EN GUIDE FÖR TILLRÄCKLIGT GOD INFORMATIONSSÄKERHET VID INFÖRANDE AV VÄLFÄRDSTEKNIK OCH DIGITALA TJÄNSTER

2021-11-02

Sveriges Kommuner och Regioner

Inledning

Informationssäkerhet upplevs av kommuner som ett abstrakt område. Det finns mycket material om informationssäkerhet framtaget på nationell nivå, men aktörerna är många och mängden information så pass omfattande att det kan bli svårt för kommuner att navigera i materialet. Det kan vara en anledning till att informationssäkerhetsarbetet vid införandet av välfärdsteknik och digitala tjänster inom äldreomsorgen inte görs tillräckligt, är lågt prioriterat eller att kunskap saknas. Kompetenscenter Välfärdsteknik har utifrån dessa utgångspunkter skapat denna guide för att stödja kommuner att uppnå tillräckligt god informationssäkerhet.

Informationssäkerhet är det arbete som görs för att hindra att information läcker ut, förvanskas eller förstörs, men det ingår även att se till att information är tillgänglig när den behövs. Grundprincipen är att ansvaret för själva informationssäkerhetsarbetet ska ligga i det ordinarie verksamhetsansvaret. Denna guide vänder sig därför till medarbetare inom vård och omsorg som på ett eller annat sätt har ansvar för informationssäkerheten i uppdrag, projekt, processer eller liknande. I sammanhanget blir denna guide särskilt lämplig för projektledare, digitaliseringsstrateger och utvecklare som arbetar med införande av välfärdsteknik och digitala tjänster.

Myndigheten för samhällsskydd och beredskap (MSB) har tagit fram ett omfattande material som finns på informationssäkerhet.se och flera av de länkar som finns i delområdena nedan hänvisar till det materialet. MSB har tagit fram ett översiktligt metodstöd om systematiskt informationsarbete och hur det kan gå tillväga. Metodstödet grundas på de internationella standarderna för informationssäkerhet i ISO/IEC 27000-serien.

IMY:s (Integritetskyddsmyndigheten) beskrivning av informationssäkerhet

SIS:s (Svenska Institutet för standarder) beskrivning av informationssäkerhet

SKR:s (Sveriges Kommuner och Regioner) beskrivning av informationssäkerhet i generella drag och om informationssäkerhet avs välfärdsteknik

MSB:s metodstöd för systematiskt informationssäkerhetsarbete

Informationssäkerhet.se metodstöd för systematiskt informationssäkerhetsarbete

En översikt om MSB:s metodstöd

Sveriges Kommuner och Regioner
info@skr.se, www.skr.se
Post: 118 82 Stockholm *Besök:* Hornsgatan 20
Tfn: 08-452 70 00 *Org nr:* 222000-0315

Pressjour: 08-452 71 01
press@skr.se

Innehållsförteckning

Guide för tillräckligt god informationssäkerhet 1
1. Ledningssystem 1
2. Säkra informationen 2
Kontrollera åtkomst 2
Klassning av information 2
3. Säkra nätverket 3
Flexibel och säker åtkomst 3
Analys och skydd 3
4. Säkra enheterna 4
Säkra Operativsystem 4
5. Säkra identiteterna 5
Användar-ID 5
Lösenord 5
Stark autentisering 5
6. Information och utbildning för medarbetare 5
7. Information och utbildning till brukare 6

Sveriges Kommuner och Regioner
info@skr.se, www.skr.se
Post: 118 82 Stockholm *Besök:* Hornsgatan 20
Tfn: 08-452 70 00 *Org nr:* 222000-0315

Pressjour: 08-452 71 01
press@skr.se

Sveriges Kommuner och Regioner

Guide för tillräckligt god informationssäkerhet

Ur ett informationssäkerhetsperspektiv finns det sju aspekter som behöver säkerställas för att uppnå en acceptabel säkerhetsnivå när välfärdsteknik och digitala tjänster introduceras i kommunal äldreomsorg. I den här guiden har dessa sju aspekter sammanfattats i sju avsnitt med grundläggande information. För att få mer kunskap finns det under varje avsnitt länkar till myndigheter och andra organisationer som tagit fram material i sammanhanget.

1. Ledningssystem

All verksamhet förutsätter en organisation, medarbetare och strukturer. Att upprätthålla kvaliteten i en verksamhet förutsätter ett systematiskt och fortlöpande arbete med alla dessa delar, vilket socialtjänsten är van vid i arbete med ledningssystem för kvalitet (SOSFS 2011:9). Informationssäkerhet är inget undantag, men det är ett kommunövergripande ledningssystem till skillnad från ledningssystem för kvalitet som enbart berör socialtjänsten och hälso-och sjukvård i kommunen. Ett ledningssystem för informationssäkerhet (LIS) fungerar som ett stöd för styrning av informationssäkerhetsarbetet. Det ger en överblick för kontroll och granskning av informationssäkerheten för att kunna säkerställa att samtliga informationstillgångar är skyddade.

Grunden till LIS är de fem internationella ISO-standarder som kallas 27000-serien. Dessa fem standarder innehåller begreppsdefinitioner, krav för att införa ett LIS, vägledning för att tolka kraven, riktlinjer för säkerhetsåtgärder och riskhantering samt vägledning för hur effekten av LIS kan mätas och bedömas. Det finns också en svensk standard för informationssäkerhet inom hälso- och sjukvården som bygger på patientdatalagens bestämmelser och ISO/IEC 27002 med benämningen SS- EN ISO 27799. Som en vägledning i arbetet kan socialtjänsten använda Socialstyrelsens föreskrift HSLF-FS 2016:40 som är framtagen för hälso- och sjukvården.

Utifrån dessa standarder skapar LIS förutsättningar för ett strukturerat och systematiskt informationssäkerhetsarbete. Det underlättar också för verksamheten att uppnå aktuella krav och ramverk som kommunen måste förhålla sig till, såsom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen) och EU:s Dataskyddsförordning (GDPR), såväl som att agera vid snabba omställningar och situationer.

Sveriges Kommuner och Regioner
info@skr.se, www.skr.se
Post: 118 82 Stockholm *Besök:* Hornsgatan 20
Tfn: 08-452 70 00 *Org nr:* 222000-0315

Pressjour: 08-452 71 01
press@skr.se

Av ledningssystemet ska det exempelvis framgå hur informationssäkerhetsarbetet i kommunen ska organiseras och planeras, vilka roller som omfattas, deras ansvar samt hur incidenter ska hanteras. Detta genom policys, styrdokument, riktlinjer och processer som nämnden (vanligtvis) har antagit och beslutat om. Dessa behöver därefter kommuniceras ut till alla medarbetare i hela verksamheten.

MSB:s beskrivning av Ledningssystem

Informationssäkerhet.se sammanfattning av ISO 27000-serien

Svenska Institutet för Standarders (SIS) sammanfattning av ISO 27000

Ledningssystem för informationssäkerhet i hälso- och sjukvården

Socialstyrelsens föreskrift och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården, HSLF-FS 2016:40

SKR:s förklaring av NIS-direktivet

IMY:s introduktion till GDPR

2. Säkra informationen

I det systematiska informationssäkerhetsarbetet ingår att ha framtagna rutiner som beskriver vad som ska göras, av vem och med vilken intervall för att säkra informationen.

Kontrollera åtkomst

En del i att säkra informationen handlar om att kontrollera att inte obehöriga har åtkomst till information. Detta kan man till exempel göra genom kontinuerliga loggkontroller där man bland annat kan se misslyckade inloggningsförsök, sökningar och att bara personal med rätt behörighet har tillgång till informationen.

MSB:s information om att följa upp och bevaka

Klassning av information

Information som hanteras kan ha olika behov av skydd. Varje system eller tjänst behöver utredas för att bedöma vilken skyddsnivå som är lämplig. Exempel på system eller tjänst kan vara verksamhetssystem, planeringssystem, kommunikationssystem, sensorer och mobila trygghetslarm.

Skyddsnivå bestäms utifrån de tre olika perspektiven konfidentialitet, riktighet och tillgänglighet.

- Konfidentialitet: **endast** behöriga personer får ta del av informationstillgångarna.
- Riktighet: informationstillgången går att lita på, den är korrekt och inte manipulerad.
- Tillgänglighet: informationstillgången finns tillgänglig när den behövs.

För varje av ovanstående perspektiv bedöms sedan hur stora eller små konsekvenserna blir om informationen skulle läcka ut. Här används tre nivåer av konsekvenser: *allvarlig, betydande* och *måttlig*. Klassificeringen ger ett stöd för den som hanterar informationstillgången hur informationen värderas och ger på så sätt en vägledning på vilka hanteringskrav som ska appliceras.

SKR:s självskattningsverktyg KLASSA

SKR:s vägledning om KLASSA

SKR:s normativa vägledning om KLASSA för IoT

SKR:s vägledning Upphandling av välfärdsteknik 3.0

3. Säkra nätverket

Information kan skyddas med hjälp av nätverksåtgärder, framförallt för att hindra obehörig åtkomst. Med nätverk menas både trådbundet nätverk och trådlös Wi-Fi som antingen är öppet/publikt eller skyddat/privat.

Flexibel och säker åtkomst

Nätverk inom vård och omsorg ska inte vara öppet för alla. Syftet med det är att skydda sekretessbelagd information och för att bevara ordning och reda, spårbarhet och kvalitet. Säkerställ att de nätverk som används är säkra och stabila för att skydda integritet och användning av data.

Användare och enheter som behöver tillgång till nätverket ska kunna identifieras. Detta för att hantera övriga användare och bedöma om de ska ges begränsad åtkomst, blockeras eller tas bort. Kommunens egna nätverk har vanligtvis sådana typer av åtkomstkontroller redan etablerade, likaså i nätverk på boenden och i andra verksamheter.

Analys och skydd

Inom allt informationssäkerhetsarbete är det centralt att tänka utifrån risker och att identifiera samt bedöma eventuella risker som skulle kunna äventyra informationssäkerheten. Detta görs genom en riskanalys.

Det kan handla om både oavsiktliga incidenter orsakat av mänskliga faktorn samt avsiktliga angrepp med ekonomisk, politisk eller brottslig motivering. Ett exempel på

risk med nätverk är driftstörningar, vilket i sin tur medför förlust av åtkomst till verksamhetssystem. Andra exempel på risker är återkommande uppkopplingsproblem, systemfel och buggar.

En riskanalys går ut på att besvara frågorna ”Vad kan hända?”, ”Hur påverkas de registrerade?”, ”Hur sannolikt är det?” och ”Vad blir konsekvenserna?”. Därefter formuleras åtgärder, hur hotet ska bemötas utifrån fyra strategier (accepteras, minskas, överföras, undvikas), varje risk ska sedan tilldelas en ansvarig person (riskägare) som ansvarar för uppföljning.

MSB:s vägledning om riskanalys

MSB:s rekommendation för kontinuitetshantering

Säkerhetspolisens rekommenderade åtgärder för cybersäkerhet

4. Säkra enheterna

Inom vård och omsorg har datorer, läsplattor och mobiltelefoner blivit alltmer betydelsefulla för att utföra arbetsuppgifter och insatser. För att skydda informationen som hanteras i dessa enheter, exempelvis i mobil dokumentation och digitala scheman, blir det viktigt att säkra enheternas operativsystem.

Säkra Operativsystem

Operativsystem är ett eller flera program som sköter datorns och mobiltelefonens inre arbete. Exempel på operativsystem för datorer är Windows och Mac OS, för mobiltelefoner Android samt iOS. Vid införskaffande eller uppföljning av befintliga operativsystem behöver man säkerställa att de operativsystem som används eller ska användas uppfyller grundläggande krav och kriterier på säkerhet.

Precis som när man säkrar informationen (avsnitt 2, ovan) genom loggkontroller kan man även här använda sig av loggning för att identifiera och agera på obehörig användning och på så vis säkra operativsystemet. Loggningen kan anpassas efter kommunens behov. Loggning gör det möjligt att övervaka aktiviteter som till exempel en viss händelse, tidpunkt och vem som haft tillgång.

För arbetet med systematisk informationssäkerhet förutsätter det att det finns krav, rutiner och åtgärder fastställda och att arbetet genomförs kontinuerligt. Här kan det handla om att ha verktyg för hantering av eventuella risker, att det framgår vad som ska göras när och om enheten inte fungerar samt att det finns en framtagen åtgärdsplan.

MSB:s information om rekommenderade säkerhetsåtgärder

5. Säkra identiteterna

För att skydda informationen i ytterligare ett steg är att endast behöriga får tillgång till system och nätverk.

Användar-ID

Varje användare tilldelas en unik användaridentitet som består av en särskild kombination av bokstäver och siffror och är knuten till ett användarkonto. För att exempelvis få åtkomst till ett verksamhetssystem eller planeringssystem krävs vanligtvis både ett användar-ID och ett personligt lösenord. Gruppkonton får inte förekomma.

Lösenord

Säkerställ att kommunen har starka lösenord vid inloggning eftersom lösenord är den främsta åtgärden som förhindrar att obehöriga får tillgång till information och användarkonton. Ett starkt lösenord innehåller minst 12 tecken av både stora och små bokstäver, siffror och specialtecken. Här gäller det att inte använda uppgifter såsom namn och favorithobby eller vanligt förekommande ord som kan kopplas till användaren.

Stark autentisering

Autentisering handlar om att bekräfta användarens identitet. För känslig information används vanligen en stark autentisering, som är en tvåstegsinloggning som betyder att en identitetskontroll görs med hjälp av två skilda former av information. Man brukar säga att det är någonting man *har* (tagg, certifikat, koddosa), någonting man *vet* (lösenord, PIN) och/eller någonting man *är* (biometri). Det kan till exempel vara en kombination av en tagg och sifferkod för att öppna ett digitalt lås, eller ett SITHS-kort och pinkod för att komma åt ett verksamhetssystem.

Det saknas tydliga lagkrav för socialtjänsten för autentisering vid åtkomst till patient- eller brukaruppgifter i öppna nätverk, såsom internet och molntjänster. Eftersom risken för obehörig åtkomst är sannolikt hög bör stark autentisering alltid användas vid åtkomst till patient- eller brukaruppgifter i öppna nätverk.

MSB:s information om säkra lösenord

Socialstyrelsens stöd om elektronisk åtkomst för hälso- och sjukvård

6. Information och utbildning för medarbetare

Informationssäkerhet omfattar alla medarbetare. I det kontinuerliga arbetet med att uppnå och säkerställa informationssäkerhet samt stärka säkerhetskulturen är medarbetarens kunskap av yttersta väsentlighet. Kunskapen främjas genom att

tillgängliggöra information kontinuerligt för medarbetarna och att de känner till vem de vänder sig till vid frågor.

Medarbetarnas kunskap säkras genom utbildning. Vård och omsorg hanterar känslig och konfidentiell information därför behövs det skapas en gemensam förståelse för grundläggande informationssäkerhet och digital säkerhet. Exempelvis genom hur arbete med dator, mobil och annan digital teknik sker på ett säkert sätt. Saknas resurser för att skapa egen utbildning finns MSB:s grundläggande utbildningsprogram Digitala informationssäkerhetsutbildning. Även If Skadeförsäkring erbjuder en kostnadsfri kurs om informationssäkerhet för verksamheter.

MSB:s utbildning Digital informationssäkerhetsutbildning för alla (DISA)

If:s kurs i informationssäkerhet

7. Information och utbildning till brukare

När välfärdsteknik eller digitala tjänster ska testas, köpas in och införas behöver brukare informeras om det både före, under och efter sådana initiativ. Detta för att främja digital delaktighet och öka den enskildes kunskap om exempelvis trygg användning och säker inloggning.

I det systematiska informationssäkerhetsarbetet ingår det att ha generella rutiner för hantering av personuppgifter och konfidentiell information. Det ingår även att kontinuerligt informera brukare om hur deras personuppgifter behandlas. Vidare behöver rutinerna anpassas så att de stämmer överens med aktuell välfärdsteknik eller digital tjänst.

För att öka digitala delaktighet finns flera verktyg att tillgå. Arbetsförmedlingen och Google Digitalakademin har utformat korta grundläggande kurser om digitala kunskaper på webbplatsen Digitala jag, däribland om säkerhet och integritet vid användning av digitala tjänster. Det finns utbildning om bland annat virus och integritet som Kungliga biblioteket erbjuder kostnadsfritt. Även Post- och Telestyrelsen (PTS) har tagit fram vägledning som underlättar äldres vardag genom guider, kurser och inspiration. Ytterligare exempel på handledning är Demensförbundets instruktioner för digitala möten, fotodelning och online handel.

Digitala jag kurs om säkerhet och integritet

Kungliga bibliotekets utbildning Digiteket

PTS vägledning Digitalhjälpen

Demensförbundets instruktioner om Surfa, handla och umgås digitalt