Verksamhetssystem	Kan skickas öppet via exempelvis e-post
Intern	- Om informationen sprids felaktigt kan det innebära måttlig negativ effekt för Malå kommun, enskilda individer eller andra organisationer - Information som kan delas begränsat internt och externt.	- Kan innehålla personuppgifter - Arbetsdokument	- Lagra på din Onedrive eller i Teams - Verksamhetssystem	Skickas via e-post, men bör prövas innan den skickas i avseendet vilken information som delas.
Konfidentiell	- Information som om den sprids till obehöriga kan medföra betydande negativ effekt för Malå kommun, enskilda individer eller andra organisationer. - Delas med försiktighet till behöriga	- Skyddsvärda personuppgifter (personnummer, lön, värderande uppgifter, lagöverträdelse etc) - Nödplan, RSA, etc.	Lagras i avsedda verksamhetssystem som är behörighetsanpassade eller lokalt på H:	- Skickas i utskrivet format, ej via e-post. - Kan delas i möten via Teams eller plattform för säkra möten (riskbedömning görs inför möten som eventuellt hanterar konfidentiell information)
Strikt Konfidentiell	- Information som om den sprids till obehöriga kan medföra allvarlig negativ effekt för Malå kommun, enskilda individer (fara för liv) eller andra organisationer. - Delas endast med stor försiktighet till behöriga.	- Känsliga personuppgifter (hälsa, religion etc) - Skyddade personuppgifter - Personärenden - Sekretessbelagd information	Lagras i avsedda verksamhetssystem som är behörighetsanpassade eller lokalt på H:	- Skickas på ett säkert sätt, exempelvis med rekommenderat brev i säkerhetspåse, eller delas i för ändamålet avsedda verksamhetssystem - Kan delas i möten via plattform för säkra möten

5.1 Allmänna handlingar

En stor del av den information som vi behandlar inom Malå kommun är offentlig enligt offentlighetsprincipen. Detta gäller såväl de dokument du skriver och sparar i molnet, men även den information som finns i dina sms- och e-postkonversationer. Chattar i Teams kan även de begäras ut och är därför offentliga. Därmed är det viktigt att tänka på hur du kommunicerar i den digitala miljön och hur du sparar ner den dokumentation du skapar.

5.2 Pappersdokument

- Papper med Konfidentiell och Strikt konfidentiell information (känslig information) får inte lämnas framme och ska låsas in när du lämnar ditt skrivbord, även för kortare stunder.
- När du arbetar med känslig information, information där flera personer vistas, ta för vana att vända pappret med texten nedåt för att undvika oavsiktlig exponering.
- Vid utskrift ska dokument omgående hämtas upp.
- Pappersdokument som innehåller känslig information ska strimlas.

5.3 Muntlig information och möten

- En stor del av kommunens information hanteras muntligt och man ska komma ihåg att även muntlig information kan vara skyddsvärd eller sekretessbelagd.
- Endast öppen information får kommuniceras hörbart utanför arbetsplatsen. Det är viktigt att ta hänsyn till vid exempelvis telefonsamtal på tåget, hemma eller diskussioner med arbetskamrater på platser som inte är arbetsplatsen.
- Om du har ett möte där känslig information behandlas behöver du säkerställa att endast behöriga mötesdeltagare deltar på mötet. För möten som avhandlar Strikt konfidentiell information ska ett säkert digitalt mötessystem användas.

5.4 E-post

E-post är för många medarbetare det vanligaste och viktigaste sättet att kommunicera internt inom kommunen och till externa parter. Det är dock viktigt att tänka på att kommunikation med e-post normalt sett är helt öppen. Att sända e-post som inte är skyddad, till exempel med kryptering, kan jämföras med att skicka ett vykort. Användaren är alltid ansvarig för den e-post som skickas från sitt e-postkonto. E-postkonton som delas av flera, till exempel myndighetsbrevlådor och funktionsbrevlådor ska ha utpekade ansvariga. Den som är ansvarig för en delad brevlåda ska säkerställa att alla användare har utbildning i hur brevlådan ska hanteras. E-postkontot är som ovan nämnts offentlig.

5.5 Teams

Teams är ett värdefullt verktyg för kommunen. Det möjliggör samarbete och är ett praktiskt sätt att diskutera, chatta och förvara filer. Men vi måste alltid tänka oss för vilken information som vi hanterar i Teams då informationen som hanteras där alltid

delas med andra. Teams är inte en lagringsplats för personlig information.

5.6 Internet och sociala medier

Tänk på vilken information du delar på internet och i sociala medier. Du får inte sprida upphovsrättsskyddat material eller känslig information. För material som används i tjänsten får nedladdning och installation av upphovsrättsligt skyddat material inte ske utan lagligt stöd eller skriftligt tillstånd från rättighetsinnehavaren. Aktiviteter och uttalanden på internet kan påverka både allmänhetens uppfattning om den enskilda tjänstepersonen och kommunen som organisationen. Som representant för kommunen har du ett ansvar att agera med gott omdöme på internet och sociala medier. Publicera därför inget något som är oärligt, osant, vilseledande eller kränkande. All kommunikation från kommunens datorer ska vara öppen, saklig och etisk, oavsett om kommunikationen sker i privat syfte eller inte. I enlighet med kommunens värdegrund är det inte tillåtet att besöka webbplatser med till exempel brottslig verksamhet, rasism, diskriminering, extrempolitiskt eller pornografiskt innehåll.

5.7 Säkerhetskopiering

Det är viktigt att information lagras på ett sådant sätt att den görs möjlig att återskapa om den avsiktligt eller oavsiktligt skulle bli raderad. Information som används i verksamheten ska lagras på godkända lagringsplatser så att informationen säkerhetskopieras. Om information har gått förlorad, exempelvis om man av misstag råkat radera ett dokument av värde, ska IT-supporten kontaktas för att kontrollera om möjlighet finns att återskapa den senaste säkerhetskopian.

6 Mobila enheter

Mobila enheter som mobiltelefoner, bärbara datorer och surfplattor är nödvändiga arbetsredskap men innebär även risker. Eftersom de är uppkopplade till nätverk kan de utnyttjas av angripare för att stjäla lösenord eller infektera nätverket med skadlig kod. Malå kommun äger både de mobila enheterna som används i tjänsten och den information som lagras på dem. Användare ska vara medvetna om att kommunen har rätt att granska informationen på enheterna och att allmänheten kan begära ut information enligt offentlighetsprincipen. För att säkerställa kommunens informationssäkerhet måste alla mobila enheter skyddas genom åtgärder:

- Skydda enheter med lösenord och aktivera flerfaktorsautentisering där det är möjligt
- Automatiskt skärmlås ska vara aktiverat
- Pinkod ska användas. Enkla pinkoder som 0000, 1234, ska inte användas
- Använd kommunens mobila enheter för arbete, ej för privat bruk
- Använd endast godkända applikationer för att minska risken för skadlig kod,
- Låna inte ut kommunens mobila enheter till någon
- Ändra inte de uppsatta säkerhetsinställningarna i enheterna
- Anmäl förlust av enheten omgående till den som tilldelat dig enheten
- Återlämna mobila enheter till arbetsgivaren vid anställningens slut eller vid byte till en annan enhet.

7 Lösenordshantering

Lösenord används för att logga in till de flesta av kommunens informationssystem. Lösenord ska därför hanteras som en värdehandling. De ska skyddas mot obehörig åtkomst och lagras på ett säkert sätt. Ett lösenord ska innehålla minst 12 tecken, varav versal och siffra ska användas. Det ska inte gå att gissa sig till eller ha någon anknytning till dig personligen.

Använd gärna lösenordsfraser, en lösenordsfras är ett lösenord som består av flera ord i följd, vilket gör det längre, säkrare och lättare att komma ihåg än ett kort och krångligt lösenord.

Här är exempel på lösenordsfraser som är exakt 12 tecken långa och som innehåller siffra, versal och specialtecken (endast som exempel – skapa alltid egna):

Sol-Husen9!?
Fisk@Bord8#X
Bok+Stenar4!
Lampa_Rum7?X
Mus!Havre2-Q

- Lösenord du använder i tjänsten ska inte vara samma som du använder privat.
- Lösenord får inte återanvändas vid byte.

8 Skadlig kod (virus)

Kommunen har implementerat programvaror för viruskontroll och genomför kontinuerliga kontroller i nätverket för att hantera det växande hotet av skadlig kod. Skadlig kod kan installeras på datorer eller nätverk utan administratören eller användarens vetskap i syfte att störa IT-system eller obehörigt samla in information. Användare behöver vara medveten om risken för skadlig kod och olika angreppssätt och hur man ska agera vid misstanke om enheten man arbetar vid har blivit utsatt. Om du misstänker att du blivit utsatt för skadlig kod ska du omedelbart kontakta IT-support och avvakta vidare instruktioner.

9 Spårbarhet och loggning

Alla aktiviteter i kommunens datorer, nätverk och IT-system loggas. Loggarna används för felsökning och utredning av incidenter och störningar eller för att förhindra brott. Loggar lagras under en viss tid, och är åtkomliga endast för en begränsad grupp administratörer. Spårbarhet innebär att man genom loggning kan identifiera vem som har gjort vad och när och följa förloppet för olika händelser i datorer, informationssystem och passersystem. All Internettrafik och e-post loggas centralt. Malå kommun har som arbetsgivare rätt att, vid misstanke om brott eller oegentligheter, gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning och riktlinjer. Vid misstanke om brott kan loggfilerna komma att lämnas ut för extern utredning, exempelvis vid polisanmälan då incidenten faller under brottsbalken.

10 Användning av Artificiell Intelligens (AI)

AI-tjänster på internet kan användas som stöd i arbetet, men innebär risker för informationssäkerhet och integritet. Kommunen tillhandahåller i dagsläget ingen egen AI-tjänst, det innebär att eventuella AI-tjänster som finns fritt tillgängliga på internet används på eget initiativ och ansvar.

Vid användning av externa AI-tjänster gäller följande:

- Du får inte lägga in information som ägs av kommunen, till exempel handlingar, interna dokument, arbetsmaterial eller uppgifter om verksamheten.
- Du får inte lägga in personuppgifter eller annan känslig information.
- Utgå från att information som matas in kan sparas och användas av tjänsteleverantören.
- Resultat som genereras av AI ska alltid granskas kritiskt. Du som medarbetare ansvarar för att innehållet är korrekt, lämpligt och förenligt med gällande lagar och interna riktlinjer innan det används i kommunens verksamhet.
- AI-tjänster får inte användas som underlag för beslut som påverkar enskilda personer eller vid myndighetsutövning.

Vid osäkerhet ska du avstå från att använda AI-tjänsten och i stället kontakta chef eller ansvarig funktion.

Du kan läsa mer om detta i Anvisning – för användare av AI.

10 Fysisk säkerhet

10.1 Tillträde till våra lokaler

Alla medarbetare har ett ansvar för att säkerställa att endast behörig personal vistas i våra lokaler. Det är viktigt inte minst ut ett informationssäkerhetsperspektiv, men även när det kommer till en trygg och säker arbetsplats för alla.

Inhyrd personal, exempelvis konsulter med längre uppdrag eller Arbetsförmedlingen som hyr plats på kommunhuset tilldelas passerkort med rätt tillträdesbehörighet.

All annan personal som har ett behov av tillträde, bedöms från fall till fall av Säkerhetsskyddschef, eller i dennes frånvaro biträdande säkerhetsskyddschef.

10.1.1 Besökare

Gäster och kunder anmäler sig i Kontaktcenter, som i sin tur meddelar tjänsteperson som ska besökas. Därefter hämtar berörd tjänsteperson sin gäst/kund i entrén. Efter besöket följer tjänsteperson besökaren ut igen.

10.1.2 Säkerhetszoner

Våra lokaler är tillträdesbegränsade och skyddas av elektroniska lås.

På dessa dörrar förs det logg av passager. Det vill säga att det finns en spårbarhet om något skulle inträffa som behöver kollas upp. Det är ansvarig chef som tilldelar behörighet till medarbetare.

10.2 Nycklar och passerkort

Passerkort är en personlig värdehandling och ska hanteras som det. Det är aldrig tillåtet att låna ut ett passerkort eller nyckel, du är personligen ansvarig för den skada som uppstår om du lånar ut dina nycklar eller passerkort.

10.3 Din arbetsplats

- När arbetsplatsen lämnas ska datorn alltid vara låst. Ett enkelt sätt att göra det är att trycka windowstangenten + L
- Lösenord eller konfidentiell information-får inte lämnas framme.
- Papper och flyttbara lagringsmedia (till exempel USB-minnen) med konfidentiell information ska hanteras så att ingen obehörig kan ta del av innehållet.

11 Distansarbete

Regler för distansarbete finns att läsa i personalhandboken i HUMA – Anvisning Distansarbete