



Eskilstuna  
kommun

# Informationssäkerhetsinstruktion för användare, medarbetare och förtroendevalda

20130311

Användarinstruktion v 1.6

## Informationssäkerhetsinstruktion för användare, medarbetare och förtroendevalda - en sammanfattning.

Eskilstuna kommun behöver stärka skyddet kring den information som vi använder i vår dagliga verksamhet. Denna *informationssäkerhetsinstruktion* beskriver hur vi vill att du som medarbetare eller förtroendevald inom Eskilstuna kommun ska hantera informationen samt använda IT-system på ett säkert sätt. *Informationssäkerhetsplanen* utgör övergripande, generellt, underlag.

### Bakgrund.

*Information* är idag en integrerad del i verksamhetens vardag, oftast kritisk för arbetet, på alla nivåer i organisationen. Ledningsfunktionen har ett ansvar för *informationssäkerheten* och bifogat material är det underlag som utgör grunden för att skapa styrande, planerande och praktisk information inom området.

Syftet med en övergripande *Informationssäkerhetsplan* är att för såväl anställda (motsv) som arbetsgivare tydliggöra parternas spelregler vilket leder till ökad trygghet och rättssäkerhet vid exempelvis incidenter. Såväl arbetsgivare som arbetstagare behöver känna tillit till en spelplan som anger vilket ansvar och vilka befogenheter som gäller.

*Målsättningen* är att skapa ett öppet och lärande regelverk anpassat till Eskilstuna kommuns värderingar och normer. Detta medför balans mellan öppenheten att använda IT som en resurs men samtidigt skydda känslig information som berör individer och verksamhet. Lagstiftning och regelverk är här styrande.

Den övergripande *informationssäkerhetsplanen* har tre underliggande instruktioner:

- Användarinstruktion för elever samt för kunder, brukare och externa konsulter.
- Förvaltning (systemägare).
- Kontinuitet och drift.

Denna användarinstruktion sammanfattar de viktigaste informationssäkerhetsområdena som direkt berör mig som anställd. Du hittar de fullständiga dokumenten på internportalen. Tänk på att du som medarbetare har ett ansvar att ta del av den fullständiga dokumentationen då undertecknad ansvarsförbindelse avser dess innehåll.

Instruktion är antagen av kommunstyrelsen den 14 maj, § 128, och gäller från och med 20 maj 2013. Informationssäkerhetsplan med underliggande instruktioner är ett reformarbete med årlig revidering för att etablera ett adekvat LIS, Ledningssystem för informationssäkerhet, för Eskilstuna kommun.

## 1. Regler och etik för IT-användningen i kommunen i korthet

Eskilstuna kommuns IT-miljö är integrerad i en intern och extern kommunikationsvärld, där du som användare lämnar digitala spår som är hänförliga till kommunen. Därför gäller följande regelverk, där du

- Uppträder så att du ej bryter mot lagar och förordningar
- Respekterar andra människor och grupper, ej kränker eller bedriver nätmobbing
- Är aktsam om kommunens utrustning och vårdar informationen i systemen som avsett
- Arbetar i enlighet med Eskilstuna kommuns värdegrund
- Inte åsidosätter rättvisa konkurrensförhållanden.

### Tänk på att

- Lösenordet är personligt, ska hållas hemligt och bytas när man därtill uppmanas, samt får ej otillbörligt lämnas ut till någon annan
- Du endast får söka fram de uppgifter [ur verksamhetssystem som](#) du behöver i tjänsten för att fullgöra ditt uppdrag
- Surfning till webbplatser som är av karaktären pornografisk, rasistisk, kriminell eller diskriminerande (med hänsyn till religion, kön, sexuell läggning eller liknande) innebär loggning av sessionen. Se Regler för hantering och kontroll av loggar i IT-utrustning.
- Installation av program som inte är godkända av Eskilstuna kommun är ej tillåtet
- Material som är upphovsrättsskyddat och kommunlicensierade program får ej kopieras. Ej heller användas i privat eller kommersiellt syfte.
- Material av privat karaktär ska lagras utanför Eskilstuna kommuns IT-miljö, enbart arbetsrelaterat data får lagras på exvis H-katalogen eller Min webbplats i internportalen.

### Du ska

- Låsa din dator eller logga ut när du inte har uppsikt över din arbetsplats.
- Vid misstanke om att din dator utsatts för virus, skadlig programkod eller dator uppträder onormalt, anmäla till [Kundservice-IT-Kundtjänst](#)

**Privat IT-användning får inte ske på arbetstid eller innebära olägenhet för arbetsgivaren, men med tolkningsföreträde för förvaltningsledningen, så tillåts**

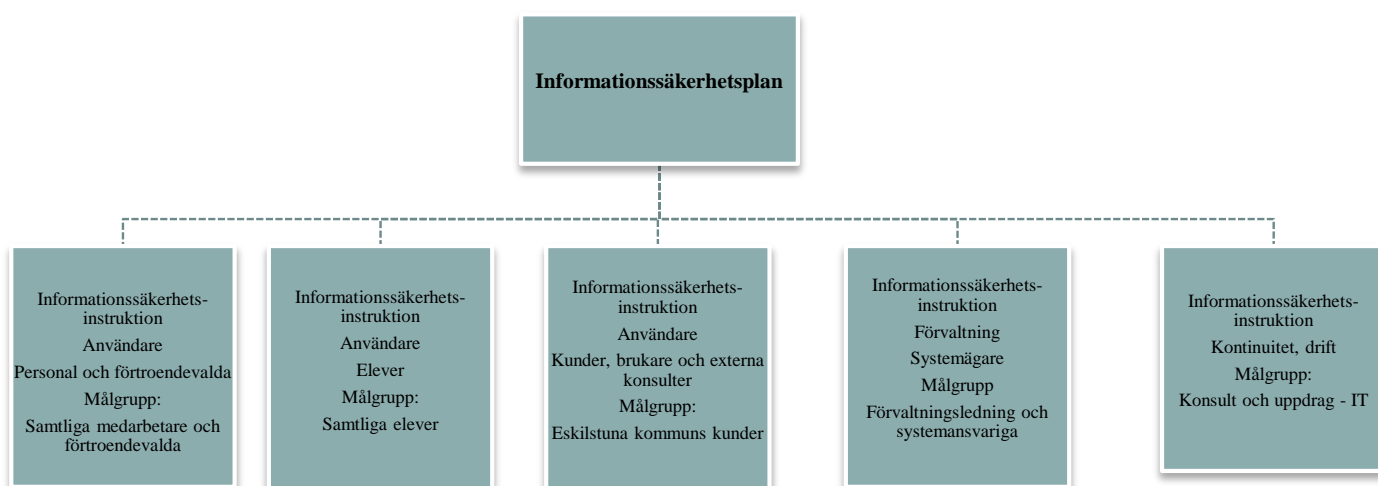
- Surfning och användning av internet i privat syfte så länge du respekterar villkoren för användningen enligt denna instruktion, exempelvis skicka/ läsa privat e-post i första hand från ditt privata e-postkonto, sociala medier med anknytning till kommunen (se även under Sociala medier på internportalen).
- Utnyttja kommunens licens för användning av Officepaketet i privat syfte, dock ej kommersiellt.
- Skriva ut privat material i enstaka exemplar (endast ett fåtal sidor).

**Eskilstuna kommun har en generös hållning till personalens IT-användning. Att du som användare följer informations säkerhetsplanen samt tillhörande instruktioner är av yttersta vikt för att Eskilstuna kommun ska kunna fortsätta med denna generösa hållning.**

## 2. Informationssäkerhet för Eskilstuna kommun

Eskilstuna kommuns informationssystem är integrerade i den vardagliga verksamheten där informationen, digitalt som på papper, representerar ett stort kapital som måste skyddas. Informationen används av anställda, förtroendevalda, elever och brukare där vi måste säkerställa tillgänglighet, säkerhet, sekretess och spårbarhet.

Den övergripande informationssäkerhetsplanen har underliggande instruktioner för mer detaljerad vägledning för dig som användare, förvaltare av informationssystemet eller ansvarig för tillgänglighet i driftmiljön.



Figur 1 Eskilstuna kommuns informationssäkerhetsplan – med underliggande instruktioner för olika målgrupper.

## 3. Användarens ansvar

Vår vardagliga verksamhet använder information ur olika aspekter: från strategisk nivå till operativ nivå, klassificerad från öppen till sekretessbelagd nivå, ofta med personuppgifter som berörs av PUL. Gränserna för var data lagras suddas ut med molnbaserade tjänster, data skickas över ett internet som ska betraktas som öppet ur sekretessynpunkt ("som att skicka vykort").

Eskilstuna kommun behöver öka medvetandet om informationssäkerhetens betydelse för att skydda kommunens data. Vi är många användare internt och vi vill exempelvis skapa mer tillgänglighet för våra medborgare via eTjänster, vilket kräver ökad tydlighet i ansvarsfrågan. Som användare har du därmed ett personligt ansvar för säkerheten i informationshanteringen. Dessa instruktioner ska du således godkänna – Ansvarsförbindelse - att du tagit del av och förstått innebörden av. Att bryta mot dessa instruktioner eller bryter mot regelverket kan innebära sanktioner och rapporteras till din närmaste chef.

Systemägaren ger styrning och har stödfunktioner för sina system och KoU-IT ger dig stöd vid teknikrelaterade frågeställningar.

Oavsett om du är kund, brukare, extern konsult, elev, förtroendevald eller medarbetare så är det **förbjudet inte tillåtet** att använda Eskilstuna kommuns utrustning på sådant sätt att du:

- \* Bryter mot lag eller annan författning.
- \* Kränker andra människor eller grupper.
- \* Underminerar eller åsidosätter Eskilstuna kommuns värdegrund.
- \* Främjar egna eller andras kommersiella eller ideella intressen eller åsidosätter rättvisa konkurrensförhållanden.

**Som användare av kommunens IT-utrustning/system får du endast söka fram de uppgifter du behöver i tjänsten eller för att fullgöra ditt uppdrag.** Att medvetet söka fram information som du inte behöver för din tjänst/ditt uppdrag kan innebära att du begår dataintrång. Det kan komma att få arbetsrättsliga konsekvenser och/eller innebära polisanmälan.

#### 4. Arbetsgivarens ansvar – rättigheter/skyldigheter

Arbetsgivaren (varje nämnd/varje personuppgiftsansvarig) ska:

- Beskriva vilka informationstillgångar (inklusive personuppgifter) som behandlas i verksamheten.
- Utforma interna regler och riktlinjer för hanteringen.
- Skapa behörighetsregler.
- Informera och utbilda personalen.

Arbetsgivaren har rätt att kontrollera att framtagna och beslutade regler följs.

##### **Integritetsskydd för medarbetare och förtroendevalda – grundregel.**

Medarbetaren och de förtroendevalda ska känna till vilka behandlingar av personuppgifter om honom eller henne som arbetsgivaren utför, vara informerad om regler och riktlinjer för IT-användningen på arbetsplatsen och kunna lita på att de följs.

Kontroll av loggar i IT-utrustning är en del av den kontrollmekanism (attest, kvalitet, internkontroll) som finns inom Eskilstuna kommun.

Kontroll av åtkomst är en aktivitet i syfte att säkerställa att användarna av kommunens IT-utrustning inte felaktigt utnyttjar sina behörigheter genom att titta på (person) uppgifter/-information som till exempel saknar relevans för arbetsuppgifterna, ändrar eller tar bort information som de inte ska hantera. Kommunens kontrollmöjligheter är dock inte oinskränkta.

#### 5. Åtkomst till information

Informationssäkerhet innebär att i styrsystem säkerställa såväl användarens identitet som behörighet, samt informationens kvalitetssäkra tillgänglighet, krav på sekretess, riktighet och spårbarhet. Utgångspunkt för all åtkomst av information skall vara klassificering av informationen som styrande för val av lösning.

De loggningsfunktioner som finns i systemen används bland annat för att spåra obehörig åtkomst. Detta är till för att skydda informationen och för att undvika att oskyldiga misstänks om oegentligheter skulle inträffa. Det är därför också i ditt eget intresse att någon annan inte ska kunna använda systemen under ditt användarnamn. Därmed är det också **förbjudet inte tillåtet** för dig att använda någon annans inloggningsfunktion.

Tänk på att du inte får skicka sekretessbelagda uppgifter, känsliga personuppgifter eller personnummer via internet med mindre än att uppgifterna är krypterade.

Identitet- och behörighetsansvar:

- Du får endast ta del av den information **i verksamhetssystem** som du behöver för arbetsuppgiften eller uppdraget. Systemägaren definierar vilka roller och hur informationen är klassificerad för åtkomst.
- Systemägaren skapar roller och ansvar för vilken åtkomst som skall gälla för systemet och din behörighet är personlig, och kan ej överföras till annan.
- Som användare får du inte vidarebefordra data ur verksamhetssystem till obehöriga personer.

## 6. Din arbetsplats

Endast av Eskilstuna kommun godkänd datorutrustning får kopplas till det administrativa nätverket. Undantag gäller för gästnät.

Mobila enheter som ansluts till trådlösa nätet (WiFi) skall ha PIN-kod vid uppstart om du synkroniserar data typ epost och kalender. Används mobila enheter för verksamhet där känsliga, PUL- eller sekretessbelagda uppgifter förekommer, skall lösningen genomgå systemsäkerhetsanalys för att avgöra om riskbilden medger rimlig lösning. Borttappad mobil enhet skall anmälas till KoU-IT för radera innehåll på distans.

Flyttbara lagringsmedia ska användas i så begränsad omfattning som möjligt.

### Programvaror

Eskilstuna kommun installerar i standardutförande, underhåller och uppdaterar nödvändiga programvaror som är av baskaraktär. Därutöver kan verksamheten i anskaffnings-processen upphandla specifika system, med beaktande av kommunens infrastruktur och vad IT-tekniska miljön medger. I övrigt gäller regelverket att kommunen skall uppfylla villkoren avseende licensfrågor:

- Eskilstuna kommuns licenser för programvara inte får kopieras eller installeras på annan utrustning än ägda av kommunen
- Kommunens licenser får ej heller användas i privat syfte som åsidosätter konkurrensförhållanden eller är av konkurrerande verksamhet
- Egna köpta och installerade program, appar och motsvarande i av kommunen ägd utrustning riskerar bli raderade vid uppdatering av datorenheten.

Alla datorer ska skrotas enligt gällande skrotningsrutin som innebär att hårddisken raderas från information med en säker raderingsalgoritm alternativt förstörs. Skrotningen utförs genom Eskilstuna kommuns försorg.

### **När du lämnar arbetsplatsen**

Vid situationer när du tillfälligtvis inte har uppsikt över din arbetsplats ska du låsa din dator genom att trycka på <ctrl+alt+delete> eller Windowsflagga+L.

### **Arbete utanför kommunens lokalansvar**

Vid arbete på distans (hemifrån, kurs, ledighet etc) är dels en medarbetarfråga med din närmaste chef, dels en systemägarfråga där klassificeringen av informationens skyddsvärde avgör villkoren för åtkomst. Inget sekretessmaterial får lagras på lokala datorn.

## **7. Internet/epost**

Surfning på internet innebär att den IP-adress som du får, hänvisar till Eskilstuna kommun som organisation och är det spår som du lämnar. All trafik går via ett filter och registreras i en logg för att KoU-IT ska kunna följa upp otillåten trafik i båda riktningar. Regelverket i filtret är definierat utifrån kommunens värdegrund, klassificerade webbsajter (ex.vis pornografiska) och direkt förbjudna webbplatser. Vid passering av gränsvärdet får du upp en ruta på din skärm där du får valet att fortsätta eller återgå. Vid fortsättning loggas sessionen och din närmaste chef (motsv) delges informationen. I övrigt gäller att gällande lagstiftning skall följas (upphovsrätt), att inte kränka människor eller grupper och i sociala medier uppträda i enlighet med kommunens värdegrund.

Epost kan vara allmän handling och följande gäller:

- Sekretessbelagd eller integritetskänslig information får inte skickas via epost såvida inte informationen krypteras
- Information till större grupper – använd internportalen.
- För privat kommunikation – använd kommersiell epost-adress.

Se upp med falska förfrågningar via e-post. Eskilstuna kommun kommer **aldrig** att be dig lämna ut ditt lösenord via e-post. En god säkerhetsgrund är att du överhuvudtaget aldrig svarar på uppmaningar där du ombeds att uppge användar-id/lösenord/kontonummer.