Informationssäkerhet för medarbetare och förtroendevalda - riktlinje



Beslutad av kommunstyrelsen 2024-03-06

Dokumentinformation

Fastställt av:	Kommunstyrelsen
Fastställt, datum:	2024-03-06
Dokumentsansvarig:	Chef säkerhetsenheten
Ansvarig för revidering:	Informationssäkerhetssamordnare
Gäller för:	Medarbetare och förtroendevalda i Lidköpings kommun
Gäller till, datum:	Gäller tills vidare. Uppdateras vid behov.

Innehållsförteckning

Informationssäkerhet för medarbetare och förtroendevalda – riktlinje 4
1 Inledning 4
2 Regler och etiska riktlinjer 4
3 Användaridentitet och lösenord 5
4 Behörigheter 5
5 Mobila enheter 6
5.1 Hantering av mobila enheter 6
5.2 Distansarbete 6
5.3 Fysisk hantering av mobila enheter 6
5.4 Särskilda regler för smarta telefoner och surfplattor 7
6 Skadlig kod 7
7 Internet och sociala medier 7
7.1 Internetanvändning 8
7.2 Användning av sociala medier 8
8 E-post 8
8.1 Ansvar 8
8.2 Allmänna handlingar 9
8.3 Privat e-post 9
8.4 E-post och känslig eller sekretessbelagd information 9
9 Lagring och säkerhetskopiering 9
10 Spårbarhet och loggning 10
11 Säkert beteende 10
11.1 Muntlig information 10
11.2 Information på skärmar och i pappersform 10
12 Skyldighet att rapportera incidenter och brister 11

Informationssäkerhet för medarbetare och förtroendevalda – riktlinje

1 Inledning

Information är en av kommunens viktigaste tillgångar och en väsentlig förutsättning för att kunna bedriva verksamheten. Kommunens informationstillgångar måste därför behandlas och skyddas på ett tillfredsställande sätt.

Informationen ska bevaras utifrån tre informationssäkerhetsaspekter:

- **Konfidentialitet:** att information enbart är tillgänglig för behöriga
- **Riktighet**: att information är korrekt, aktuell och fullständig
- **Tillgänglighet:** att information är åtkomlig i ätt tid och användbar av behörig

Detta dokument vänder sig till samtliga medarbetare och förtroendevalda. Här finns regler och råd för att hantera kommunens information på ett säkert sätt. Delar av dessa regler har medarbetare godkänt i samband med anställningsavtalets undertecknande. Dessa regler och råd gäller vid användning av digital information, muntlig information och skriftlig information på papper/analogt.

2 Regler och etiska riktlinjer

Uppträd som en god representant för kommunen. Den elektroniska utrustningen, datornät och e-post är arbetsredskap som används i tjänsten.

- För att vinna och behålla kundernas/brukarnas förtroende är det nödvändigt att arbeta med god etik och gott omdöme.
- Aktuella lagar och föreskrifter ska följas. Dessutom får det inte med syftet väcka anstöt eller på annat sätt såra eller skada någon annan.
- Det är förbjudet att i kommunens utrustning konsumera/producera pornografi, rasistisk propaganda, hot, förtal, uppmaning till droganvändning, våld eller diskriminering eller liknande som strider mot lag, avtal samt demokratiska grundprinciper.

Tänk på säkerheten. Det är viktigt att säkerställa att information inte förvanskas, förstörs eller kommer i orätta händer.

- Använd ”starka” lösenord. Blanda små och stora bokstäver, siffror och specialtecken.
- Håll inloggningsuppgifter hemliga och låna aldrig ut dem till någon annan.
- Lås alltid enheter med skärm- eller tangentbordslås när du lämnar dem utan uppsikt.
- Använd aldrig någon annans inloggningsuppgifter.

- Lagra alltid informationen på kommunens servrar, inte på lokal hårddisk och inte på moln-/internetbaserade lagringstjänster om de inte är godkända av kommunen.

Arbetsgivaren kan göra kontroller. För att kontrollera att gällande regler följs har arbetsgivaren rätt att utan att underrätta användaren i förväg logga/kontrollera/granska enskilda användares elektroniska utrustning.

- Om överträdelse sker kan kommunen polisanmäla den användning som strider mot svensk lag.
- Arbetsgivaren ser mycket allvarligt på överträdelse mot reglerna och betraktar det som ett brott mot det enskilda anställningsavtalet. Detta är något som i allvarliga fall kan leda till uppsägning eller avsked.

Om sektorerna har ytterligare säkerhetsregler så informerar ansvarig chef om detta.

3 Användaridentitet och lösenord

Användaridentiteten och lösenordet identifierar dig när du använder den elektroniska utrustningen. Du är ansvarig för allt som händer ”i ditt namn”.

- 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 eller låt någon se dig över ryggen när du loggar in. Dela inte lösenord med andra.
- Använd olika 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 webbsidor spara lösenordet. Får du frågan om lösenordet ska sparas, svara alltid Nej.
- Undvik ”säkerhetsfrågor”. De kan fungera som bakdörr till kontot.
- Om fel lösenord använts för många gånger så låses datorn, återställ ditt lösenord med hjälp av bank-id.
- För en del program används tvåfaktorsautentisering, i de fall dessa får användaren information om detta.
- Behöver du stöd kontakt Göliska IT/servicedesk eller för sektor bildning/IT-team.

4 Behörigheter

Medarbetarens anställning uppdrag utgör grunden för de behörigheter som tilldelas i syfte komma åt nödvändig information för att kunna utföra sina arbetsuppgifter. Vid behov är det den anställdes chef som ansöker om ytterligare behörigheter till berörd informationsägare/systemägare. Den anställdes chef ansvarar också för att ändra behörigheter vid förändrad anställning eller för

ändrade arbetsuppgifter. Medarbetaren ansvarar också för att meddela sin chef om behörigheterna är för omfattande.

Vid avslut av anställning ansvarar medarbetaren för att överföra informationen i e-post och information som är lagrad på tillfällig yta till rätt lagringsyta. Detta i samverkan med berörd chef.

5 Mobila enheter

Den IT-utrustning som tillhandahålls av kommunen kan vara stationär eller mobil. Exempel på mobila enheter är bärbara datorer, smarta telefoner, surfplattor, USB-minnen och annan kringutrustning.

5.1 Hantering av mobila enheter

Mobila enheter som tillhandahålls av kommunen är personliga arbetsredskap och får inte lånas eller överlåtas om det inte är enheter som delas av flera.

- E-post i arbetet får inte synkroniseras över till privata enheter.
- Uppsatta säkerhetsinställningar i enheter får inte ändras eller tas bort.
- Installerad programvara får inte kopieras eller installeras på annan enhet.
- Mobila enheter ska låsas med lösenord.
- Känslig och sekretessbelagd information ska lagras på av verksamheten anvisad plats.
- Endast godkända programvaror får installeras på enheten.
- Endast av kommunen godkänd enhet och programvara får anslutas till kommunens interna nät (STAP).
- Privat utrustning kan anslutas till kommunens gästnät.
- Iaktta stor försiktighet vid anslutning till öppna trådlösa nätverk. Det är lätt för obehöriga att läsa av trafiken.
- Iaktta stor försiktighet med inkoppling av kringutrustning, till exempel USB-minnen och kameror.

5.2 Distansarbete

- Kommunens enheter, datorer och läsplattor, är utrustade för distansarbete. Arbete utanför kontoret ställer krav på säkert beteende, se mer under pkt 11.

5.3 Fysisk hantering av mobila enheter

- Försiktighet ska iakttas vid arbete i publika miljöer. Arbete med känslig eller sekretessbelagd information får inte ske i publika miljöer.
- Mobila enheter får inte lämnas utan uppsikt i publika miljöer.
- Förlust av enhet ska omedelbart anmälas till Göliska IT och närmaste chef. För sektor bildning görs anmälan till deras IT-team. I vissa fall finns möjligheter att fjärradera information.

- Vid avslut av anställning ska mobila enheter återlämnas i enlighet med de rutiner som finns.
- Utrustningen ska i övrigt vårdas och hanteras på ett aktsamt sätt.

5.4 Särskilda regler för smarta telefoner och surfplattor

Förutom de regler som gäller allmänt för mobila enheter gäller även följande vid användning av smarta telefoner och surfplattor:

- Information som är känslig eller sekretessbelagd får inte hanteras i smart telefon eller surfplatta om inte särskild av kommunen godkänd säkerhetslösning används.
- Pinkoder, fingeravtryck eller annan autentisering måste användas till smarta telefoner och surfplattor.
- Vårda utrustningen och använd exempelvis skärmskydd och skal.

6 Skadlig kod

Skadlig kod är ett samlingsbegrepp för oönskade datorprogram som virus, trojaner, spionprogram och maskar. Dessa kan installeras på en dator eller ett nätverk utan administratörens samtycke och har utvecklats i syfte att störa IT-system, för att samla in information eller för att utnyttja datorkraft eller minneskapacitet i IT-utrustning.

- Skadlig kod kan spridas till dator eller mobila enheter om man öppnar bilagor i e-post, importerar filer eller surfar på Internet och klickar på fel länkar, inklusive sådana som finns i sociala medier.
- Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod.
- Var misstänksam och undvik att klicka på konstiga länkar eller fyll i irrelevanta uppgifter.
- Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga är förväntad. Tänk på att virusspridning kan ske via någons adressbok så även om avsändaren är känd kan det innehålla skadlig kod.
- Var observant på om IT-utrustning beter sig långsamt eller konstigt. Vid misstanke om skadlig kod, stäng av enheten och kontakta Göliska IT Service desk.

7 Internet och sociala medier

Användning av Internet och sociala medier kan vara till stor nytta på arbetet. Förutom de säkerhetsåtgärder som är kopplade till skadlig kod finns här särskilda regler för användning av Internet och sociala medier.

7.1 Internetanvändning

- Internet är främst ett arbetsverktyg i kommunen och privat internetanvändning ska inte störa ordinarie arbetsuppgifter eller medföra kostnader för kommunen.
- De regler som gäller i samhället i övrigt gäller självklart även inom kommunen. Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt dataskyddsförordningen är exempel på lagar som måste beaktas när man använder Internet.
- För material på Internet som ska användas i tjänsten får nedladdning och installation av upphovsrättsligt material (datorprogram, film, musik, m.m.) inte ske utan stöd i lag, avtal eller med skriftligt tillstånd från rättighetsinnehavaren.
- Internet är öppet för alla och endast information som kan läsas av alla får publiceras eller delas där, alltså inte all intern information och absolut inte känslig eller sekretessbelagd information.
- Loggfilen från din datortrafik är allmän handling.

7.2 Användning av sociala medier

Kommunen ser ett värde i att vara aktiv i sociala medier då det ger möjlighet till snabbare service, en personlig dialog och medverkar till att skapa delaktighet och engagemang.

- Riktlinjer för sociala medier är ett stöd för de som i sitt arbete ansvarar för kommunens sociala medier.
- För privat användning av sociala medier gäller samma yttrandefrihet som för alla andra med undantag att de inte får sprida information som omfattas av sekretess eller bryter mot eventuell tystnadsplikt. Brott mot sekretess och tystnadsplikt får endast ske inom ramen för meddelarfriheten[1].

8 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 meddelanden i e-posten riskerar att kunna läsas av obehöriga.

8.1 Ansvar

Den enskilde medarbetaren som är kontoinnehavare för ett personligt e-postkonto är alltid ansvarig för den e-post som skickas från kontot.

E-post ska hanteras i enlighet med kommunens rutiner.

[1] Med meddelarfrihet menas de regler i tryckfrihetsförordningen respektive yttrandefrihetsgrundlagen som innebär att det i viss utsträckning är möjligt att straffritt lämna normalt sekretessbelagda uppgifter för publicering i massmedier under förutsättning att finns ett utgivningsbevis

- Medarbetare är ansvarig för att löpande öppna och läsa inkommande e-post enligt kommunens rutiner.
- Vid ledighet lämna inte ut lösenordet utan hänvisa till nämnden eller kommunens brevlåda som bevakas dagligen.
- Vid avslut av anställning tas e-postkontot bort.
- E-postkonton som delas av flera, till exempel. myndighetsbrevlådor (för nämnder) och funktionsbrevlådor (t.ex. för enheter) har utpekade ansvariga.

8.2 Allmänna handlingar

- E-post som skickas till personliga brevlådor inom kommunen är allmän handling. För e-post ska alltid regler för registrering och hantering av allmänna handlingar följas.
- Ansvaret för bedömning om en handling ska registreras/diarieföras ligger hos den som ansvarar för brevlådan. Kontakta registrator vid behov av stöd.

8.3 Privat e-post

- Använd inte ditt e-postkonto i kommunen för privata ändamål.
- Använd inte ditt privata e-postkonto för arbetsmaterial.

8.4 E-post och känslig eller sekretessbelagd information

- Känslig eller sekretessbelagd information, inklusive extra skyddsvärda personuppgifter, får inte skickas med e-post. Denna typ av information får enbart skickas enligt verksamhetens anvisningar, exempelvis via säkra meddelanden.
- Skanning av dokument som innehåller känslig eller sekretessbelagd information ska inte skannas till en e-postadress utan ska enbart hanteras genom funktionen ”säker skanning” direkt till ett verksamhetssystem eller till en säker behörighetsstyrd mapp.

9 Lagring och säkerhetskopiering

Det är viktigt att information lagras på ett säkert sätt och säkerhetskopieras så att den kan återskapas. Information som lagras i kommunens nätverk, i mappen Mina dokument och på skrivbordet säkerhetskopieras (gäller för PC-användare). För användare med Mac-datorer/iPad finns särskilda anvisningar.

- Känslig eller sekretessbelagd information får endast lagras i godkända system och lagringsplatser.
- Fysiska dokument som innehåller känslig eller sekretessbelagd information ska förvaras inlåsta.

- USB-minnen och datorns C: (PC-användare) ska endast användas för tillfällig lagring. På dessa görs ingen säkerhetskopiering.

10 Spårbarhet och loggning

Spårbarhet innebär att man genom loggning kan identifiera vem som har gjort vad och när och följa förloppet för olika händelser på datorn.

11 Säkert beteende

En stor del av kommunens information hanteras muntligt och på papper. Intern information ska hållas internt och inte visas för obehöriga. En del av denna information är särskilt skyddsvärd, känslig eller sekretessbelagd.

OBS! Kap 11 ska inte tolkas som inskränkning av den grundlagsskyddade meddelarfriheten.

11.1 Muntlig information

- Intern information ska hållas inom arbetsplatsen. Det är bara öppen information som får kommuniceras hörbart utanför arbetsplatsen.
- Känslig eller sekretessbelagd information har en begränsad krets av behöriga. Man ska enbart tala om detta i stängda utrymmen och även försäkra sig om att fysiska samtal eller telefonsamtal inte hörs i intilliggande rum.

11.2 Information på skärmar och i pappersform

- Internt skriftligt material på papper eller dataskärm får inte hanteras eller lämnas så att obehöriga kan läsa den. Låt till exempel ingen läsa över din axel, ta del av information genom ett fönster eller bilrutan och placera datorskärmar så att ingen obehörig kan ta del av informationen på skärmen.
- Material som innehåller känslig eller sekretessbelagd information ska låsas in i godkända skåp när man lämnar arbetsplatsen, även för kortare stunder.
- Känslig eller sekretessbelagd information på datorskärmen ska vara skyddad från obehöriga. Skärmen ska låsas när man lämnar datorn, även för en kortare stund. Om man har ett så kallat smart kort till datorn ska detta tas ut då man lämnar arbetsplatsen.
- Vid utskrift av dokument skall detta ske, då det är möjligt, med hjälp av tjänster för säker utskrift där dokumenten skrivs ut först när mottagaren begär det.
- Besökare får inte vistas utan uppsikt i lokaler där känslig eller sekretessbelagd information kan finnas.
- Vid fysisk posttjänst ska rekommenderade försändelser användas om brev innehåller känslig eller sekretessbelagd information.

- Då känslig eller sekretessbelagd information överförs via fax ska man försäkra sig om att man har rätt nummer och att mottagarens fax är övervakad under överföringstillfället.
- Pappersdokument som innehåller känslig eller sekretessbelagd information måste vid kassering strimlas eller kastas i godkända säkerhetskärl.

12 Skyldighet att rapportera incidenter och brister

Alla medarbetare har skyldighet att rapportera incidenter eller brister som misstänkts kunna medföra negativ påverkan på kommunens information till exempel:

- IT-angrepp/intrång
- Skadlig kod
- Oskyddad känslig information
- Brister i efterlevnad av lagar och riktlinjer för informationssäkerhet

Vissa incidenter ska anmälas enligt speciella incidentrapporteringsrutiner. Det finns särskilda rutiner för olika lagstiftningar t ex personuppgiftsincidenter.

Övriga incidenter och brister ska anmälas till närmsta chef eller Göliska IT servicedesk. För sektor bildning gäller deras IT-team.

För mer information, se rutinen Informationssäkerhet, avvikelsehantering och incidentrapportering – rutin.