Civilförsvarsförbundet
www.civil.se

Beslutad av förbundsstyrelsen 2015-09-11

Informations- och säkerhetspolicy

Informations- och säkerhetspolicyn är ett levande dokument som uppdateras efter behov.

Civilförsvarsförbundet är beroende av att medlemmar och andra har ett starkt förtroende för organisationen. Därför har det också betydelse hur vi dagligen hanterar information. Om hanteringen inte sköts till fullo kan det innebära skada för både organisationen, dess medlemmar, personal, samarbetspartners och andra uppdragsgivare. Detta kan i förlängningen leda till extra kostnader och kanske till och med rättsliga påföljder för Civilförsvarsförbundet.

Informationssäkerhet finns för att skydda våra tjänster och information. Kostnaderna för säkerhetslösningarna ska vara kostnadseffektiva och vara proportionerliga till konsekvenser för bristfällig säkerhet.

Ledorden för Civilförsvarsförbundets informationssäkerhetsarbete är tillgänglighet och riktighet.

Med tillgänglighet menas att de personer som har behov av uppgifter och system ska ha tillgång till uppgifterna och systemen. Riktighet innebär att informationen ska vara korrekt och att den ska rättas om det visar sig att den är felaktig.

I övrigt ska lagar och förordningar som är tillämpliga på verksamheten efterlevas. Ett exempel är personuppgiftslagen, PUL.

Medlemmar i Civilförsvarsförbundet och anställd personal får inte uppträda på sådant sätt att de skadar förbundets namn, rykte eller relationer. Förbundets namn får inte användas på ett sådant sätt att det strider mot Civilförsvarsförbundets intressen.

Medlemmar i Civilförsvarsförbundet och anställd personal som har tillgång till administrativa eller tekniska system i förbundet förbinder sig att i dessa sammanhang att

- Använda lösenord som är minst åtta tecken långa och innehåller minst två andra tecken än bokstäver. Lösenord får heller inte vara samma som för andra tjänster som sociala medier, bloggar eller annat.
- Inte anteckna eller delge lösenord till obehörig person eller att på annat sätt handskas ovarsamt med lösenord så att andra kan ta del av lösenordet.
- Genom personlig brandvägg och regelbundet uppdaterat virusskydd säkerställa att fjärranslutna datorer med hänsyn till virus, trojaner och så vidare inte utgör ett säkerhetshot mot Civilförsvarsförbundets nätverksmiljö och andra administrativa och tekniska system.
- Ha kontroll över den dator eller annan utrustning som används för att koppla upp sig till förbundets administrativa och tekniska system. Detta för att säkerställa att inga obehöriga program eller filer laddas ner.

Utskrifter från förbundets administrativa eller tekniska system, som inbegriper personnummer eller annan information av mer personlig art, ska hanteras med extra varsamhet. Efter att utskriften fullgjort sitt syfte eller att lagkrav om arkivering upphört ska den förstöras på ett betryggande sätt.

Information om medlemmar sparas i förbundets resurs- och medlemsregister Max. Uppgifterna används i verksamheten för bland annat avisering, kallelser och utskick av medlemstidning. Medlem har rätt att en gång per år utan kostnad efter skriftlig begäran få ett registerutdrag samt få felaktiga uppgifter rättade. Gallring ska ske utifrån förbundets regler för gallring

All personal ansvarar för att säkerhetskopia löpande tas på data på den egna datorn och att denna säkerhetskopia förvaras i annan lokal än där datorn finns. Säkerhetskopiering kan ske till USB-minne eller att senaste versionen av en fil mejlas till och sparas på den egna jobb-mejlen. Personal på förbundskansliet som har enkel tillgång till nätverket ansvarar för data som är viktig för verksamheten lagras på nätverket och inte lokalt på datorn. Nätverket har betryggande backupsystem. Personalen ska hållas uppdaterad om det personliga ansvaret för datasäkerheten.

Informationsägare till data i Civilförsvarsförbundets administrativa och tekniska system, exempelvis medlems- och resursregistret Max, är Sveriges Civilförsvarsförbund. Lokalföreningar och distrikt har tillgång till data om medlemmar i den egna lokalföreningen eller distriktet.

En fungerande informations- och säkerhetspolicy ställer krav på en kontinuerlig riskhantering. Hot och risker som identifieras ska analyseras för att tillse att organisationen har tillräckligt skydd.

För Max gäller följande såsom det är beskrivet i PUL:
Personuppgiftsansvarig är Sveriges Civilförsvarsförbund.
Personuppgiftsbiträde är tjänsteleverantören av medlems- och resursregistret Max.
Personuppgiftsombud utses av generalsekreteraren.

Civilförsvarsförbundets generalsekreterare ansvar för att informations- och säkerhetspolicyn följs och uppdateras.