Revisionsrapport 2021
Genomförd på uppdrag av revisorerna
September 2021

Granskning av säkerhet och sekretess vid hemarbete

Strömsunds kommun

Building a better working world

Innehåll

1. Sammanfattning

EY har på uppdrag av kommunens förtroendevalda revisorer granskat om kommunstyrelsen och nämnderna har säkerställt att arbetet med IT-säkerhet och sekretess vid hemarbete bedrivs på ett ändamålsenligt sätt och med tillräcklig intern kontroll.

Vår sammanfattande bedömning är att kommunstyrelsen och nämnderna delvis har säkerställt att arbetet med IT-säkerhet och sekretess vid hemarbete bedrivs på ett ändamålsenligt sätt och med tillräcklig intern kontroll.

Vi grundar vår bedömning på att medarbetare vid början av hemarbete fått grundläggande information om de förhöjda riskerna, grundläggande utbildning har inletts och ordinarie rutiner är delvis tillämpliga även vid hemarbete. Det saknas dock specifika riktlinjer för hemarbete och vi bedömer att dessa är nödvändiga att upprätta för att säkerställa IT-säkerhet och sekretess vid hemarbete. Det finns ett flertal förhöjda risker att hantera, ex. behörighetstilldelning, för att inte obehörig ska få tillgång till information.

Vidare finns inga särskilda rutiner för att anmäla säkerhetshot/incidenter och förteckningslista som ska specificera till vem anmälan ska göras är inte uppdaterad. Dataskyddsförordningen ställer tydliga krav på snabb och varsam hantering av eventuella personuppgiftsincidenter. Enligt enkät är det en relativt stor andel som inte har kännedom hur en anmälan ska genomföras.

Vi har bland annat gjort följande iakttagelser:

- Det saknas särskilda riktlinjer för informationssäkerhet/sekretess vid distansarbete.
- Det saknas en uppdaterad förteckning över samtliga system med namngivna rollinnehavare, bl.a. vem incidenter ska anmälas till.
- Det saknas dokumenterade rutiner/riktlinjer för anmälan av säkerhetshot och personuppgiftsincidenter.
- Det är en låg andel av medarbetarna som vet hur de ska anmäla säkerhetshot/personuppgiftsincidenter (63% respektive 53% enligt enkät).
- Utbildning upplevs i stort som positiv av medarbetare men vissa saknar en mer djupgående utbildning.
- Det sker ingen specifik uppföljning av säkerhet och sekretess vid hemarbete. Dock saknas riktlinjer att följa upp efterlevnaden mot.

2. Inledning

2.1 Bakgrund

I ungefär ett års tid har kommuner och offentliga myndigheter uppmanat medarbetare att arbeta hemifrån för att begränsa spridningen av Covid-19. Enligt SCB:s arbetskraftsundersökning för juli-september 2020 jobbade ca en tredjedel av de tillfrågade medarbetarna i offentlig förvaltning huvudsakligen hemifrån.

Arbete i hemmet ökar risken för dataintrång och skadliga angrepp mot kommuner. En angripare kan komma åt information i hemmiljön eller öppna för åtkomst in i en organisations system.

En annan risk med hemarbete är hanteringen av sekretessbelagd information och personuppgifter. När arbetsmaterial och utrustning är i rörelse ute i samhället ökar riskerna för att papper, datorer och telefoner ska hamna i orätta händer eller skadas. Att hantera känsliga personuppgifter utanför en organisations fysiska skydd är enligt SKR egentligen inte lämpligt.

Det är väsentligt att kommunen vidtar säkerhetsåtgärder i syfte att hindra att obehöriga får tillgång till personuppgifter, sekretessbelagda uppgifter eller att de förstörs oavsiktligt även om arbetet sker hemma hos den anställde.

Revisorerna har mot bakgrund av ovanstående beslutat att granska hur kommunen arbetar med att garantera säkerhet och sekretess vid hemarbete.

2.2 Syfte och revisionsfrågor

Det övergripande syftet med granskningen är att bedöma om styrelsen och nämnderna har säkerställt att arbetet med IT-säkerhet och sekretess vid hemarbete bedrivs på ett ändamålsenligt sätt och med tillräcklig intern kontroll.

Inom ramen för ovanstående syfte ska följande revisionsfrågor besvaras:

- Finns tydliga och aktuella riktlinjer för såväl informationssäkerhet som sekretess vid distansarbete?
- Har i så fall dessa riktlinjer kommunicerats och gjorts tillgängliga för alla medarbetare som arbetar på distans?
- Finns tillräcklig kapacitet och säkra inloggningar för distansarbete?
- Har information/utbildning genomförts för personal som arbetar på distans? Tex angående sekretess, risk för bedrägeri mm.
- Finns fungerande rutiner för skyndsam hantering av eventuella incidenter?
- Sker en tillräcklig uppföljning och kontroll av säkerhet och sekretess vid hemarbete?

2.3 Avgränsning

Granskningen omfattar kommunstyrelsen, socialnämnden och barn-, kultur- och utbildningsnämnden.

2.4 Genomförande

Granskningen genomfördes med hjälp av granskning av dokumentation samt kompletterande intervjuer med IT-chef och biträdande förvaltningschef på kommunledningsförvaltningen. Därutöver genomfördes en enkät bland medarbetare som arbetar på distans. Enkäten besvarades av 393 medarbetare som arbetat på distans.

2.5 Revisionskriterier

Med revisionskriterier avses bedömningsgrunder som används i granskningen för analyser, slutsatser och bedömningar. Revisionskriterierna kan hämtas från lagar och förarbeten eller interna

regelverk, policyer beslutade av fullmäktige. Kriterier kan också ha sin grund i jämförbar praxis eller erkänd teoribildning. I denna granskning utgörs de huvudsakliga revisionskriterierna av:

- Kommunallagen (2017:725)
- Offentlighets- och sekretesslag (2009:400)
- GDPR
- Stödjande material från MSB och SKR
  - Kommunens informationssäkerhet – en vägledning (MSB 2012)

2.5.1 Informationssäkerhet

MSB definierar informationssäkerhet enligt följande i sin vägledning för kommunens informationssäkerhet 2012 (senast granskad 2019).

Informationssäkerhet handlar om att ge kommunens information rätt skydd. Det omfattar hela kommunens verksamhet och all information, oavsett om den finns i datorer, i ett telefonsamtal eller på papper. Rätt skydd omfattar följande områden:

- *Tillgänglighet:* Information är tillgänglig i förväntad utsträckning och inom önskad tid.
- *Riktighet:* Informationen skyddas mot oönskad och obehörig förändring eller förstörelse.
- *Konfidentialitet:* Informationen tillgängliggörs inte i strid med lagkrav eller lokala överenskommelser eller delges obehörig.
- *Spårbarhet:* Att i efterhand kunna spåra aktiviteter eller händelser till ett identifierat objekt eller användare.

2.5.2 MSB råd om informationssäkerhet vid distansarbete

MSB har av anledning av ökat distansarbete i samband med coronapandemin utformat råd för att säkerställa informationssäkerheten. Råden riktar sig både till den som samordnar organisationens informationssäkerhet och medarbetare som arbetar på distans.

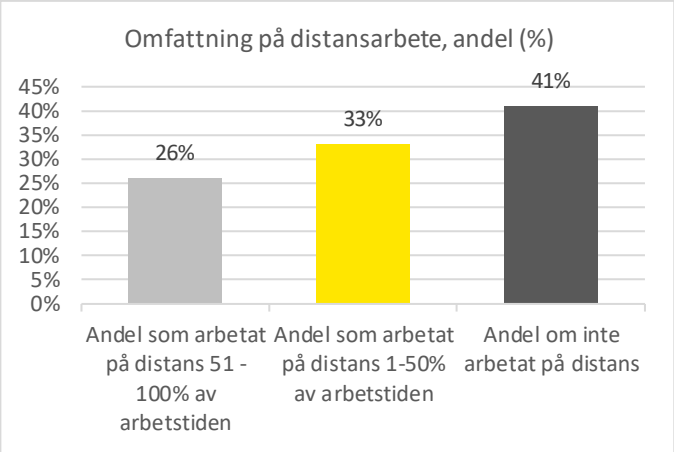
Enligt råden är det viktigt att behandla bl.a. följande frågeställningar i organisationen:

- Finns aktuella regler för distansarbete och användning av IT-system utanför organisationen?
- Vilken kapacitet har organisationen avseende hur många som kan arbeta på distans?
- Finns säkra inloggningar för distansarbete?
- Fångas incidenter upp och hanteras snabbt?
- Finns säkra arbetssätt för behörighetstilldelning vid distansarbete?

3. Granskningsresultat

3.1 Riktlinjer för informationssäkerhet och sekretess

Coronapandemin har resulterat i att personal i större omfattning än vanligt arbetar hemifrån för att minska smittspridningen. I genomförd enkät är det 59 % som svarat att de i någon omfattning arbetat hemifrån under pandemin. Se diagram till höger.



Det innebär att information hanteras och kommuniceras på ett annat sätt än tidigare. Det ställer krav på kommunen att säkerställa att information och sekretess hanteras på ett säkert sätt även i denna nya situation.

I MSB råd för att säkerställa informationssäkerheten vid distansarbete måste kommunen som arbetsgivare se över om det finns aktuella regler för distansarbete och användning av IT-system utanför organisationen. I nedan avsnitt redogör vi för våra iakttagelser inom detta område.

3.1.1 Riktlinjer som omfattar distansarbete saknas

Det finns inga särskilda riktlinjer för informationssäkerhet och sekretess som omfattar distansarbete.

IT-chef beskriver vid intervju att när det gäller IT-säkerheten är det liten skillnad vid distansarbete och arbete på arbetsplatsen. Detta eftersom det är samma IT-säkerhetslösningar oavsett vart datorn befinner sig fysiskt. Även biträdande förvaltningschef på kommunledningsförvaltningen beskriver att det i huvudsak är ordinarie rutiner som gäller vid hemarbete. Till exempel ska medarbetaren, oavsett om arbete sker i hemmet eller på arbetsplatsen, säkerställa att ingen obehörig kan höra ett telefonsamtal som är av känslig karaktär. Detsamma gäller dokument med sekretessbelagda uppgifter.

Enligt intervjuer håller samtliga HR-avdelningar i länets kommuner på att arbeta fram en länsgemensam riktlinje för distansarbete.

Det har på förvaltningsnivå genomförts olika riskanalyser och handlingsplaner inför hemarbete. Vi har tagit del av individ- och familjeomsorgens identifierade risker och åtgärder. Att bevara sekretessen är en av de identifierade riskerna och som åtgärd beskrivs att alla måste ta ansvar för att förhindra att obehöriga tar del av sekretessbelagda uppgifter samt att tänka på förvaringen.

3.1.2 Ordinarie rutiner

Policy för den kommunala verksamhetens IT-stöd (KF 2014-06-11)
Policy innehåller den övergripande ansvarsfördelningen och inriktningen för kommunens IT. Policy specificerar att IT-system och utrustning ska vara en stödfunktion för den kommunala verksamheten. IT-stöd är avsett och ska endast vara tillgängligt för de kommunalt anställda, förtroendevalda och skolelever. Säkerheten ska vara hög och infrastrukturen ska inte vara tillgänglig för externa aktörer.

Ansvarsfördelning i policy:

- IT-avdelningen: Har det strategiska ansvaret och driftsansvar för utveckling av IT-infrastrukturen och programvaror. IT-avdelningen ska vidare utifrån policy utfärda konkreta riktlinjer för hur kommunens IT-stöd ska hanteras (fastställda av KS 2013).
- Respektive förvaltning/avdelning ansvarar för de system som de använder.
- Kommunstyrelsen har enligt policy ansvar för att fastställa riktlinjer för att tydliggöra ansvarsfördelning och rutiner för hantering av IT-system, (fastställda av KS 2013).

Riktlinje för systemförvaltning och hantering av IT-utrustning (KS 2013-01-29)
Syftet med riktlinjen är att skapa ett samordnat, välfungerande och ändamålsenligt IT-stöd. Riktlinjen förtydligar ansvar för IT-utrustning och infrastruktur ytterligare. Det ska för varje system finnas en förvaltningsorganisation med följande:

- Systemägare: ansvarar för systemets omfattning och ekonomi.
- Systemförvaltare: ansvarar för planering, samordning och uppföljning av händelser som berör systemet och dess närmaste omgivning.
- Systemadministratör: ansvarar för att administrera behörigheter inom systemet
- Driftsansvarig: är IT-avdelningen i enlighet med policy.
- Användare: ansvarar för att rapportera fel och brister i systemet till systemförvaltaren.

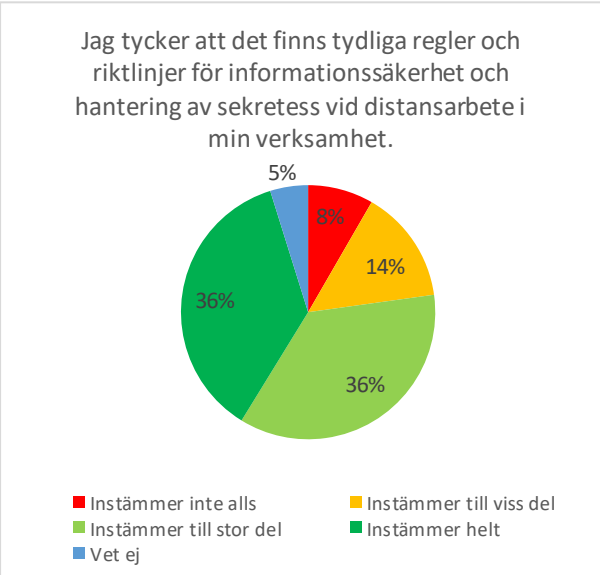
Enligt riktlinjen ska det på kommunens intranät finnas en gemensam förteckning över samtliga system med namngivna rollinnehavare enligt ovan punktlista. Enligt intervju med IT-chef är dock denna lista inte uppdaterad.

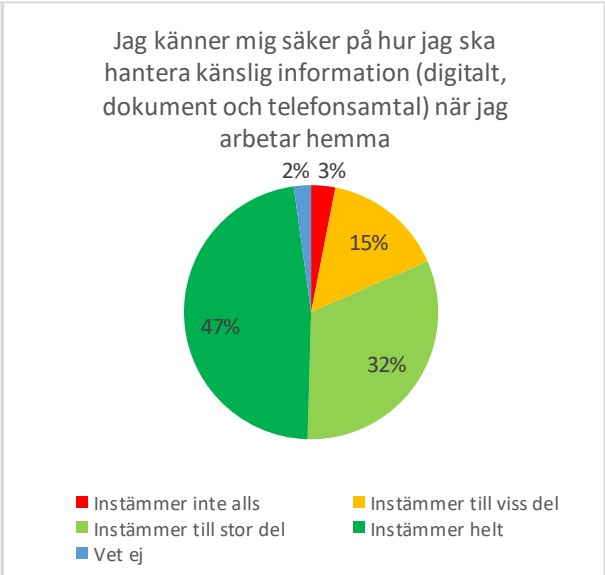
Det ligger på varje verksamhet att initiera och budgetera för inköp av verksamhetsspecifika system.

Riktlinje för hantering av uppgifter om personer med skyddad identitet (KS 2018-06-19)
Riktlinjen innehåller instruktioner för hur uppgifter om personer med skyddad identitet ska hanteras. Riktlinjen beskriver bland annat vilka kontaktvägar som kan användas och på vilket sätt information som lagras och delas kan bli säkrare. Exempelvis vilka kommunikationskanaler som är säkra och tillåtna att använda.

Enkätresultat – regler och riktlinjer

För att få en bild av hur informationssäkerheten och sekretess vid hemarbete upplevs av de anställda skickade vi ut en enkät som de fick besvara. Trots avsaknaden av specifika regler och riktlinjer för informationssäkerhet och sekretess vid distansarbete är det 72% som svarat att de instämmer helt eller stor del på frågan om det finns tydliga riktlinjer. Det är dock 22% som svarat att de inte instämmer eller endast instämmer till viss del. Vidare är det 79% som instämmer helt eller till stor del på frågan om de känner sig säkra på hur känslig information ska hanteras vid hemarbete. Se nedan diagram.





Vi har inte observerat några markanta skillnader mellan respektive förvaltning.

3.1.3 Bedömning

Det finns inga särskilda riktlinjer för informationssäkerhet eller sekretess specifikt för distansarbete. Vi bedömer att befintliga riktlinjer inte ger medarbetarna nödvändiga instruktioner för att hantera information på ett säkert sätt vid distansarbete, bortsett från Riktlinje för hantering av uppgifter om personer med skyddad identitet som reglerar kommunikationsvägar oavsett arbetsplats. Vi saknar tydliga riktlinjer som är specifika för distansarbete och som enligt MSBs vägledning för kommunens informationssäkerhet är väsentliga, t.ex. en riktlinje för mobilt arbete respektive riktlinjer för behörighetsadministration som beaktar behörighetstilldelning vid distansarbete. Ytterligare riktlinjer kan vara aktuella efter en behovsanalys. Även om majoriteten av medarbetare upplever befintliga riktlinjer som tillräckliga så är det en betydande andel som inte gör det. Det kan bero på att olika arbetsroller hanterar olika mängd information och har därmed olika behov av riktlinjer. Behov av riktlinjer har också en tendens att uppstå först efter en allvarlig incident inträffat.

3.2 Kapacitet och inloggning vid distansarbete

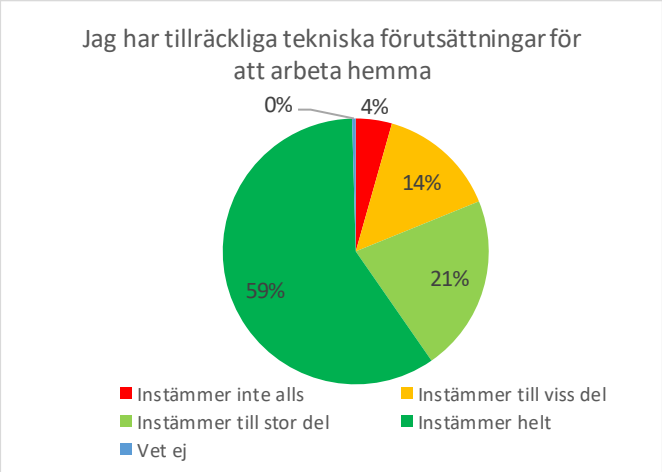
Vid distansarbete är det viktigt att medarbetare fortsatt har tillgång till de resurser och den information som de behöver för att utföra sitt arbete på ett säkert sätt. I nedan avsnitt redogör vi för våra iakttagelser kring kommunens åtgärder för att säkra tillgången till resurser och information.

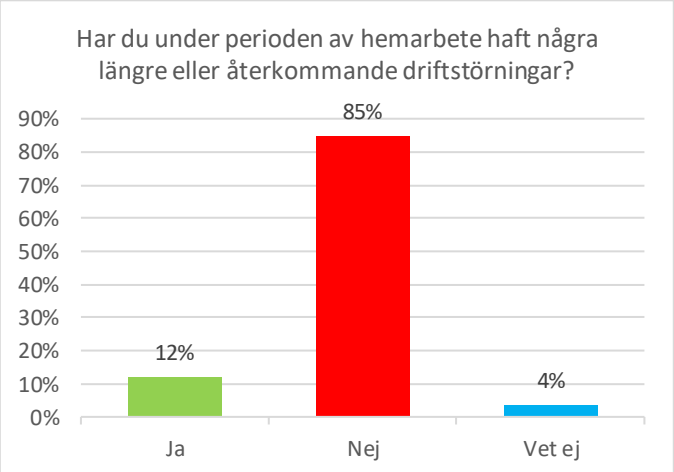
3.2.1 VPN och tekniska förutsättningar

Kommunen använder sig av VPN Cisco AnyConnect för att skapa en säker anslutning vid distansarbete. När medarbetaren loggar in på sin arbetsdator så loggar datorn även in på VPN-tjänsten. Det innebär att all datatrafik ska gå via VPN-tunneln och enligt intervju med IT-chef är kapaciteten tillräcklig även om samtliga användare är inloggade. Det innebär att samtliga kan vara uppkopplade mot VPN samtidigt och kommunen behöver inte prioritera vilka som ska vara uppkopplade. IT-chefen beskriver att IT-säkerhet via VPN-uppkopplingen är lika säker som om arbete skett på arbetsplatsen. Däremot finns alltid risken att medarbetare hanterar informationen på ett mindre säkert sätt vid distansarbete (t.ex. sparar dokument lokalt på datorn och inte låser in fysiska dokument). Vid inloggning på datorer krävs en 8 siffrig kod med versaler och siffror i kombination.

Enkätresultat – Tekniska förutsättningar

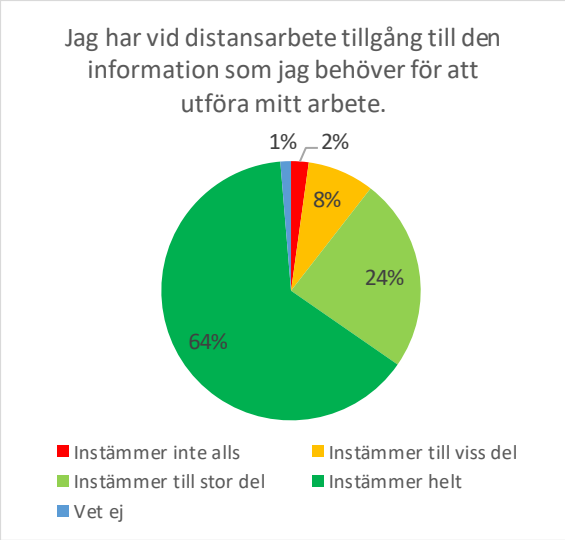
I enkät har 80% svarat det de instämmer helt eller till stor del på frågan om de har tillräckliga tekniska förutsättningar för att arbeta hemifrån (t.ex. tillräcklig internetuppkoppling m.m.). Vidare är det 12% som svarat att de någon gång drabbats av en längre eller återkommande driftstörning som påverkat arbetet. Se nedan diagram.

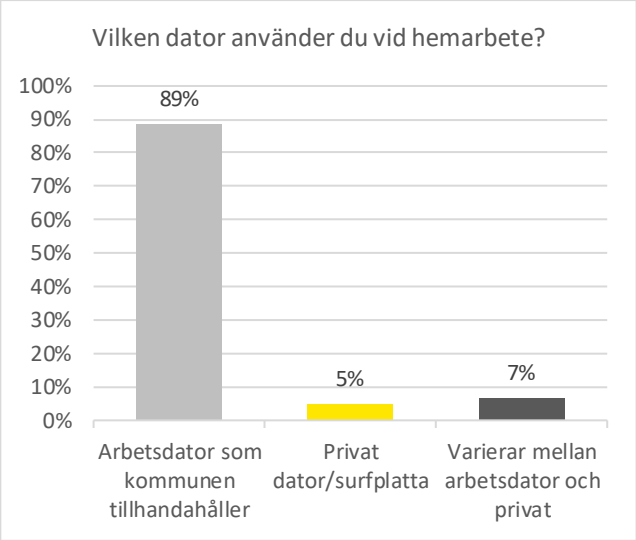




Av de medarbetare som drabbats av driftstörningar är det 11% (3 personer) som svarat att de under driftstörningen hanterade informationen på ett mindre säkert sätt, t.ex. mailade information till sin privata dator.

Den VPN-tjänst som är installerad på datorerna som kommunen tillhandahåller till medarbetarna ger tillgång till gemensamma arbetsytor, filer och annan information som krävs för att utföra arbetet. I enkät är det 88% som svarat att de instämmer helt eller till stor del på frågan om de har tillgång till den information de behöver för att arbeta hemifrån. I enkät framkommer dock att det förekommer att medarbetare använder privata datorer/surfplattor i arbetet, även om majoriteten (89%) använder sin arbetsdator. Privata datorer är inte anslutna till den VPN-tjänst som används för att skapa en säker förbindelse och skydda den information som används i arbetet.





Vissa arbetsuppgifter kan inte utföras i hemmet. Det är 74% som svarat att de varit tvungna att resa in till sin ordinarie arbetsplats för att utföra vissa uppgifter. I kommentarerna uppges att det främst är lärare som av olika anledningar behövt hålla fysiska lektioner eller tjänstepersoner som åkt in till arbetsplatsen för att skriva ut dokument samt kolla posten. Vidare har flertalet uppgett att de åkt in till kontoret för underskrifter.

3.2.2 Bedömning

Vi bedömer att det i allt väsentligt finns tillräcklig kapacitet och säkra inloggningar för distansarbete.

Kommunen använder sig av VPN, vilket är en vedertagen teknisk lösning för att skapa en skyddad nätverksanslutning och höja informationssäkerheten. Majoriteten av medarbetare som svarat på enkäten uppger att de har tillräckliga tekniska förutsättningar och tillgång till nödvändig information för att utföra sitt arbeta på distans. Vissa uppgifter måste dock utföras plats och kan inte ersättas av något digitalt arbetssätt, t.ex. rättning av praktiska prov. Dock finns digitala underskriftstjänster som kan ta bort behovet av att åka in till sin arbetsplats för att underteckna dokument. Vidare förekommer, dock i liten omfattning enligt enkät, att medarbetare hanterar arbetsinformation på sin privata dator som inte är ansluten via VPN.

3.3 Utbildning och information

För att information ska hanteras säkert krävs inte bara regler och tekniska lösningar som ökar säkerheten. Det är väsentligt att berörda medarbetare får information och utbildning i vilka regler som gäller respektive hur de ska tillämpas. Vidare är det viktigt att medarbetare får utbildning för att hantera de utökade risker som följer av hemarbete.

3.3.1 Information

Efter att krisledningsgruppen i april 2020 beslutat att alla som har möjlighet att utföra sina arbetsuppgifter hemifrån ska göra det, så har de informerat medarbetarna om vissa riktlinjer. Informationen har publicerats på kommunens intranät och innehåller viss vägledning om informationssäkerhet vid hemarbete. Informationen belyser att det vid hemarbete är extra viktigt att tänka på hur känslig information tas emot, hanteras och sprids.

Informationen lyfter särskilt fram nedan risker:

- Förvara information i pappersform och i anteckningar på ett säkert sätt. Säkerställ att inte andra kan komma åt informationen.
- Vid digitala möten, bedöm risken att andra kan höra eller se informationen som förmedlas.
- Lås alltid datorn när du går ifrån arbetsplatsen
- Låt ingen annan använda din arbetsdator.
- Använd inte USB-minnen mellan din arbetsdator och din privata dator.
- Skicka inte känslig information via e-post.
- Bedrägeriförsöken har blivit fler under den senaste tiden. Var särskilt uppmärksam på e-post och sms som verkar misstänkt. Klicka inte på länkar eller bilagor från okända avsändare. Ladda inte ner program som kommer via e-post, sms eller olika webbsidor.

Informationen grundas på genomförd risk- och konsekvensanalys för hanteringen av coronarelaterad information.

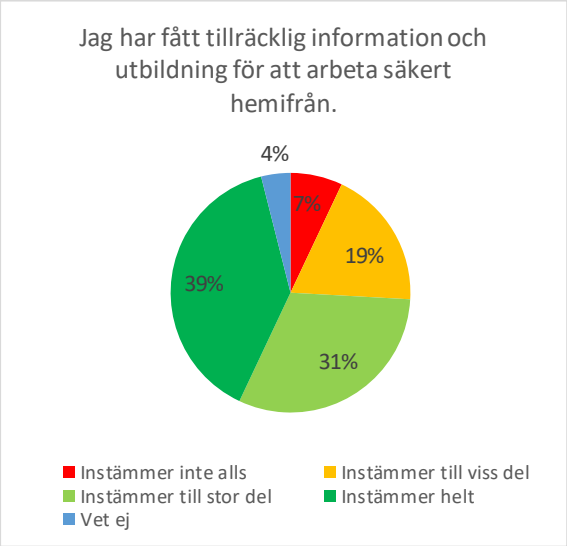
3.3.2 Utbildning

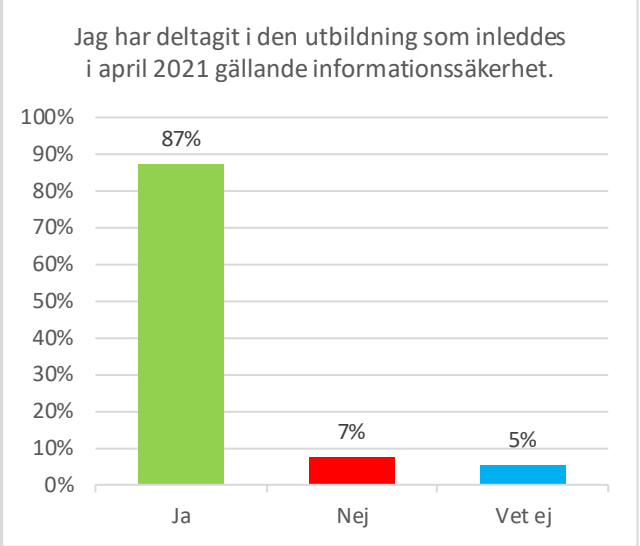
En utbildning gällande informationssäkerhet är påbörjad i april 2021 och beräknas pågå till slutet av 2021. Utbildning är inköpt via Junglemap som tillhandhåller olika kurser kring informationssäkerhet. Den kurs som är påbörjad inom kommunen heter "Digital säkerhet" och riktar sig till samtliga medarbetare för att stärka deras kunskaper kring digital informationssäkerhet. Kursen ges ut genom så kallad nanolearning, d.v.s. att kursen ges ut i små doser under en längre tid. Varannan tisdag skickar IT ut ett mail med digitalt utbildningsmaterial. Kursen består av totalt 14 utbildningstillfällen.

Intervjuade personer upplever att utbildningen har ökat medvetenheten kring de risker som finns kopplade till informationssäkerheten kopplade till IT. Det har varit fler som hört av sig till IT-support med ärenden kring säkerhet. Eventuellt kommer nyckelpersoner inom informationssäkerhet utbildas ytterligare för att erhålla spetskompetens.

Enkätresultat – information och utbildning

I genomförd enkät är det 70% som svarat instämmer helt eller till stor del på frågan om de upplever att de fått tillräcklig information och utbildning för att arbeta säkert hemifrån. Vidare är det 87% som deltagit i den utbildning om informationssäkerhet som inleddes i april 2021. Se nedan diagram.





Synpunkter som lämnats av de som inte upplever information och utbildning som tillräcklig är att information respektive utbildning är allmän och inte särskilt djupgående. Vidare upplever flertalet att utbildning erbjudits sent eftersom de redan arbetat hemifrån i ett år när utbildningen påbörjades.

3.3.3 Bedömning

Personal som arbetat hemifrån har fått grundläggande information om de mest överhängande riskerna som bör beaktas vid hemarbete. Vidare har det i april 2021 inletts en utbildningsinsats gällande allmän informationssäkerhet kopplat till digital säkerhet. En majoritet av berörda medarbetare har enligt enkät deltagit i utbildningen och 70 % upplever information och utbildning i stort som tillräcklig. En del medarbetare upplever information och utbildning som för generell och inte tillräckligt djupgående. Vi bedömer att det troligtvis hänger ihop med avsaknaden av specifika rutiner/riktlinjer för hemarbete som kan innehålla mer detaljerade riktlinjer beroende på verksamhet.

3.4 Uppföljning, kontroller och rutiner vid incidenter

För att säkerställa efterlevnaden av riktlinjer för säkerhet och sekretess vid hemarbete är det viktigt att det genomförs en tillräcklig uppföljning och kontroller. Vidare är det viktigt att ordinarie rutiner för säkerhetskontroll inte blir lidande i för stor utsträckning på grund av hemarbetet. Hemarbete ställer ytterligare krav på tydliga och kända rutiner för en skyndsam hantering av eventuella incidenter eftersom medarbetare inte på samma sätt kan fråga kollegor om stöd.

I nedan avsnitt presenterar vi våra iakttagelser kring uppföljning, kontroller och rutiner för hantering av incidenter.

3.4.1 Uppföljning och kontroller

I intervju med IT-chef beskrivs att genom att datorerna ansluts till kommunens nätverk via VPN så upptäcks eventuell skadlig trafik av IT-säkerhetssystem på samma sätt som arbete på plats. Enligt intervju kontrollerar IT och systemansvariga loggar[1] med regelbundna mellanrum i syfte att upptäcka skadlig trafik eller läckt information. Det finns dock inga dokumenterade rutiner för hur ofta detta ska ske eller hur det ska dokumenteras. Enligt intervju har det hittills inte upptäckts någon risk eller faktiskt läckage av information. Vidare genomförs penetrationstester av konsulter som hanterar brandväggen. Vid intervju beskrivs att Strömsund är en mindre kommun och har inte resurser att genomföra alla önskvärda tester. Däremot får kommunen nytta av större kommuners

[1] Förteckning över händelser i ett system.

tester om de använder samma system eftersom systemutvecklaren släpper uppdateringar till samtliga användare för att åtgärda eventuella upptäckta brister vid test.

I övrigt har det inte genomförts någon särskild uppföljning eller kontroll av säkerhet- och sekretess specifikt för hemarbete. Däremot beskriver förvaltningschef för vård- och socialförvaltningen att de har lagt in avstämningsmöten med tätare intervall under perioden av hemarbete för att kunna stämma av eventuella frågeställningar.

3.4.2 Inaktuell förteckningslista med roller

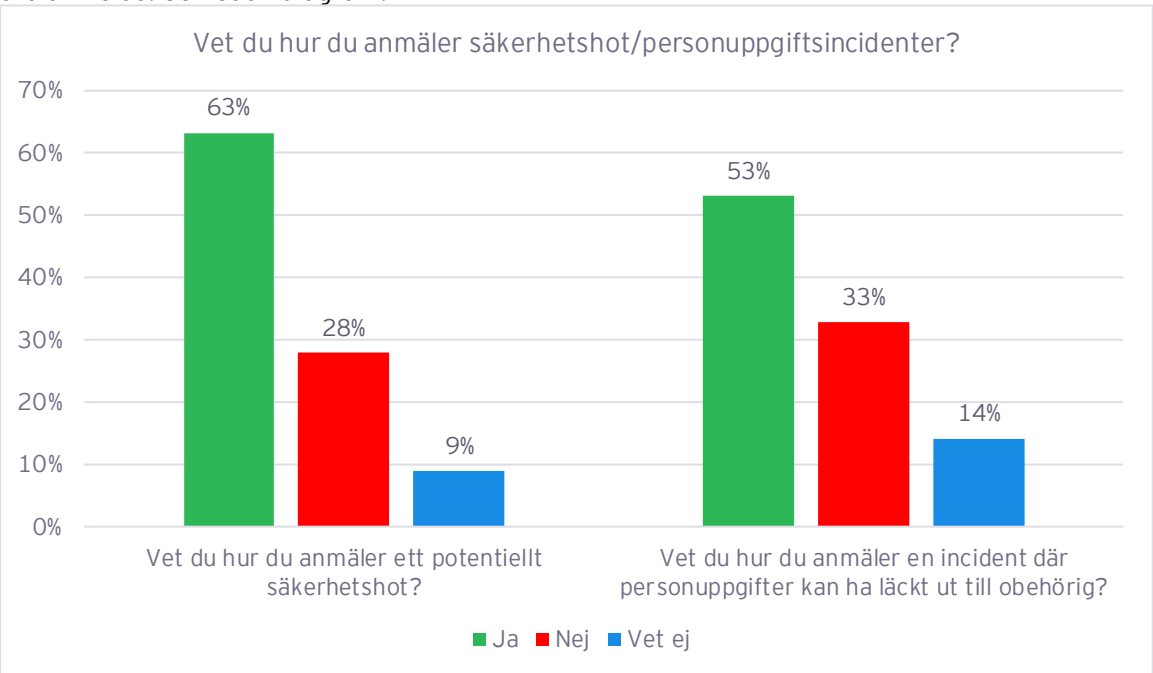
I riktlinje för systemförvaltning och hantering av IT-utrustning anges att användare av systemen ansvarar för att rapportera fel och brister i systemet till systemförvaltaren. Systemförvaltaren utses av systemägaren och ska vara namngiven på en förteckningslista som ska finnas tillgänglig på intranätet. Förteckningslistan är dock inte uppdaterad och innehåller därmed inte aktuella uppgifter om vem brister ska anmälas till. Förteckningslistan ska även innehålla uppgift om vem som är systemadministratör och ansvarig för att administrera behörigheter. Det är respektive systemägare som ansvarar för att meddela ändringar till IT-avdelningen, som uppdaterar den gemensamma förteckningen.

3.4.3 Rutiner för hantering av personuppgiftsincidenter och säkerhetshot.

Det saknas dokumenterade rutiner för att anmäla och hantera incidenter respektive säkerhetshot.

I dataskyddsförordningen (GDPR) definieras en personuppgiftsincident som "en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats".

I genomförd enkät svarar 63% att de är medvetna om till vem och hur ett säkerhetshot ska anmälas. Vid en personuppgiftincident är det endast 53% som svarat att de vet hur och till vem en incident ska anmälas. Se nedan diagram.



Av de 22 personer som någon gång anmält ett hot eller incident är det 14 personer som i enkäten uppger att de fått återkoppling på anmälan, d.v.s. 64% har fått återkoppling på anmälan.

Vid intervju med IT-chef beskrivs att nuvarande arbetssätt vid en incident är att kontakta nätverkstekniker eller IT-chef för en första bedömning av ärendet. Båda beskrivs vara tillgängliga via

telefon dygnet runt. Om nödvändigt kan de spärra uppkoppling och konton för den berörda enheten i väntan på fortsatt utredning.

3.4.4 Bedömning

Vi bedömer att det genomförs vissa kontroller av säkerhet och sekretess genom ordinarie rutiner. Det har däremot inte genomförts någon särskild uppföljning eller kontroll specifikt för hemarbete. Det blir dock svårt att göra någon särskild uppföljning eftersom det saknas särskilda riktlinjer för hemarbete att följa upp och kontrollera efterlevnaden emot.

Vi bedömer att det inte finns fungerande rutiner för skyndsam hantering av eventuella incidenter.

Vi grundar bedömningen på att förteckningslista som ska specificera roller och till vem en incident/säkerhetshot ska anmälas till är inaktuell. Artikel 33 i dataskyddsförordningen ställer dessutom krav på att personuppgiftsincidenter ska anmälas till Datainspektionen inom 72 timmar, såvida det inte är osannolikt att incidenteten medför en risk för fysiska personers rättigheter och friheter. Då det saknas en aktuell förteckningslista och särskild rutin för anmälan bedömer vi risken som stor att detta krav inte uppfylls vid en eventuell incident.

För att kunna hantera eventuella säkerhetshot samt minimera skadan vid en incident är det viktigt att samtliga i organisationen vet hur och till vem detta ska anmälas.

4. Sammanfattande bedömning

Vår sammanfattande bedömning är att kommunstyrelsen och nämnderna delvis har säkerställt att arbetet med IT-säkerhet och sekretess vid hemarbete bedrivs på ett ändamålsenligt sätt och med tillräcklig intern kontroll.

Revisionsfråga	Bedömning
Finns tydliga och aktuella riktlinjer för såväl informationssäkerhet som sekretess vid distansarbete? Har i så fall dessa riktlinjer kommunicerats och gjorts tillgängliga för alla medarbetare som arbetar på distans?	Nej. Det finns inga särskilda riktlinjer för informationssäkerhet eller sekretess specifikt för distansarbete. Vi bedömer att befintliga riktlinjer inte ger medarbetarna nödvändiga instruktioner för att hantera information på ett säkert sätt vid distansarbete, bortsett från Riktlinje för hantering av uppgifter om personer med skyddad identitet som reglerar kommunikationsvägar oavsett arbetsplats. Vi saknar tydliga riktlinjer som är specifika för distansarbete och som enligt MSBs vägledning för kommunens informationssäkerhet är väsentliga, t.ex. en riktlinje för mobilt arbete respektive riktlinjer för behörighetsadministration som beaktar behörighetstilldelning vid distansarbete. Ytterligare riktlinjer kan vara aktuella efter en behovsanalys. Även om majoriteten av medarbetare upplever befintliga riktlinjer som tillräckliga så är det en betydande andel som inte gör det. Det kan bero på att olika arbetsroller hanterar olika mängd information och har därmed olika behov av riktlinjer. Behov av riktlinjer har också en tendens att uppstå först efter en allvarlig incident inträffat.
Finns tillräcklig kapacitet och säkra inloggningar för distansarbete?	Ja. Vi bedömer att det i allt väsentligt finns tillräcklig kapacitet och säkra inloggningar för distansarbete. Kommunen använder sig av VPN, vilket är en vedertagen teknisk lösning för att skapa en skyddad nätverksanslutning och höja informationssäkerheten. Majoriteten av medarbetare som svarat på enkäten uppger att de har tillräckliga tekniska förutsättningar och tillgång till nödvändig information för att utföra sitt arbeta på distans. Vissa uppgifter måste dock utföras plats och kan inte ersättas av något digitalt arbetssätt, t.ex. rättning av praktiska prov. Dock finns digitala underskriftstjänster som kan ta bort behovet av att åka in till sin arbetsplats för att underteckna dokument. Vidare förekommer, dock i liten omfattning enligt enkät, att medarbetare hanterar arbetsinformation på sin privata dator som inte är ansluten via VPN.
Har information/utbildning genomförts för personal som arbetar på distans? Tex angående sekretess, risk för bedrägeri mm.	Ja. Personal som arbetat hemifrån har fått grundläggande information om de mest överhängande riskerna som bör beaktas vid hemarbete. Vidare har det i april 2021 inletts en utbildningsinsats gällande allmän informationssäkerhet kopplat till digital säkerhet. En majoritet av berörda medarbetare har enligt enkät deltagit i utbildningen och 70 % upplever information och utbildning i stort som tillräcklig. En del medarbetare upplever information och utbildning som för generell och inte tillräckligt djupgående. Vi bedömer att det troligtvis hänger ihop med avsaknaden av specifika rutiner/riktlinjer för hemarbete som kan innehålla mer detaljerade riktlinjer beroende på verksamhet.
Finns fungerande rutiner för skyndsam hantering av eventuella incidenter?	Nej. Vi bedömer att det inte finns fungerande rutiner för skyndsam hantering av eventuella incidenter. Vi grundar bedömningen på att förteckningslista som ska specificera roller och till vem en incident/säkerhetshot ska anmälas till är inaktuell. Artikel 33 i dataskyddsförordningen ställer dessutom krav på att personuppgiftsincidenter ska anmälas till Datainspektionen

Revisionsfråga	Bedömning
	inom 72 timmar, såvida det inte är osannolikt att incidenteten medför en risk för fysiska personers rättigheter och friheter. Då det saknas en aktuell förteckningslista och särskild rutin för anmälan bedömer vi risken som stor att detta krav inte uppfylls vid en eventuell incident. För att kunna hantera eventuella säkerhetshot samt minimera skadan vid en incident är det viktigt att samtliga i organisationen vet hur och till vem detta ska anmälas
Sker en tillräcklig uppföljning och kontroll av säkerhet och sekretess vid hemarbete	Nej. Vi bedömer att det genomförs vissa kontroller av säkerhet och sekretess genom ordinarie rutiner. Det har däremot inte genomförts någon särskild uppföljning eller kontroll specifikt för hemarbete. Det blir dock svårt att göra någon särskild uppföljning eftersom det saknas särskilda riktlinjer för hemarbete att följa upp och kontrollera efterlevnaden emot.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen och nämnderna att:

- Genomför en behovsanalys och upprätta nödvändiga rutiner/riktlinjer för att säkerställa att medarbetare har nödvändiga instruktioner för att arbeta säkert hemifrån.
- Undersök vilka roller som är i behov av en mer djupgående utbildning och tillgodose detta behov.
- Upprätta tydliga dokumenterade riktlinjer för anmälan av säkerhetshot och personuppgiftsincidenter.
- Uppdatera förteckningslista med systemroller.

Skellefteå den 10 september 2021

David Larsson
Verksamhetsrevisor, EY

PerÅke Brunström
Certifierad kommunal yrkesrevisor, EY

Bilaga 1: Källförteckning

Intervjuade funktioner

- IT-chef
- Biträdande förvaltningschef kommunledningsförvaltningen

Dokument

- Policy för den kommunala verksamhetens IT-stöd (KF 2014-06-11)
- Riktlinjer för hantering av IT-utrustning och IT-system (KS 2013-01-29)
- Riktlinjer för hantering av uppgifter om personer med skyddad identitet (KS 2018-06-19)
- Riskanalys gällande hemarbete
- Information om hemarbete, publicerat på kommunen intranät
- Sekretess och säkerhetsskydd – information till krisledningsorganisationen
- Riskanalys och handlingsplan för hemarbete - IFO