# Riktlinjer för informationssäkerhet

## För medarbetare och förtroendevalda

Beslutande instans: Kommunstyrelsen

Beslutsdatum och -paragraf: ÅÅÅÅ-MM-DD §

Dokumentansvarig: Informationssäkerhetssamordnare

Revideras av: Kommunstyrelsen

Dokumentet riktar sig till: Medarbetare, förtroendevalda och extern personal

Giltighetstid: Tills vidare

Diarienummer: KS 2024/208

# Innehåll

# 1. Inledning

Dessa riktlinjer beskriver det ansvar du som medarbetare, förtroendevald eller extern personal har vid hantering av information i Skara kommun. Riktlinjen innehåller på sina ställen även regler som du som medarbetare, förtroendevald och extern personal har att förhålla dig till när du hanterar Skara kommuns information.

Riktlinjerna vänder sig till alla medarbetare och förtroendevalda i Skara kommun. De gäller även extern personal som har åtkomst till Skara kommuns information, exempelvis inhyrda konsulter.

Observera att din förvaltning/avdelning/enhet kan ha mer detaljerade anvisningar eller rutiner avseende sådant som tas upp i de här riktlinjerna.

## 1.1. Vad är informationssäkerhet?

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för vår information.

Information finns överallt i en organisation. Den är en av kommunens viktigaste tillgångar och en förutsättning för att våra verksamheter ska fungera. Information kan förekomma i olika former – den kan vara muntlig, skriftlig eller finnas i IT-system. Information förekommer främst i form av text – men även bilder, symboler, filmer och ljud utgör information. Viss information är känslig och måste skyddas så att obehöriga inte kan ta del av den. Det handlar ofta om hänsyn till den personliga integriteten och att undvika att enskilda individer kommer till skada.

Informationssäkerhet bygger på tre grundprinciper:

| | |
|---|---|
| **Konfidentialitet** | att information endast finns tillgänglig för behöriga. |
| **Riktighet** | att information är korrekt, aktuell, fullständig och inte kan ändras av obehöriga. |
| **Tillgänglighet** | att information finns tillgänglig för behöriga när den behövs. |

## 1.2. Så skyddar vi vår information

Information kan skyddas på flera olika sätt – tekniskt, fysiskt och administrativt.

- **Tekniskt skydd** kan vara till exempel brandväggar (det vill säga program som skyddar datornät eller enskilda datorer från intrång och attacker via internet) eller behörighetsstyrning i ett verksamhetssystem (IT-system).

- **Fysiskt skydd** kan vara till exempel skalskydd på en byggnad eller nycklar eller passerkort till dörrar, lås och skåp.

- **Administrativt skydd** kan vara till exempel regler och rutiner (som dessa riktlinjer!).

    - En typ av administrativt skydd är **utbildning.** Genom utbildning ökar vi vår medvetenhet, får kunskap om hur vår information får hanteras och lär oss hur vi ska tillämpa våra säkerhetsåtgärder.

**Kunskap är makt!**
Kommunen har tillgång till utbildningar och utbildningsmaterial inom informationssäkerhet. Gå in på intranätet eller fråga din chef om du vill veta mer!

## 1.3. Du är viktig!

Säkerhet är inte starkare än den svagaste länken. Därför är informationssäkerheten i Skara kommun beroende av hur du som medarbetare och förtroendevald hanterar kommunens information och hur du förhåller dig till de säkerhetsåtgärder som omfattar informationen.

Det spelar nämligen ingen roll hur många säkerhetsåtgärder vi inför i våra verksamhetssystem om du ändå lämnar ut dina inloggningsuppgifter, och det spelar ingen roll hur många låsta dörrar vi har till våra lokaler om du ändå släpper in obehöriga. Att sådana handlingar oftast görs omedvetet hjälper dessvärre inte – informationssäkerheten påverkas oavsett om du begår misstag eller gör någonting medvetet.

Men! Det är inte lätt att alltid göra rätt. Därför är det av största vikt att du har de rätta förutsättningarna för att kunna uppträda på ett så säkert sätt som möjligt. Syftet med de här riktlinjerna är att ge dig dessa förutsättningar.

Vid frågor och funderingar, kontakta informationssäkerhetsstödet på din förvaltning, alternativt kommunens informationssäkerhetssamordnare.

## 1.4. Informationssäkerhetsförbindelse

I samband med att du anställs, blir förtroendevald eller anlitas som konsult i kommunen ska du underteckna en informationssäkerhetsförbindelse. Denna förbindelse är utgångspunkten för de informationssäkerhetsrelaterade regler du förväntas följa under din tid i kommunen.

# 2. Säkert beteende

I stort sett all kommunens information hanteras muntligt, fysiskt eller digitalt. Det viktigaste du som medarbetare och förtroendevald kan bidra med för att hålla informationen skyddad är att ha ett medvetet och säkert beteende. Då kan du, likt en fysisk brandvägg, på ett effektfullt sätt skydda kommunens information.

## 2.1. Skydda muntlig information

- Tänk på vad du delar med dig av och till vem. Endast den som är behörig ska ha åtkomst till känslig eller sekretessbelagd information.

- Välj ett avskilt rum eller gå undan för att vara säker på att obehöriga inte kan ta del av fysiska samtal, telefonsamtal eller videosamtal där känslig eller sekretessbelagd information hanteras.

- Välj *Säkra möten (TDirect Säkra Meddelande)* om du ska ha samtal eller möten där känslig eller sekretessbelagd information ska hanteras. Läs mer om detta i avsnitt 8.1.3.

- Stäm av med Göliska IT om du blir inbjuden till ett videomöte och du är osäker på om det är ett säkert videomötessystem.

## 2.2. Skydda digital information

- Lås alltid datorn när du lämnar den, även om det bara är för en kort stund.

  Kortkommando:  eller 
  

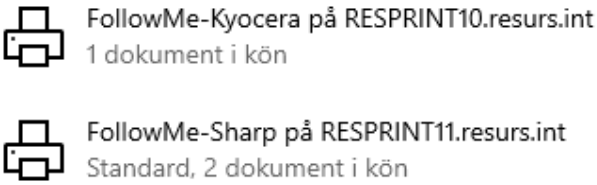
- Lås alltid smarttelefon eller surfplatta när du inte ska använda den.

- Om du har en säkerhetsnyckel för att logga in i olika system så ska det skyddas, lämna till exempel aldrig ett kort i datorn.

- Du får inte skicka känslig eller sekretessbelagd information med vanlig e-post. Om du behöver dela med dig av sådan information kan du istället använda dig av tillägget *Säkra meddelanden* i Outlook. Läs mer om detta i avsnitt 8.1.3.

- Du får inte scanna dokument som innehåller känslig eller sekretessbelagd information till en e-postadress, utan dessa ska enbart hanteras genom funktionen *Säker scanning* direkt till ett verksamhetssystem eller till en säker behörighetsstyrd mapp (P:\Gem\Skanning).

- Vid utskrift av dokument ska du använda tjänst för säker utskrift (t.ex. *FollowMe*). Då skrivs dina utskrifter inte ut förrän du själv loggar in med tagg eller lösenord på skrivaren. På det sättet minskar risken att dina utskrifter plockas upp av någon annan eller kan läsas av någon som inte har rätt till det.




- Internt skriftligt material på papper eller skärm får inte hanteras eller lämnas så att obehöriga kan läsa den. Låt till exempel ingen läsa över din axel eller ta del av information genom ett fönster eller bilrutan. Placera din datorskärm så att ingen obehörig kan ta del av informationen på den.

> ***Tips!***
> Om du hanterar skriftligt material på skärm i miljöer där det kan vara svårt att hindra obehöriga från att se skärmen kan du be din chef beställa ett sekretessfilter att sätta över skärmen. Med ett sådant kan innehållet på din skärm endast läsas av den som sitter rakt framför den.

## 2.3. Skydda fysisk information

- Lås in material som innehåller känslig eller sekretessbelagd information när du inte använder den.

- Du får inte låta besökare vistas utan uppsikt i lokaler där känslig eller sekretessbelagd information kan finnas.

- Om brev innehåller känslig eller sekretessbelagd information ska du vid fysisk posttjänst använda dig av rekommenderad försändelse.

- Undvik att använda fax. Om känslig eller sekretessbelagd information måste överföras via fax ska du försäkra dig om att du har rätt nummer och att mottagarens fax är övervakad under hela tiden överföringen sker.

- När känslig eller sekretessbelagd information i pappersform ska kasseras ska du se till att den förstörs på godkänt sätt. Det kan till exempel göras genom strimling eller genom att den kastas i godkända säkerhetskärl.

# 3. Användaridentitet och lösenord

## 3.1. Personligt användarkonto i kommunens administrativa nätverk

När du anställs, anlitas eller blir förtroendevald i kommunen tilldelas du ett personligt användarkonto med tillhörande lösenord i Göliska IT:s gemensamma inloggningstjänst. Detta är din *användaridentitet*. Den är kopplad till just dig och du behöver den för att du ska komma åt dina individuella resurser, såsom e-post och dokument. Du är ansvarig för allt som händer ”i ditt namn”.

**Läs mer här:**

Hur du ska skapa och hantera lösenord kopplat till din användaridentitet i kommunens system kan du läsa om i instruktionen *Riktlinje för lösenord – personligt användarkonto (ADM)*. Finns på Skara kommuns och Göliska IT:s webbplats.

## 3.2. Personligt användarkonto i förvaltningsspecifika verksamhetssystem

Om du har ett personligt användarkonto i ett för din verksamhet förvaltningsspecifikt verksamhetssystem ska du följa reglerna för utformning av användarnamn och lösenord som gäller för just det systemet.

## 3.3. Lösenord eller tvåfaktorsauktorisering

Beroende på vilken information som hanteras i ett system så används **lösenord** eller **tvåfaktorsautentisering**.

### 3.3.1. Lösenord

I alla situationer där du skapar och hanterar lösenord ska du tänka på följande.

- Ett lösenord ska så långt som möjligt vara ”starkt” och innehålla minst 8 tecken. Blanda små och stora bokstäver, siffror och specialtecken.

- Lösenord är strängt personliga. Lämna därför aldrig ut ditt lösenord! Skriv inte upp lösenordet och låt inte någon se när du loggar in. Dela inte lösenord med andra.

- Du bör inte använda samma lösenord för olika tjänster. Använd inte samma lösenord i jobbet som du har privat. Återanvänd inte hela eller delar av tidigare lösenord. Byt lösenord ofta.

- Låt inte externa webbsidor spara lösenordet. Får du frågan om lösenordet ska sparas, svara alltid nej.

- Undvik ”säkerhetsfrågor” vid lösenordshantering. De kan fungera som bakdörr till kontot.

### 3.3.2. Tvåfaktorsautentisering

Tvåfaktorsautentisering, eller tvåstegsinloggning, innebär att det krävs något mer än bara lösenordet för att logga in. Det medför att det blir betydligt svårare för någon obehörig att logga in på dina konton.

Tvåstegsautentisering ökar säkerheten genom att den ställer krav på att man vid inloggning, utöver lösenord, måste använda något av följande:

- **”Något du vet”:** till exempel en kod via sms eller krav på att besvara en säkerhetsfråga.
- **”Något du har”:** ett fysiskt föremål som kan användas som autentisering, till exempel ett kort eller en dosa.
- **”Något du är”:** biometrisk data – som till exempel fingeravtryck eller ansiktsigenkänning.

Vid tvåfaktorsautentisering i Skara kommun och i V6-kommunerna använder du dig av en säkerhetsnyckel (”något du har”). Det finns tre säkerhetsnycklar att använda. De är SITHSkort, Feitian-nyckel och BankID/Mobilt BankID.

Följ regelverken för respektive säkerhetsnyckel. Läs mer om de olika säkerhetsnycklarna i rutan nedan.

**Mer om säkerhetsnycklar**

**SITHS-kort**
SITHS är en elektronisk identitetshandling som används för säker identifiering av både personer och system inom regioner, kommuner, privata vårdgivare och statliga myndigheter. SITHS används till exempel vid inloggning i tjänster, för elektronisk signering och för säker kommunikation mellan system.

**Feitian-nyckel**
En Feitian-nyckel är en säkerhetsnyckel i form av en hård liten bricka som används för säker inloggning. Vid inloggning via en mobil enhet lägger användaren brickan eller nyckeln mot baksidan av telefonen och skriver därefter sitt användarnamn eller lösenord.

**BankID**
BankID/Mobilt BankID är en e-legitimation. En e-legitimation kan jämföras med en fysisk ID-handling som till exempel ID-kort eller körkort. Den enda skillnaden är att du använder e-legitimationen för att legitimera dig digitalt, till exempel på internet.

# 4. Åtkomst och behörigheter

Som anställd eller förtroendevald i Skara kommun är det viktigt att du har åtkomst (behörighet) till den information som är nödvändig för att du ska kunna utföra ditt jobb eller uppdrag.

Den information som du har åtkomst till har du ansvar för att behandla på ett säkert sätt. För att du inte ska behöva ta ansvar för information som inte behövs för att du ska kunna utföra dina arbetsuppgifter eller ditt uppdrag ska du därför inte heller ha åtkomst till sådan information. Ditt passerkort ska till exempel inte ge dig tillträde till utrymmen du inte behöver vistas i och du ska inte kunna läsa information i ett verksamhetssystem som inte är relevant för dig.

## 4.1. Behörighetsnivåer

Mycket av kommunens information finns i olika verksamhetssystem. Ett system kan innehålla alltifrån allmänna, offentliga handlingar till handlingar som lyder under strikt sekretess. På samma sätt kan fysiska utrymmen innehålla olika typer av information. Ett läkemedelsrum innehåller till exempel mer känslig information än kafeterian i stadshuset. Därför behöver system och utrymmen vara indelade i så kallade behörighetsnivåer, så att det går att säkerställa att informationen som finns där endast behandlas av den som behöver och får behandla den. Det är ägaren till informationen – det vill säga oftast en chef – som bestämmer vilka behörighetsnivåer som ska finnas i respektive system eller utrymme.

Som medarbetare är det din anställning och dina arbetsuppgifter som utgör grunden för de behörigheter du behöver ha. Det är din chef som ansöker om behörigheter för dig.

För dig som förtroendevald är det ditt politiska uppdrag som utgör grunden för de behörigheter du behöver ha.

## 4.2. Behörigheter ska följas upp

Om ditt uppdrag eller din anställning ändras ska även dina behörigheter justeras, så att de motsvarar dina nya behov av åtkomst.

Din chef ansvarar för att minst en gång om året se över dina arbetsuppgifter och/eller ditt uppdrag och bedöma vilka åtkomster och behörigheter du behöver för att kunna utföra dem. Inom vissa verksamheter finns det rutiner för att kontrollera behörigheter oftare än en gång om året.

# 5. Hantering av IT-utrustning – hur får jag använda min dator och telefon?

Som anställd eller förtroendevald i kommunen ska du ha tillgång till den IT-utrustning som krävs för att du ska kunna utföra ditt arbete eller uppdrag. IT-utrustning (en ”enhet”) kan vara stationär och/eller mobil och beställs av chef eller verksamhetsansvarig.

Exempel på IT-utrustning i form av mobila enheter är bärbara datorer, smarttelefoner, surfplattor och USB-minnen.

IT-utrustning som tillhandahålls av kommunen får inte lånas ut eller överlåtas, om det inte är utrustning som delas av flera.

## 5.1. Hur får jag hantera kommunens information i mina privata enheter?

**Du bör inte hantera kommunens information i dina privata enheter.** Du bör till exempel inte synkronisera din e-post i arbetet eller ladda ner kommunens Teams- eller OneNote-konto till din privata mobiltelefon. Detta beror på att din privata telefon inte har kommunens säkerhetslösningar installerade och att du på din privata telefon kan ha laddat ner appar eller besökt internetsidor som utgör risk för övrig information på din telefon.

Om du behöver ansluta dina privata enheter till nätverk på arbetsplatsen får du ansluta dig till kommunens gästnät.

### Mer om appar och insamlande av information

En app du laddar ner behöver oftast samla in information från din enhet för att kunna fungera i enlighet med sitt syfte. En kompass-app behöver till exempel ha tillgång till enhetens platsinformation, en bildredigerings-app behöver ha tillgång till dina bilder och en inspelnings-app behöver ha tillgång till din mikrofon. Ibland är vissa appar utformade så att de även samlar in information som inte är strikt nödvändig för appens funktionalitet. Ibland delar apputvecklaren med sig av den information som inhämtas till en tredje part.

Tik-Tok är ett exempel på en app som samlar in och delar med sig av en mängd information från sina användare. Flera offentliga arbetsgivare i Sverige har av den anledningen förbjudit sina anställda att ha Tik-Tok installerat i sina tjänstetelefoner.

Läs mer om hur du för kommunens räkning får använda sociala medier såsom Tik-Tok i avsnitt 7.2.

## 5.2. Kommunens enheter

### 5.2.1. Inställningar

- Du får inte ändra eller ta bort säkerhetsinställningar i kommunens enheter.

- Programvara (t.ex. Office-paketet) som finns installerad på kommunens enheter är endast avsedd för kommunens enheter. Du får inte utan särskilt tillstånd kopiera eller installera den på dina privata enheter.

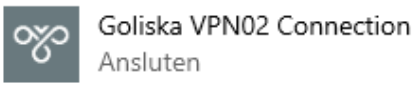
### 5.2.2. Autentisering och lösenord

- Du ska låsa dina mobila enheter med lösenord.

- Till smarttelefoner och surfplattor ska du använda pinkoder, fingeravtryck, Face ID, eller annan personlig autentisering.

### 5.2.3. Uppkoppling och anslutning

- Kommunens datorer är försedda med VPN (virtuellt privat nätverk), vilket skapar en krypterad anslutning till internet. Detta får du inte ta bort.




- Du får endast ansluta av kommunen godkända enheter och programvaror till kommunens interna nät (STAP).

- Var mycket försiktig med att ansluta dig till öppna trådlösa nätverk. Det är lätt för obehöriga att läsa av trafiken. Koppla hellre upp dig mot din smarttelefons nätverk (”Internetdelning”).

- Var mycket försiktig när du kopplar in kringutrustning, till exempel USB-minnen och kameror. Du ska helst undvika användning av USB-minnen.

### 5.2.4. Förlust av mobil enhet

- Om du tappar bort en mobil enhet ska det rapporteras och hanteras som en informationssäkerhetsincident enligt kommunens rutiner. Se kapitel 13.

- I vissa fall finns det möjlighet att fjärradera information – kontakta Göliska IT (0771-77 70 00).

### 5.2.5. Särskilt om din tjänstetelefon eller -surfplatta

Om du använder din tjänstetelefon eller -surfplatta för privat bruk är det viktigt att du säkerställer att ditt privata användande inte utgör en risk för kommunens information. Du bör av den anledningen vara restriktiv med vilka programvaror (t.ex. appar) du laddar ner på din tjänstetelefon. Appar kan samla in mer information än nödvändigt från telefonen och i vissa fall dela med sig av den till en tredje part. Läs mer om appar i rutan i avsnitt 5.1.

Om du har en tjänstetelefon eller -surfplatta som är kopplad till MDM-systemet kan du använda den mer fritt. Se mer information i rutan nedan.

#### Mer om MDM-styrda enheter

Att koppla en mobiltelefon eller en surfplatta till ett MDM-system innebär att kommunen (genom Göliska) kan skapa två separata delar i telefonen – en som kommunen/Göliska har kontroll över och en som kan användas helt privat. Informationen som ligger i den del som kan kontrolleras av Göliska är då helt avskild från övrig information på telefonen. På det sättet minskar kommunen riskerna med privat användning av tjänstetelefoner.

Med den MDM-styrda delen av telefonen kan Göliska göra följande:

- Låsa telefonen om den tappats bort eller misstänks ha stulits.
- Fjärradera informationen på telefonen.
- Styra vilka appar som kan laddas ner och användas.

**Särskilt om fjärradering**
Om Göliska behöver fjärradera informationen på din telefon eller surfplatta (vid till exempel avslut av anställning eller om du tappat bort den) kommer *samtlig* information på enheten raderas. Även den information du har i din privata del av telefonen eller surfplattan.

För att inte riskera att bli av med din privata information är det därför viktigt att du har fungerande säkerhetskopiering av informationen i den privata delen av enheten.

**Särskilt om appar i MDM-systemet**
I den delen av enheten som kontrolleras av Göliska kontrollerar kommunen (via Göliska) vilka appar som får och inte får laddas ner på enheten. På det sättet minskar man risken för nedladdning av appar som riskerar att samla på sig och dela med sig av kommunens information.

I den privata delen av telefonen finns det inga begränsningar på vilka appar du kan ladda ner.

**OBS!** Vissa förinstallerade appar, såsom ”Bilder” delas av både den delen som Göliska kontrollerar och den privata. Detta gör att du inte får ta arbetsrelaterade bilder som innehåller sekretesskyddade eller på annat sätt känsliga uppgifter med din telefon eller surfplatta, även om den är kopplad till MDM-systemet.

# 6. Distansarbete

Vid distansarbete är risken att du exponerar känslig information större än när du arbetar på arbetsplatsen. När du arbetar på distans behöver du därför vara extra medveten om vilken typ av information du hanterar, så att du hanterar informationen på ett korrekt sätt även då.

**Observera!**
Du får i publika miljöer aldrig hantera information som är konfidentiell enligt säkerhetsskyddslagen.

## 6.1. IT-utrustning och uppkoppling vid distansarbete

För att du ska komma åt kommunens resurser (t.ex. verksamhetssystem) vid distansarbete krävs det att du har tillgång till IT-utrustning, programvaror och behörigheter enligt kommunens standard.

Även om du befinner dig utanför kommunens nätverk är kommunens datorer alltid uppkopplade mot VPN (se avsnitt 5.2.3). Det innebär att din kommunikation är skyddad, men det innebär inte att din dator är skyddad från intrång utifrån. Det är därför viktigt att du undviker öppna trådlösa nätverk (på till exempel restauranger och hotell) och att det nätverk du använder är tillräckligt säkert för att inte skapa en risk för den tekniska säkerheten. Använd hellre funktionen med internetdelning på din arbetstelefon eller surfplatta.

Lämna aldrig IT-utrustning olåst eller utan uppsikt!

Beakta i övrigt vad som står i kapitel 5, om hantering av mobila enheter.

**Läs mer här**

Läs mer om distansarbete i Skara kommuns rutin *Rutin för distansarbete.*

# 7. Internet och sociala medier

Genom att använda internet och sociala medier har kommunen möjlighet att kommunicera med våra medborgare och nå ut med information.

Användning av internet och sociala medier är emellertid inte riskfritt, utan för med sig risk för informationssäkerheten. För att användningen inte ska utgöra ett oacceptabelt hot mot verksamheten krävs därför att du som medarbetare och förtroendevald agerar på ett säkert sätt när du använder dem.

## 7.1. Användning av internet

När du använder internet gäller de lagar och regler som gäller i samhället i övrigt. Du har till exempel fortfarande rättigheter och skyldigheter enligt tryckfrihetsförordningen, kan begå brott enligt brottsbalken och bryta mot lagen om upphovsrätt och dataskyddsförordningen.

Du ska vara försiktig med vilka webbplatser du besöker och får inte besöka webbplatser med innehåll som kan väcka anstöt eller på annat sätt är olämpliga, såsom hemsidor med pornografiskt, rasistiskt eller brottsligt innehåll. Tänk på att loggfiler med information om din datatrafik, det vill säga information om hur du använt internet, är en allmän handling som kan begäras ut av allmänheten.

På internet får du endast publicera och dela information som finns i offentliga allmänna handlingar (det vill säga uppgifter som inte omfattas av sekretess).

**Läs mer här**

Läs mer om allmänna handlingar i *Riktlinjer för dokument- och ärendehantering i Skara kommun.*

## 7.2. Användning av sociala medier

Användning av sociala medier för kommunens räkning ska ske på uppdrag av chef och i enlighet med kommunens riktlinjer för kommunikationskanaler och grafisk profil. Vid användandet ska du alltid beakta informationssäkerhetsaspekterna genom att säkerställa att:

- du inte tappar kontrollen över den information du publicerar (tillgänglighet),
- du inte publicerar felaktig information och att den information du publicerar inte kan ändras av någon obehörig (riktighet),
- du inte publicerar mer än det du avsett och att du inte delar med dig av sådant som enligt lag eller av andra anledningar inte ska delas med andra (konfidentialitet).

Vid användning av sociala medier är det, som i alla situationer, viktigt att du tar hänsyn till det skydd för personuppgifter som finns reglerat i dataskyddsförordningen (GDPR). Bilder/fotografier där det går att identifiera en person är ett exempel på personuppgifter som har detta skydd.

### Särskilt om sociala medie-appar

När du publicerar innehåll på sociala medier ska du vara försiktig med vilka appar du använder och hur du använder dem. Se mer om detta i avsnitt 5.1. Om du till exempel behöver använda appar som Tik-Tok i tjänsten ska du göra det via en mobiltelefon som är avskild från kommunens övriga information. Kontakta enheten för HR och kommunikation.

**Läs mer här**

Läs mer om hur du ska göra vid användande av sociala medier i *Riktlinjer för kommunikationskanaler och grafisk profil.*

Läs mer om behandling av personuppgifter i kommunens styrande dokument avseende GDPR.

# 8. E-post och kalender

E-post är för många medarbetare det vanligaste sättet att kommunicera internt inom kommunen och med externa parter. Kalenderbokningar i Outlook är det vanligaste sättet att boka in möten på.

## 8.1. E-post

Du som enskild medarbetare eller förtroendevald är alltid ansvarig för den e-post som skickas från ditt personliga e-postkonto och du ansvarar för att hantera inkommande e-post enligt kommunens rutiner.

### 8.1.1. E-post är allmänna handlingar

E-post som skickas till personliga brevlådor inom kommunen är i stort sett alltid allmänna handlingar och ska hanteras enligt gällande rutiner för detta.

**Läs mer här**

Läs mer om hantering av allmänna handlingar i *Riktlinjer för dokument- och ärendehantering i Skara kommun.*

### 8.1.2. Privat e-post

Du ska undvika att använda ditt e-postkonto i kommunen för privata ändamål. Du bör också undvika att använda ditt privata e-postkonto för arbets- eller uppdragsmaterial. Se mer i avsnitt 5.1.

Det är inte tillåtet att automatiskt vidarebefordra e-post till privata e-postadresser.

### 8.1.3. Skicka känslig eller sekretessbelagd information digitalt

Du får inte skicka känslig eller sekretessbelagd information med vanlig e-post. Om du behöver dela med dig av sådan information kan du istället använda dig av tillägget *Säkra meddelanden*. Därigenom kan du kommunicera känslig och sekretessbelagd information internt i kommunen, till andra myndigheter och till medborgare. För att använda systemet behöver du (och mottagaren) logga in med en tvåfaktorsinloggning (t.ex. BankID).

Om du tillfälligt behöver lagra information du ska skicka med Säkra meddelanden kan du använda dig av den så kallade T:-katalogen. Läs mer i avsnitt 9.2.

Om du ska scanna känslig eller sekretessbelagd information ska du använda dig av *Säker scanning*. Se avsnitt 2.2.

**Läs mer här**

Läs mer om hur du använder *Säkra meddelanden* och *Säkra möten* på Göliska IT:s webbplats. Sök på ”Kommunicera känslig information digitalt”.

## 8.2. Kalender

När du gör en bokning i din Outlook-kalender kan alla medarbetare som har e-postadressen skara.se se uppgifter om Ämne och Plats för bokningen. Om du dessutom använder dig av prefix såsom SAM: eller TJÄ: kan Ämne och Plats läsas av användare i samtliga Göliska-kommuner.

Detta medför att du behöver vara försiktig med vad du skriver i ämnesraden för bokningen. Du ska inte uppge mer information än du behöver. Du bör till exempel inte skriva personnamn eller andra personuppgifter.

# 9. Lagring och säkerhetskopiering

Det är viktigt att den information som finns i kommunens verksamheter är lagrad (sparad) på ett säkert sätt och att information som inte får gå förlorad kan återskapas vid en eventuell förlust. Det är därför viktigt att vi sparar den information vi hanterar på rätt ställen. Ju mer skyddsvärd eller känslig information är, desto säkrare lagringsplatser krävs. Följ aktuell dokumenthanteringsplan!

Vilket lagringsställe du ska använda i varje enskilt fall avgörs av hur stort behov av skydd informationen som ska lagras har. Om du inte vet var en viss informationstillgång (till exempel ett dokument) ska lagras – kontakta din chef.

## 9.1. Allmänt om hantering och lagring av information

Du får överhuvudtaget inte *hantera* känslig eller sekretessbelagd information på **smarttelefon eller surfplatta** om du inte använder en av kommunen särskilt godkänd säkerhetslösning. Förtroendevaldas surfplattor är som huvudregel utrustade med en sådan säkerhetslösning.

Du får inte *lagra* känslig eller sekretessbelagd information på **mobila enheter** (om mobila enheter, se kapitel 5). Lagra den istället i aktuellt verksamhetssystem.

Du får inte *lagra* information på ställen **som inte säkerhetskopieras**.

## 9.2. Lagringsställen

Nedan följer en tabell med exempel på lagringsställen som finns i kommunen.

| Lagringsplats | Säkerhets-kopieras? | Får användas för att spara information? | Får användas för att spara känslig eller sekretessbelagd information? | Övrigt |
|---|---|---|---|---|
| **"Molnet"** OneDrive (M365) | Ja | Ja | Nej | Gäller samtliga M365-applikationer |
| **Verksamhetssystem** T.ex. Lifecare, Evolution, Raindance | Ja | Ja | Ja | Följ instruktionerna för respektive verksamhetssystem |
| **Den här datorn Mina dokument Skrivbordet** | Ja | Ja | Ja | Endast åtkomligt för den enskilda användaren |
| **P:-katalogen på datorn** | Ja | Ja | Ja | Tänk på att andra kan ha tillgång till dina P:-mappar |
| **C:-katalogen på datorn** | Nej | Ja, i undantagsfall | Nej | Får endast sparas här högst tillfälligt |
| **T:-katalogen på datorn** | Nej | Ja, dock högst tillfälligt (raderas efter 3 timmar) | Ja, dock högst tillfälligt (raderas efter 3 timmar) | Bra för att tillfälligt spara t.ex. säkra meddelanden |
| **USB-minnen** | Nej | Nej | Nej | Undvik USB-minnen |
| **Låsbara skåp** | Nej | Ja | Ja | |

# 10. Spårbarhet och loggning

De flesta IT-system skapar så kallade loggar. Genom loggning kan man spåra aktiviteter. Det går att identifiera vem som har gjort vad och när och följa förloppet för olika händelser. Därigenom möjliggör man till exempel incidenthantering och kan kontrollera användare för att se till att de följer lagar och interna regler.

Vid viss typ av loggning kan det du gör ”i ditt namn”, det vill säga med din användaridentitet, spåras tillbaka till dig.

Loggar är att betraktas som allmänna handlingar och kan begäras ut.

# 11. Nätfiske och skadlig kod

När du hanterar information digitalt löper du ständig risk för att utsättas för så kallat nätfiske och skadlig kod. I avsnitten nedan finns några tips på hur du kan känna igen nätfiske och hur du kan göra för att skydda dig.

**Nätfiske** är ett av de vanligaste tillvägagångssätten vid IT-relaterad brottslighet. Med nätfiske försöker brottslingen locka dig att klicka på länkar som leder till hemsidor som laddar ner skadlig kod eller som uppmanar dig att lämna olika typer av uppgifter, till exempel personuppgifter eller inloggningsuppgifter.

Oftast kommer nätfisket i form av e-postmeddelanden, men det kan också dyka upp via webbsidor, sociala medier, dropbox, som sms eller i ett telefonsamtal.

**Skadlig kod** är ett samlingsbegrepp för oönskade programvaror som exempelvis virus- och spionprogram. Dessa kan användas för att ge obehöriga tillgång till information i ett IT-system. Skadlig kod kan spridas vid öppning av bilagor i e-post, men även vid import av filer eller vid besök på olämpliga sidor på internet.

## 11.1. Nätfiske utnyttjar våra mänskliga sidor

Vid nätfiske innehåller e-postmeddelandet eller webbsidan ofta flera känslomässiga triggers. Det står att det är bråttom, att du riskerar att förlora information om du inte gör en viss uppdatering eller att ett erbjudande om pengar eller andra gåvor riskerar att upphöra.

Dessutom ser e-postmeddelandet eller informationen oftast ut att komma från en trovärdig avsändare. Det är vanligt att det är en organisation eller användare som du känner till, i ett e-postmeddelande kan det till exempel se ut som om en kollega är avsändaren. Det kan också komma från ett känt företag eller en känd organisation, exempelvis din bank eller Skatteverket.

## 11.2. Granska kritiskt

Det är viktigt att ha kritiska ögon. Ofta kan du hitta dålig stavning eller felaktig grammatik. Det kan finnas länkar som inte stämmer, länkar som till exempel omdirigerar dig till en falsk inloggning. Ställer du dig med muspekaren över en länk (utan att klicka) kan du se vilken webbadress länken dirigerar till. Du kan då bedöma om länken ser ut att leda till ett okänt eller olämpligt ställe och vid misstanke om bedrägeri avstå från att klicka på den överhuvudtaget.

## 11.3. Använd olika lösenord

En metod för att skydda sig från nätfiske och skadlig kod är att inte använda samma lösenord till flera inloggningsställen, såväl privat som på jobbet.

***Observera!***
Om du skulle råka dela med dig av uppgifter eller annan information – se till att byta lösenord omedelbart! Händelsen ska därefter hanteras som en informationssäkerhetsincident enligt kommunens rutiner. Se kapitel 13.

## 11.4. Håll dig själv och datorn uppdaterad

För att du och din dator alltid ska vara utrustad med det senaste skyddet är det viktigt att du tar del av nyheter och instruktioner från Göliska IT och att du genomför de programuppdateringar som skjuts ut därifrån.

## 11.5. Anmäl misstänkt nätfiske

Kommunen har vid ett antal tillfällen utsatts för nätfiske-attacker. Ibland generella och ibland mer riktade. Det är viktigt att vi tillsammans ser upp, granskar och anmäler misstänkt nätfiske. **Meddela alltid Göliska IT:s Servicedesk (0510-77 70 00 eller servicedesk@goliskait.se)** om du behöver hjälp att bedöma ett misstänkt mejl eller om du misstänker att du har blivit utsatt för en nätfiske-attack.

***Observera!***
Om du vet eller misstänker att nätfiske lett till att information delats med obehöriga, ändrats på ett felaktigt sätt eller gått förlorad ska du hantera det som en informationssäkerhetsincident enligt kommunens rutiner. Se kapitel 13.

**Läs mer här**

Läs mer om hur du ska hantera bluffmejl på Skara kommuns intranät. Sök på *”Hur gör jag om jag får ett bluffmejl?”*.

För mer information och tips kan du besöka MSB:s hemsida. Sök på *”Skydda dig mot nätfiske och skadlig kod”*.

# 12. Avslut av anställning eller uppdrag

Om din anställning, ditt uppdrag eller ditt avtal med kommunen ändras eller upphör ska du lämna tillbaka eller överföra de tillgångar du haft tillgång till eller hanterat under din tid i kommunen.

I detta ingår att du ska lämna tillbaka fysiska och elektroniska tillgångar, såsom dator och passerkort. Det innebär även att information i form av kunskap och erfarenhet som du har samlat på dig under din tid i kommunen ska dokumenteras och överföras till organisationen.

När du avslutar din anställning eller slutar ditt uppdrag som förtroendevald ska dina behörigheter avslutas och din åtkomst till system tas bort.

## 12.1. Lämna tillbaka fysiska och elektroniska tillgångar

Fysiska och elektroniska tillgångar som ska lämnas tillbaka när du avslutar din anställning eller ditt uppdrag är:

- användarklienter (t.ex. bärbar dator)
- bärbara lagringsenheter (t.ex. USB-minnen)
- specialistutrustning (t.ex. surfplatta, telefon)
- hårdvara för autentisering till informationssystem, platser och fysiska arkiv (t.ex. passerkort, nycklar)
- fysiska kopior av information (t.ex. papper, pärmar)

## 12.2. Överför kunskaper och erfarenheter

När du arbetar eller på annat sätt verkar inom kommunen samlar du på dig kunskaper och erfarenheter som kan vara viktiga för den fortsatta verksamheten. För att säkerställa att information inte försvinner med dig behöver du därför dokumentera och överföra relevant information innan du slutar.

Observera att det sekretessavtal du undertecknade när du anställdes eller påbörjade ditt uppdrag i kommunen även omfattar tiden efter anställningen eller uppdraget.

## 12.3. Vem har ansvaret?

Det är din chef som ansvarar för att dina tillgångar lämnas tillbaka och att dina kunskaper och erfarenheter överförs. Chefen ansvarar också för att avsluta dina behörigheter och ta bort din åtkomst till system.

# 13. Avvikelser och incidenter

En viktig del i ett välfungerande arbete med informationssäkerhet är att kommunen har tydliga rutiner för hur man ska hantera avvikelser och incidenter. Både för att säkerställa att kommunen uppfyller de lagkrav som finns på området och för att kommunen ska kunna utnyttja incidenter, felaktigheter och misstag till att ta lärdom inför det fortsatta arbetet och göra förbättringar.

En informationssäkerhetsincident är en händelse som leder till att information kommer i orätta händer, förloras eller uppdateras felaktigt.

Som medarbetare och förtroendevald i kommunen har du skyldighet att rapportera incidenter eller brister som misstänkts kunna medföra negativ påverkan på kommunens information. Även svagheter i skydd (brister) ska rapporteras. Det kan till exempel handla om larm som inte fungerar eller öppna dörrar och fönster efter kontorstid.

## 13.1. Olika typer av informationssäkerhetsincidenter

En informationssäkerhetsincident kan, utöver att vara en ”ren” informationssäkerhetsincident vara en personuppgiftsincident, en NIS-incident eller en säkerhetsskyddsincident. Hur en incident ska hanteras beror på vilken typ av incident det är fråga om samt hur allvarlig den är. Gemensamt för samtliga varianter är dock behovet av skyndsam hantering och noggrann uppföljning.

Om du upptäcker en avvikelse eller en incident ska du omgående rapportera den enligt kommunens rutiner för incidentrapportering. I de fall det föreligger akut risk för våra IT-system ska du även kontakta Göliska IT. Se avsnitt 11.5.

**Läs mer här**

Läs om hur du ska hantera avvikelser och incidenter i *Rutin för informationssäkerhet – rapportering av informationssäkerhetsincidenter.*