Riktlinje för utbyte av sekretessbelagd digital information mellan interna och externa parter

---

Kommunalförbundet ITSAM och dess medlemskommuner

Reviderad: 20161227
Ersätter: 20130510
Dnr: 2013/00036

1.0 Syfte
Syftet med denna riktlinje är att reglera handhavandet med sådan information som kan skada person eller organisation genom röjning av sekretessbelagda uppgifter.
Riktlinjen är styrande tillsammans med övergripande Informationssäkerhetspolicy IT, externa lagar och regelverk (patientdatalagen, PUL mm) och gäller hantering av känslig information avseende på i de fall av verksamheten sekretessbelagd information ska överföras till part inom eller utanför den egna organisationen.

2.0 Omfattning
Riktlinjen gäller för all digital sekretessbelagd information såsom information av personlig natur eller annan information som innehåller persondata inom socialförvaltningen, omsorgsförvaltningen eller annan förvaltning som administrerar information innehållande personuppgifter.

Exempel på information som sekretessbeläggs:

- Journalhandling
  Med journalhandling avses enligt patientdatalagen framställning i skrift eller bild samt upptagning som kan läsas, avlyssnas eller på annat sätt uppfattas endast med tekniskt hjälpmedel (handling, skriven eller ritad på papper, diskett, CD, video, DVD, bilder)
- Utredningsplaner
- Annan information innehållande uppgifter om personer med skyddad identitet

En verksamhet som överför sekretessbelagd information är skyldig att följa de rutiner som är kopplade till denna riktlinje samt till övergripande informationssäkerhetspolicy IT samt informationssäkerhetsinstruktionen InfoSäk A samt informationssäkerhetsinstruktionen InfoSäk F.

3.0 Regler
Det är endast tillåtet att kommunicera sekretessbelagd information (dit hör t.ex. namn och personnummer på personer) under förutsättning att både avsändare och mottagare är säkert identifierade och informationen är krypterat under transporten.
För överföring av sekretessbelagd information får enbart identifieringsmekanismer och anslutningssystem administrerade och kontrollerade av kommunalförbundet ITSAM användas och som möter interna och externa krav.

3.1 Säker identifiering
Säker identifiering uppnås genom minst två-faktors autentisering i informationsutbytessystemet. Med två-faktors autentisering menas att den som ska identifiera sig har något unikt man har(dosa, certifikat mm) med tillhörande lösenord eller PIN(något man vet)

3.2 Kryptering
Krypteringsnivå på sekretessbelagd information ska följa externa regelverk såsom riktlinjer från datainspektionen mm samt interna riktlinjer.

3.3 Loggning och spårbarhet
Identifiering och autentisering samt eventuella dokumentnamn loggas för att säkerställa spårbarheten i systemet. Informationsinnehåll som skickas över säkra kanaler ska inte loggas av sekretesskäl.

4.0 Verkställighet
Kommunalförbundet ITSAM förbehåller sig rätten att vid misstanke om användning av andra tjänster än de som godkänts av Kommunalförbundet ITSAM för informationsutbyte gällande sekretessbelag information stänga ner datakommunikationen till vederbörandes arbetsplats samt rapportera missförhållandet till ansvarig chef.