Riktlinje för informationssäkerhet

Svenska Röda Korset

Fastställd av GS 2020-07-06

INNEHÅLLSFÖRTECKNING

1 INLEDNING

Alla organisationer är beroende av information för att kunna utföra sina uppdrag. Information handlar om allt det vi gör, exempelvis om våra projekt och verksamheter, vår personal, vår ekonomi och samhället runtom oss. Information kan vara i form av tal, text, ljud, bilder och video, och kan hanteras i både fysisk och digital form.

Den information som används inom Svenska Röda Korset är värdefull både för oss som organisation och för enskilda individer. Därför måste vi skydda vår information så att endast behöriga personer får ta del av den, så att den finns när vi behöver den och så att vi kan lita på att den är riktig och inte manipulerad.

Utvecklingen med informationshantering i IT-system och andra nya funktionaliteter innebär förbättringar i många avseenden. Samtidigt innebär beroendet av informationssystem att sårbarheten och riskexponeringen ökar om inte säkerhetsaspekterna beaktas. Därför arbetar Svenska Röda Korset aktivt med informationssäkerhet.

Syftet med dessa riktlinjer är att sätta ramarna för hur vi inom Svenska Röda Korset hanterar, sparar och delar information med varandra och externa aktörer. Informationssäkerhet har inget egenvärde, utan ska bidra till att Svenska Röda Korset når sina övergripande visioner, strategier och mål.

Genom att arbeta systematiskt och långsiktigt upprätthåller vi ett tillräckligt skydd som är anpassat efter våra verksamheters förutsättningar och behov. Det är nödvändigt för att vi ska uppnå verksamhetsmålen och för att våra målgrupper, anställda, frivilliga och förtroendevalda, givare, samarbetspartners och allmänheten ska känna förtroende för oss.

1.1 Om informationssäkerhet

Informationssäkerhetsarbetet innebär att värdera all information efter sin känslighet och med hjälp av administrativa och tekniska skyddsåtgärder säkerställa att den finns tillgänglig när den behövs, att den är korrekt och att obehöriga inte kan få tillgång till den. Kortfattat handlar informationssäkerhet om att ge information rätt skydd utifrån tre aspekter:

- Tillgänglighet: att information görs åtkomlig för behörig person vid rätt tillfälle.
- Riktighet: att information skyddas mot oönskad förändring.
- Konfidentialitet: att information skyddas mot obehöriga.

Information har i olika grad krav på sig gällande de tre aspekterna. Kraven kan härledas från rättsliga krav eller från Svenska Röda Korsets egna målsättningar. Dessutom har individer och aktörer i vår omvärld behov och förväntningar som ställer krav på vår informationssäkerhet.

Det är viktigt att komma ihåg att informationssäkerhet inte begränsas till säkerhet i IT-system, utan att det omfattar säker hantering av information i alla dess former och oavsett hur den lagras, bearbetas och kommuniceras. Ett stort ansvar vilar på de enskilda personer som hanterar informationen.

1.2 Riktlinjens omfattning och avgränsning

Denna informationssäkerhetsriktlinje gäller för hantering av information, i alla dess former, inom Svenska Röda Korset. Informationssäkerhetsriktlinjen kompletterar våra riktlinjer om IT-säkerhet, riktlinjer för insamling och riktlinjer för skydd av personuppgifter.

För att kunna säkerställa en god nivå av informationssäkerhet i en organisation är det viktigt att informationssäkerhetsarbetet bedrivs systematiskt och långsiktigt, och att det förankras hos alla medarbetare. Denna riktlinje vänder sig därför till alla förtroendevalda, frivilliga, anställda, delegater, praktikanter, studerande, konsulter, arvoderaderade eller andra som har åtagit sig uppdrag för, eller på annat sätt representerar, Svenska Röda Korset i Sverige och/eller utomlands. I denna riktlinje kallas alla dessa olika personer sammantaget för ”rödakorsare”.

2 INFORMATIONSSÄKERHET I SVENSKA RÖDA KORSET

2.1 Verksamhetsdriven informationssäkerhet och informationsklassning

Svenska Röda Korset jobbar med en verksamhetsdriven informationssäkerhet, vilket utgår från att verksamheter har bäst kunskap om hur känslig och kritisk deras informationsmängder är, och därmed informationens skyddsvärde. En verksamhetsdriven informationssäkerhet innebär att verksamheter har ansvar för sin informationssäkerhet och ställer krav på de aktörer som hanterar informationen utifrån informationens skyddsvärde.

För att skapa en anpassad och effektiv informationssäkerhet bör så kallad informationsklassning tillämpas. Genom informationsklassning definieras skyddsbehovet för olika typer av information med syftet att ge känslig och kritisk information ett starkare skydd än annan information. Chefer och medarbetare inom samma verksamhet ska utgå ifrån en enhetlig modell för informationsklassning baserad på interna och externa krav på informationens tillgänglighet, riktighet och konfidentialitet. Informationsklassning innebär inte att skyddsbehovet för varje enskilt informationsobjekt eller dokument ska bedömas, men det ska finnas tydliga skyddsbedömningar för olika huvudtyper av dokument.

En utgångspunkt för alla verksamheter och rödakorsare är att de efterlever Svenska Röda Korsets riktlinjer för skydd av personuppgifter (GDPR)[1] och våra IT säkerhetsriktlinjer[2].

2.1.1 Särskilt om hantering av känslig information

Känslig information (inklusive sekretessbelagd information) ska märkas så att detta framgår. Det är väsentligt att varje medarbetare känner till vilken information, inom i första hand sitt eget ansvarsområde, som är känslig och hur den ska hanteras. Om du som rödakorsare känner dig osäker på hur en viss typ av information ska hanteras ska du vända dig till din chef eller ordförande. Om du hanterar personuppgifter i ditt uppdrag är det särskilt viktigt att dessa hanteras på ett tryggt sätt och att den personliga integriteten respekteras.

[1] Riktlinjer för skydd av personuppgifter hittar du här: https://www.rodakorset.se/globalassets/rodakorset.se/dokument/svenska-roda-korsets-riktlinjer-for-skydd-av-personuppgifter.pdf. På hemsidan kan du läsa mer: https://www.rodakorset.se/personlig-integritet/

[2] Riktlinjer för IT-säkerhet: https://kunskapsbanken.rodakorset.se/hc/sv/articles/360009855197-Riktlinjer-för-IT-säkerhet-

Externa parter, som till exempel myndigheter, kan ställa särskilda krav på hur information som de delar med Svenska Röda Korset ska hanteras. Sådana krav ska alltid följas. Är informationen belagd med formell sekretess eller är den säkerhetsklassad gäller särskilda rutiner för hantering.

2.2 Informationssäkerhet i praktiken

Utöver det specifika informationssäkerhetsarbete som ska göras inom våra olika verksamheter finns det generella tips och råd kring hur säker informationshantering kan gå till i praktiken. Dessa rör hantering av information i fysisk form men framförallt digitalt:

- Anteckningar och papper kan innehålla viktig information, förvara dem i säkerhet och kom ihåg att låsa utrymmen där känslig information finns.
- Vid arbetsmöten (såväl fysiska som digitala), bedöm risken att andra kan höra eller se informationen som förmedlas.
- Skydda din dator och smarta enheter (mobiltelefon, läsplatta, router etc.) med starka lösenord.
- Var extremt försiktig med att klicka på länkar, bilagor eller annat som kommer via e-post, sms eller olika webbsidor. Var uppmärksam på att det är en för dig välkänd avsändare.
- Om någon ber dig stänga av säkerhetsfunktioner för att exempelvis kunna leverera en tjänst får du inte följa den uppmaningen.
- Häng med i säkerhetsuppdateringarna. Tillverkare av datorer och mobiler skickar regelbundet ut säkerhetsuppdateringar. Installera dessa direkt. De innehåller viktiga förbättringar som hjälper till att skydda utrustningen. För din arbetsdator sker det mesta automatiskt. För mobilen är det viktigt att du inte väntar för länge.
- Tänk igenom vilka appar du laddar ner och ta regelbundet bort de appar som inte används. Acceptera alltid automatiska uppdateringar av apparna. Appar som inte uppdateras kan innebära säkerhetsrisker. Viktigt framför allt till din arbetsmobil.
- Använd inte USB-minnen mellan privat utrustning och din arbetsdator eftersom virus kan spridas mellan enheter.

2.3 Identifiering, rapportering och hantering av incidenter och tillbud

En incident är en händelse som kan få negativ påverkan på Svenska Röda Korsets verksamhet, det kan vara resultatet av en avsiktlig handling eller något som skett utan uppsåt. Exempel på en incident kan vara om Svenska Röda Korsets verksamheter eller kontor blivit utsatt för, eller hotas av, dataintrång, driftavbrott, otillåten hantering av information, brand, eller stöld.

Det kan handla om att en medarbetare har fått sin dator eller mobiltelefon stulen eller om en Secondhand-butik som brunnit där viktiga papper gått förlorade. En IT-incident kan vara att du misstänker att du fått virus på din dator, att du får ett mejl med en misstänkt länk som du uppmanas trycka på, eller att hela nätverket slutar fungera på ett kontor.

Ett tillbud är en händelse som hade kunna leda till skada men som slutade väl. Även om det går bra och ingenting händer är det viktigt att ta tillbudet på allvar. Tillbudet är en signal om att något allvarligt skulle kunna hända nästa gång och att man behöver göra något för att det inte ska ske.

2.3.1 Anmäla incidenter och tillbud

Upptäcker, eller misstänker, du att en incident eller tillbud har skett ska du rapportera detta till din närmaste chef, eller om du arbetar i en krets till din kretsstyrelse. Rapporteringen bör ske så fort som möjligt för att ärendet ska kunna hanteras skyndsamt.

2.3.2 Anmäla IT-incidenter

Om det är en IT-incident ska du kontakta IT servicedesk. Alla som använder Svenska Röda Korsets IT-resurser ska notera och rapportera observerade eller misstänkta incidenter. Rapportering kan göras dygnet runt via deras tjänsteportal[3] eller mejl till servicedesk@redcross.se.

Incidenter ska hanteras skyndsamt. För att säkerställa att eventuella incidenter får minimal påverkan på vår verksamhet följs en formaliserad intern process för hantering av incidenter. Genom denna process ser vi till att lämpliga åtgärder kan vidtas både på kort och på lång sikt.

3 ROLLER OCH ANSVAR

Det är viktigt att alla rödakorsare är medvetna och har grundläggande kunskap om informationssäkerhet. För detta krävs regelbunden utbildning och information om de krav och rutiner som gäller.

Grundprincipen är att ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret. Det gäller från ledningsgrupp till den enskilde medarbetaren, och innebär att den som är ansvarig för ett visst verksamhetsområde också är ansvarig för informationssäkerheten inom det. Chefer och kretsstyrelser har därmed ett särskilt ansvar att se till att medarbetare och frivilliga är införstådda i de verksamhetsspecifika regler som gäller.

För det övergripande informationssäkerhetsarbetet har dock vissa roller ett särskilt ansvar, dessa listas och beskrivs nedan:

Kretsstyrelser är ytterst ansvariga för informationssäkerheten inom sin verksamhet, Svenska Röda Korset har dock ett ansvar att skapa förutsättningar för kretsarna att uppnå en god informationssäkerhet genom exempelvis utbildningar och stöd.

Generalsekreterare är ytterst ansvarig för Svenska Röda Korsets verksamhet i enlighet med styrelsens beslut. Generalsekreteraren ansvarar även för att riktlinjer hålls aktuella samt för att planlägga och löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.

Informationssäkerhetsansvarig har det övergripande och strategiska ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet. Informationssäkerhetsansvarig ska arbeta i samråd med IT-chef, IT-säkerhetsansvarig och enhetschef för digital utveckling.

IT-chef på Svenska Röda korset ansvarar för att säkerheten i organisationens IT-miljö är tillförlitlig och motsvarar interna (verksamhetens) och externa (legala) krav. IT-enheten har även ansvar för att säkerställa att IT-systemen fungerar tillfredsställande samt att bidra med

[3] Länk till Servicedesks tjänsteportal där IT-incidenter ska rapporteras: https://kompassen.redcross.se/hc/sv/articles/360000447017-Registrera-%C3%A4rende-hos-IT-Servicedesk

kontinuerlig utveckling på respektive avdelning och har befogenheter att utveckla rutiner och processer så att verksamheten kontinuerligt effektiviseras.

IT-säkerhetsansvarig på Svenska Röda Korset är samordningsansvarig för IT-säkerhetsarbetet inom organisationen och säkerställer att Svenska Röda Korset tillhandahåller relevant information kring IT-säkerhetsfrågor.

Dataskyddsombudet på Svenska Röda Korset har det övergripande ansvaret för att säkerställa att vi efterlever gällande lagstiftning rörande skydd av personuppgifter (se vidare Svenska Röda Korsets riktlinje för skydd av personuppgifter).

Anställda har ett ansvar att hantera information på ett säkert sätt och vara uppmärksamma på brister och incidenter rörande informationssäkerheten, samt att meddela dessa till närmaste chef eller kretsstyrelse, eller till servicedesk om bristerna gäller IT. Vill du som anställd ha stöd eller vägledning kring hur du säkerställer en högre informationssäkerhet, vänd dig till din närmaste chef eller kretsstyrelse om du är anställd i krets.

4 UPPFÖLJNING OCH RAPPORTERING

Informationssäkerhetsansvarig tillsammans med IT-säkerhetsansvarig ska årligen rapportera läge och status gällande informationssäkerhet till generalsekreteraren och Svenska Röda Korsets styrelse. Särskilda skäl, som exempelvis allvarliga incidenter, brister eller behov, kan motivera ytterligare rapporteringar.