Riktlinje för åtkomstkontroll

Kommunalförbundet ITSAM och dess medlemskommuner

Reviderad: 20161227
Ersätter: 20140107
Dnr: 2013/00036

1.0 Syfte
Detta dokument beskriver säkerhetskraven gällande kontroll av vid identifiering och autentisering för användare och utrustning inom Kommunalförbundet ITSAM och inom dess medlemskommuner.

2.0 Omfattning
Riktlinjen reglerar hur man eller vad beroende på roll, funktion eller arbetsuppgift identifierar och autentiserar sig för att erhålla åtkomst till verksamhetssystem via kommunalförbundets datanät och från datanät som ligger utanför kommunalförbundets administrativa och tekniska kontroll.
Alla användare och all utrustning omfattas av denna riktlinje och definieras i Informationssäkerhetsinstruktionen Förvaltning IT samt i Informationssäkerhetsinstruktionerna Användare Personal, Användare Övriga och Användare Elever (Infosäk A-P, Infosäk A-Ö, Infosäk A-E).

3. 0 Definition
Vissa kommunala verksamheter hanterar information där användningen av denne regleras av lagar och förordningar. Exempel på detta är hanteringen av patientdata och information om personer med skyddade uppgifter som regleras av PUL och patientdatalagen.
Kommunera använder idag tjänster och information som administreras och lagras hos externa parter där kommunikationen sker över oskyddade nät såsom Internet. Kravet för åtkomst till dessa är bl a förhöjd säkerhet vid identifiering och autentisering, s k 2-faktorstyp, för att säkerställa identitet, sekretess och spårbarhet.
Med identifiering menas att användare eller utrustning hävdar sin identitet m h a användarnamn, lösenord eller certifikat i systemen. Autentiseringen är beviset att rätt användare eller utrustning hävdar rätt identitet. Detta kan vara m h a lösenord, certifikat med tillhörande PIN-kod mm. Säkerhetsnivåer för identifiering är:

- 1-faktors identifiering (svag nivå): AnvändarID samt något man vet såsom lösenord
- 2-faktors identifiering (stark nivå): Som ovan samt något man har såsom kort, telefon mm för generering av engångskod
- 3-faktors identifiering (stark nivå): Som ovan samt någon egenskap man besitter såsom fingeravtryck mm

4. 0 Riktlinje

4.1 Identifiering och autentisering av användare (fysisk person)
Alla som ska ha åtkomst till verksamhetskritiska system ska använda en 2-faktors identifierings- och autentiseringsmetod. Datorer som används vid åtkomst till känsliga uppgifter ska vara kontrollerad och hanterade av Kommunalförbundet ITSAM, detta gäller såväl fysisk som virtuell dator.
System som anses verksamhetskritiska specificeras i Informationssäkerhetsinstruktion Förvaltning och informationsinstruktion Kontinuitet och Drift IT (Infosäk F och Infosäk KD).

4.2 Identifiering och autentisering av utrustning
Utrustning som ska ha åtkomst till verksamhetskritiska eller centrala system ska använda en 2-faktors identifierings- och autentiseringsmetod. Datorer som används vid åtkomst till känsliga uppgifter ska vara kontrollerad och hanterade av Kommunalförbundet ITSAM, detta gäller såväl fysisk som virtuell dator.
System som anses verksamhetskritiska specificeras i Informationssäkerhetsinstruktion Förvaltning och informationsinstruktion Kontinuitet och Drift IT (Infosäk F och Infosäk KD).

4.3 Kommunikation
För att upprätthålla nivåerna för integritet, sekretess och riktighet för säkerhetsklassade system vid fjärrarbete via datanät som inte kontrolleras och hanteras av Kommunalförbundet ITSAM ska kommunikationen vara krypterad vid in- och utloggningsfas och under sessionstid.

4.2 Ansvar
Alla användare som identifierar och autentiserar sig mot kommunala verksamhetssystem och får åtkomst till dessa har ett ansvar att skydda information mot obehörig åtkomst. Misstänker man att information eller att identifieringsuppgifter såsom lösenord, certifikat mm är röjt till obehöriga skall detta rapporteras omgående till systemadministratör och till systemförvaltare.

För den som implementerar och ansluter utrustning som i sin tur får åtkomst till verksamhetskritiskta eller centrala system har ansvaret för att denna utrustning konfiguraras i enlighet med denna och dess övergripande styrande dokument.

5.0 Verkställighet

Användare som inte följer denna riktlinje kommer bli föremål för disciplinära åtgärder såsom kontolåsning, varning eller avstängning.