§ 92 Dnr KS-2026-000002 007

Revisionsrapport, Granskning av cyberattack 2025

Kommunstyrelsens beslut

1. Kommunledningskontorets tjänsteskrivelse utgör kommunstyrelsens yttrade över rapporten.

2. Kommunledningskontoret får i uppdrag att återredovisa status på åtgärder utifrån revisionens rekommendationer under första kvartalet 2027.

Sammanfattning

De förtroendevalda revisorerna i Skellefteå kommun har granskat hur kommunen hanterade den cyberattack som drabbade systemleverantören Miljödata AB och således även Skellefteå kommun. Deras sammanfattande bedömning är att kommunstyrelsen delvis hanterade konsekvenserna av cyberattacken på ett ändamålsenligt sätt.

Utifrån granskning har det i rapporten konstateras att kommunstyrelsen inom flera områden visat på målmedvetenhet och handlingskraft i sitt incidenthanteringsarbete. Kommunen har en väl etablerad krisorganisation med tydliga rutiner och riktlinjer för incidenthantering och granskningen visar att kommunen i ett tidigt skede av attacken aktiverade ett arbete för att förstå attackens omfattning och konsekvenser. Däremot noterar revisionen att det finns förbättringsåtgärder som kommunstyrelsen behöver vidta gällande bland annat kravställning på leverantörer, uppföljning och åtgärdshantering av informationssäkerhetsincidenter med mera.

Utifrån genomförd granskning rekommenderar revisionen kommunstyrelsen att ta fram relevanta styrdokument, rutiner och riktlinjer, säkerställa robusta säkerhetskrav och uppföljning av leverantörsavtal, implementera befattningsanpassade utbildningsinsatser samt att säkerställa kontinuerlig insyn i incidenthantering. En stor del av dessa rekommendationer har under år 2025 redan identifierats av förvaltningen för support och lokaler samt kommunledningskontoret, ett arbete pågår med att genomföra förbättringar i syfte att anpassa verksamheten till kraven i Cybersäkerhetslagen (2025:1506) som trädde i kraft 2026-01-15.

Förvaltningen framför att den inte delar kommunen revisionens synpunkt på att anmälan inte var i tid till Integritetsskyddsmyndigheten (IMY).

Beslutsunderlag

Protokollsutdrag, kommunstyrelsens arbetsutskott 2026-02-19 § 50
Tjänsteskrivelse, kommunledningskontoret 2026-01-19
Skrivelse, revisionen december 2025
Rapport, granskning av cyberattack 2025

Beslutet sänds till

Kommunledningskontoret, säkerhet
Kommunledningskontoret, finans och juridik
Revisionen

Kommunledningskontoret
Handläggare
Patrik Moberg

TJÄNSTESKRIVELSE

2026-01-19

Diarienummer
KS-2026-000002

Kommunstyrelsen

Tjänsteskrivelse Revisionsrapport, Granskning av beredskap och hantering vid attack mot extern systemleverantör

Förslag till beslut

1. Kommunledningskontorets tjänsteskrivelse utgör kommunstyrelsens yttrade över rapporten.

2. Kommunledningskontoret får i uppdrag att återredovisa status på åtgärder utifrån revisionens rekommendationer under första kvartalet 2027.

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Skellefteå kommun har EY granskat kommunstyrelsen hur kommunen hanterade den cyberattack som drabbade systemleverantören Miljödata AB och således även Skellefteå kommun. Deras sammanfattande bedömning är att kommunstyrelsen delvis hanterade konsekvenserna av cyberattacken på ett ändamålsenligt sätt.

Utifrån granskning har det i rapporten konstateras att kommunstyrelsen inom flera områden visat på målmedvetenhet och handlingskraft i sitt incidenthanteringsarbete. Kommunen har en väl etablerad krisorganisation med tydliga rutiner och riktlinjer för incidenthantering och granskningen visar att kommunen i ett tidigt skede av attacken aktiverade ett arbete för att förstå attackens omfattning och konsekvenser. Däremot noterar revisionen att det finns förbättringsåtgärder som kommunstyrelsen behöver vidta gällande bland annat kravställning på leverantörer, uppföljning och åtgärdshantering av informationssäkerhetsincidenter etc.

Utifrån genomförd granskning rekommenderar revisionen kommunstyrelsen att ta fram relevanta styrdokument, rutiner och riktlinjer, säkerställa robusta säkerhetskrav och uppföljning av leverantörsavtal, implementera befattningsanpassade utbildningsinsatser samt att säkerställa kontinuerlig insyn i incidenthantering. Stor del av dessa rekommendationer har under år 2025 redan identifierats av avdelningen för IT- och verksamhetsutveckling samt Säkerhetsavdelningen och ett arbete pågår med att genomföra förbättringar i syfte att anpassa verksamheten till kraven i Cybersäkerhetslagen (2025:1506) som trädde i kraft 15 januari 2026.

Däremot delar kommunen inte revisionens synpunkt på att anmälan inte var i tid till Integritetsskyddsmyndigheten (IMY).

Beslutsunderlag

Tjänsteskrivelse, kommunledningskontoret

Beslutet sänds till:

Kommunstyrelsen

Kristina Sundin Jonsson
Kommundirektör

Patrik Moberg
Säkerhetschef

Beskrivning av ärendet

På uppdrag av de förtroendevalda revisorerna i Skellefteå kommun har EY granskat kommunstyrelsen hur kommunen hanterade den cyberattack som drabbade systemleverantören Miljödata AB. **Deras sammanfattande bedömning är att kommunstyrelsen delvis hanterade konsekvenserna av cyberattacken på ett ändamålsenligt sätt**. EY föreslår följande:

- **Ta fram relevanta styrdokument, rutiner och riktlinjer**

Kommunstyrelsen rekommenderas tillse att relevanta styrdokument fastställs för att stödja ett heltäckande informationssäkerhetsarbete. Detta inkluderar krav på hantering av personuppgifter och gallring, tydliga rutiner för både känsliga och mindre känsliga händelser samt kontinuerlig uppdatering av styrdokument.

- **Säkerställ robusta säkerhetskrav och uppföljning av leverantörsavtal**

Kommunstyrelsen rekommenderas att säkerställa att leverantörsavtal innehåller tydliga och ändamålsenliga säkerhetskrav, inklusive specifika tidsfrister för incidentrapportering samt säkerställa att rutiner för uppföljning och revidering av leverantörskrav görs regelbundet under avtalstiden.

- **Implementera befattningsanpassade utbildningsinsatser**

Kommunstyrelsen rekommenderas att stärka informationssäkerhetsutbildningen genom att införa befattningsanpassade insatser för medarbetare som hanterar känsliga uppgifter.

- **Säkerställ kontinuerlig insyn i incidenthantering**

Kommunstyrelsen rekommenderas att tillse att den har god kännedom om säkerhetsåtgärder genom att tydliggöra vilken information som ska rapporteras vid incidenthantering samt säkerställa att återrapportering sker för händelser med potentiellt betydande omfattning. Rekommendationen riktas delvis mot framtida hantering av incidenter med hänvisning till kommande cybersäkerhetslagen.

Vidare bedömer revisorerna följande:

- *Vid själva attacken agerade kommunen snabbt och isolerade systemen, men rapporteringen till Integritetsskyddsmyndigheten (IMY) skedde inte tillräckligt skyndsamt enligt gällande regelverk. Återgång till normalläge dokumenterades inte formellt och informationsflödet till politiken var begränsat.*

<u>Kommentar till ovanstående punkter:</u>

Gällande den rekommendera åtgärden **att *tillse att relevanta styrdokument fastställs för att stödja ett heltäckande informationssäkerhetsarbete*** så bedriver Skellefteå kommun ett aktivt arbete med att se över befintliga

styrdokument, rutiner och riktlinjer inom området. I arbetet omfattas ett antal områden så som informationssäkerhet, dataskydd och systemförvaltning. Arbetet inleddes under 2025 och pågår fortsatt, fokus i arbetet nu är att skapa en tydlig helhet utifrån de områden styrdokumenten ska omfatta.

När det gäller **att säkerställa robusta säkerhetskrav och en ändamålsenlig uppföljning av leverantörsavtal** har kommunens arbete med systematisk informationssäkerhetsklassning av informationssystemen skapat ett heltäckande underlag för att bedriva ett riskbaserat arbetssätt. Underlaget möjliggör en riskklassificering av befintliga leverantörsavtal som behöver kompletteras. Genom processen för IT-anskaffning finns ett övergripande styrande ramverk som gäller alla nya anskaffningar. Detta ramverk kan biläggas eller inkorporeras i äldre avtal utan att hela avtalet behöver omförhandlas.

Skellefteå kommun har sedan 2023 en etablerad modell för att organisera verksamhetsprocesser och tillhörande informationssystem i förvaltningsobjekt. Modellen säkerställer ett tydligt ansvar för att identifiera informationens skyddsvärde och fastställa relevanta säkerhetskrav på riskhantering och leverantörskontroll. Inom respektive förvaltningsobjekt bedrivs ett systematiskt och dokumenterat arbete genom objektplaner, vilket möjliggör kontinuerlig övervakning, uppföljning och kontroll av leverantörer. Detta kan genomföras genom säkerhetsrevisioner, granskningar och tester av efterlevnad.

Kommunen är i slutfasen av ett projekt med fokus på digitalt självförsvar för att öka medarbetarnas kompetens och medvetenhet om informationssäkerhet. Digitalt självförsvar ska bli en digital utbildning indelad i olika utbildningsblock, där det dels finns grundutbildning som alla medarbetare ska ta del av, samt delar med fördjupning inom olika områden beroende på vilken roll en medarbetare har. Till exempel finns en fördjupning för de som jobbar med sekretessreglerade eller känsliga uppgifter i det som kallas K3 (konfidentialitetsnivå 3). När detta under våren 2026 lanseras bedöms **revisionens rekommendation om att stärka informationssäkerhetsutbildningen genom att införa befattningsanpassade insatser för medarbetare** som hanterar känsliga uppgifter vara hanterat. Nya cybersäkerhetslagen ställer också krav på utbildning för ledningen vilket kommer att säkerställas, här är det troligt att kommunen kommer att luta sig mot och nyttja SKR:s kommande utbildning.

Vad avser punkten om att **säkerställa kontinuerlig insyn i incidenthanteringen** så kommer kommunens styrande dokument för civil beredskap (fredstida kriser och krig) att revideras under 2027. Det är dock värt att notera att merparten av händelser som medför att en eller flera verksamheter behöver samverka har, av t ex tjänsteperson i beredskap (TiB), inte bedömts vara av den magnitud att kommunstyrelsen behöver informeras. Följden av att TiB skulle behöva informera kommunstyrelsen varje gång kommunen går upp i förstärkningsläge skulle kunna medföra ett flertal ärenden per år då detta i regel sker vid t. ex mer omfattande väderhändelser och IT-störningar. Av kommunens krisledningsplan framgår att följande gäller: *”Kommundirektör, eller av kommundirektör annan utsedd, informerar krisledningsnämndens ordförande om att stabsläge är beslutat. Vid behov meddelar*

krisledningsnämndens ordförande övriga ledamöter och förbereder nämnden på att inställa sig för sammanträde". Vid en framtida revidering av krisledningsplanen skulle texten kunna ändras så att kommunstyrelsen också informeras om kommunstyrelsen så önskar.

Angående revisionens redovisning av den tidsfrist (inom 72 timmar) som gäller för anmälan av personuppgiftsincident kan följande sägas. Enligt dataskyddsförordningen ska den personuppgiftsansvarige (dvs nämnden) anmäla incidenten inom 72 timmar till Integritetsskyddsmyndigheten (IMY) från det att denne fått vetskap om incidenten. Gällande tolkningen av tidsfristen framgår bland annat följande av en vägledning för anmälan av personuppgiftsincident som utarbetats av Europeiska dataskyddsstyrelsen: *"I princip bör den personuppgiftsansvarige därför anses ha fått "vetskap" så snart personuppgiftsbiträdet (i detta fall Miljödata) har informerat om incidenten."* När den personuppgiftsansvarige informerats om incidenten behöver denne göra en bedömning av uppgifterna för att ta ställning till vilka åtgärder som behöver vidtas. Incidenten anmäldes ca 48 timmar efter att den personuppgiftsansvarige fått meddelandet om incidenten från Miljödata. Kommunen delar därmed inte revisionens synpunkt på att anmälan inte var i tid till IMY.

Revisionsrapport 2025
Genomförd på uppdrag av revisorerna
December 2025

Granskning av beredskap och hantering vid attack mot extern systemleverantör

Skellefteå kommun

The better the question. The better the answer.
The better the world works.

Shape the future
with confidence

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Skellefteå kommun har EY genomfört en granskning i syfte att bedömda hur kommunen hanterat den cyberattack som drabbade systemleverantören Miljödata AB och således även Skellefteå kommun i augusti 2025. Ingen data läckte från kommunen men systemen låg nere i en vecka medan attackens omfattning utreddes.

Vår **sammanfattande bedömning** är att kommunstyrelsen *delvis* hanterade konsekvenserna av cyberattacken på ett ändamålsenligt sätt.

Utifrån granskning konstateras att kommunstyrelsen inom flera områden visat på målmedvetenhet och handlingskraft i sitt incidenthanteringsarbete. Kommunen har en väl etablerad krisorganisation med tydliga rutiner och riktlinjer för incidenthantering och granskningen visar att kommunen i ett tidigt skede av attacken aktiverade ett arbete för att förstå attackens omfattning och konsekvenser. Däremot bedöms kommunstyrelsen inte ha ställt tillräckliga krav på leverantörer vad gäller rapportering av informationssäkerhets-incidenter.

Dessutom noteras brister i kommunens arbete med hantering av personuppgifter samt kommunstyrelsens kravställning kring återrapportering, uppföljning och åtgärdshantering av informationssäkerhetsincidenter. Kommunstyrelsen som ytterst ansvarig för riskhantering, styrning och regelefterlevnad bör hålla sig väl informerad om informationssäkerhetsincidenter samt tillse att kommunen har förutsättningar att ändamålsenligt hantera oönskade händelser. Kommande regelverk, i form av cybersäkerhetslagen, skärper kraven på styrelsens engagemang och uppföljning.

Baserat på genomförd granskning är bedömningen att det funnits brister kopplat till kommunens förebyggande arbete för att hantera IT-angrepp samt arbetet med uppföljning och utvärdering. Det pågår ett arbete inom kommunen i syfte att stärka informationssäkerhetsarbetet, arbetet har initierats innan cyberattacken i augusti 2025 och fler åtgärder har identifierats i samband med attacken. Arbetet är vid granskningstillfället inte färdigställt. Kommunstyrelsen rekommenderas därför att vidta åtgärder för att förbättra sin motståndskraft och minimera sin sårbarhet inför framtida cyberangrepp. En förbättrad motståndskraft mot cyberangrepp kan bidra till att avbrott i samhällsviktig verksamhet, förluster av känslig information eller andra betydande konsekvenser minskar.

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Ta fram relevanta styrdokument, rutiner och riktlinjer
- Säkerställa robusta säkerhetskrav och uppföljning av leverantörsavtal
- Implementera befattningsanpassade utbildningsinsatser
- Säkerställa kontinuerlig insyn i incidenthantering

Innehållsförteckning

Sammanfattning 1

Innehållsförteckning **2**

1. Bakgrund **3**

1.1 Syfte och revisionsfrågor *3*

1.2 Avgränsningar *3*

1.3 Revisionskriterier *4*

1.4 Metod och genomförande *4*

2. Granskning **6**

2.1 Revisionsfråga 1: Har kommunstyrelsen skapat tillräckliga förutsättningar för att hantera cyberattacker och dess konsekvenser? *6*

2.2 Revisionsfråga 2: Agerade kommunstyrelsen i enlighet med fastställda riktlinjer och rutiner i samband med den genomförda cyberattacken? *8*

2.3 Revisionsfråga 3: Har kommunstyrelsen följt upp och utvärderat konsekvenserna av cyberattacken i tillräcklig omfattning? *10*

3. Samlad bedömning och rekommendationer **12**

Bilaga 1: Förtydligande av rekommendationer 14

Bilaga 2: Intervjuade 15

Bilaga 3: Dokumentförteckning 16

Bilaga 4: Definitioner 19

1. Bakgrund

Skellefteå kommun och dess nämnder hanterar stora mängder digital information. Möjligheten att effektivt hantera sådan information i IT-system är idag en förutsättning för i stort sett all verksamhet som bedrivs inom offentlig sektor. Bristfällig säkerhet i informationshanteringen kan därför innebära risker för både anställda och invånare.

I samband med den omfattande cyberattacken som riktades mot systemleverantören Miljödata i augusti 2025 drabbades även Skellefteå kommun såsom kund till leverantören. Attacken innebar att tre av kommunens IT-system som hanterar personaladministrativa uppgifter blev otillgängliga. Dessa system används bland annat för att hantera rehabiliteringsärenden, arbetsskador och andra HR-relaterade processer. Systemen hanterar således känsliga persondata men anses inte vara väsentliga för att hantera den dagliga driften.

Kommunen agerade snabbt genom att gå upp i förstärkningsläge och vidta åtgärder för att isolera systemen och förhindra vidare spridning. En incidentrapport skickades till Integritetsskyddsmyndigheten (IMY) eftersom det fanns farhågor om att känsliga personuppgifter kunde ha läckt, men efter utredning meddelade kommunen att inga uppgifter från Skellefteå kommun hade exponerats i attacken.

Händelsen har aktualiserat vikten av robusta säkerhetsrutiner och kontinuitetsplaner inom kommunens verksamheter. Den har också gett upphov till en översyn av kommunens förmåga att hantera digitala störningar och stärka motståndskraften mot framtida cyberhot.

Kommunens revisorer har till följd av cyberattacken samt utifrån sin risk- och väsentlighetsanalys valt att genomföra en granskning avseende hur kommunen har hanterat attacken och dess konsekvenser.

1.1 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om kommunstyrelsen hanterade konsekvenserna av cyberattacken på ett ändamålsenligt sätt. Inom ramen för syftet ska granskningen besvara följande revisionsfrågor:

I granskningen besvaras följande revisionsfrågor:

- Har kommunstyrelsen skapat tillräckliga förutsättningar för att hantera cyberattacker och dess konsekvenser?
- Agerade kommunstyrelsen i enlighet med fastställda riktlinjer och rutiner i samband med den genomförda cyberattacken?
- Har kommunstyrelsen följt upp och utvärderat konsekvenserna av cyberattacken i tillräcklig omfattning?

1.2 Avgränsningar

Granskningen avgränsas till kommunens hantering av de konsekvenser som orsakades i samband med den cyberattack som drabbade systemleverantören Miljödata AB i augusti 2025. Vidare avgränsas granskningen till att enbart genomföra dokumentanalys och

intervjuer med Skellefteå kommun. EY har varken haft kontakt med leverantören eller granskat leverantörens agerande, processer och rutiner i samband med cyberattacken.

1.3 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:

- Lagen om extraordinära händelser (2006:544)
- MSBFS 2015:5 föreskrifter och allmänna råd om kommuners risk- och sårbarhetsanalyser
- MSBFS 2018:11 frivillig rapportering av incidenter i tjänster som är viktiga för samhällets funktionalitet
- Av kommunfullmäktige antagna styrdokument
- Tillämpliga delar i standard-serien ISO 27000

1.4 Metod och genomförande

Granskningen genomförs enligt god revisionssed inom informationssäkerhetsområdet. Bedömningar görs mot Myndigheten för samhällsskydd och beredskaps (MSBs) ramverk för LIS (Ledningssystem för informationssäkerhet), MSB:s specifika riktlinjer för kontinuitetshantering och standarden ISO 27000.

Granskningen inleds genom ett uppstartsmöte tillsammans med relevanta personer i kommunens verksamhet. Detta för att skapa en förståelse kring cyberattackens omfattning, påverkan och kommunens strategi för att hantera konsekvenser vid ett cyberangrepp. EY kommer därefter att utreda hur kommunen har bedrivit arbetet för att hantera dessa konsekvenser samt vad de framöver kan göra för att stärka sitt arbete och hantering av externa leverantörer för at motverka liknande störningar framöver. Granskning genomförs med stöd från styrande dokumentation och annat material som har tillkommit till följd av kommunens hantering av attacken. Därutöver kommer EY genomföra intervjuer med relevanta personer.

Utredningen resulterar i en sammanställd rapport som beskriver iakttagelser och bedömningar avseende kommunens förutsättningar för att hantera cyberattacken och dess konsekvenser, hur väl kommunen agerade i enlighet med fastställda riktlinjer och rutiner, samt hur kommunen har följt upp konsekvenserna av attacken. Avslutningsvis presenteras rekommendationer på vad kommunen kan göra framöver för att stärka sin motståndskraft mot framtida störningar. Innan den slutliga rapporten sammanställs genomförs en delrapportering med revisorerna i syfte att informera om utredningens framfart. Innan den slutliga rapporten presenteras för revisionen kommer även representanter från kommunen få möjlighet att faktagranska rapportens innehåll.

Vi använder följande bedömningsskala för bedömning utifrån revisionsfrågorna:

I allt väsentligt uppfylld	Grön
Delvis uppfylld	Gul
Ej uppfylld	Röd

2. Granskning

I följande kapitel analyseras det underlag som ligger till grund för EY:s granskning av Skellefteå kommuns hantering av cyberattacken som drabbade kommunens systemleverantör Miljödata i augusti 2025. Miljödata levererar tre system till Skellefteå kommun vilka används av chefer och HR för rehabiliteringsärenden, arbetsskador, tillbud och arbetsrättsliga ärenden. Skellefteå kommun hanterar således personuppgifter såväl som hälsodata, vilket klassificeras som känslig data enligt dataskyddsförordningen (GDPR), i systemen. Ingen data läckte från kommunen i samband med attacken men systemen låg nere i en vecka medan attackens omfattning utreddes. Granskningen presenteras i tre delar med utgångspunkt i rapportens tre frågeställningar som rör Skellefteå kommuns förutsättningar, agerande och uppföljning i samband med cyberattacken.

2.1 Revisionsfråga 1: Har kommunstyrelsen skapat tillräckliga förutsättningar för att hantera cyberattacker och dess konsekvenser?

Det försämrade säkerhetsläget i Europa och Sverige har ökat IT-angrepp mot offentliga verksamheter och deras leverantörer. Kommuner behöver därför arbeta förebyggande i enlighet med lagkrav och direktiv för att stärka motståndskraften mot cyberattacker. Detta genom att säkerställa robusta säkerhetsåtgärder och kontinuerlig riskhantering genom relevanta styrdokument samt operativa rutiner och riktlinjer. Det innefattar även ett proaktivt riskarbete och kravställning gentemot leverantörer.

2.1.1 Iakttagelser

Kommun har i sitt förebyggande risk- och krishanteringsarbete tagit fram ett antal styrande dokument och riktlinjer som syftar till att beskriva och kravställa kommunens agerande vid störningar i verksamheten. Vid tid för granskningen noteras att flertalet styrdokument för kommunens informationssäkerhetsarbete är under revidering. Kommunen har kommunövergripande och IT-specifika krisledningsplaner som tagits fram av säkerhetsavdelningen såväl som av IT-avdelningen. Det finns även centrala riktlinjer för krisberedskap med tydlig processbeskrivning för hantering av särskilda händelser, samhällsstörningar eller extraordinära händelser. Vidare arbetar kommunen regelbundet med risk- och sårbarhetsanalyser, som likt arbetet med krisledningsplaner genomförs både centralt på kommunövergripande nivå och specifikt för kommunens IT-verksamhet. Kommunen har en även tagit fram riktlinjer och metoder som specificerar hur sammahällsviktiga verksamheter, som identifierats i risk- och sårbarhetsanalysen, ska bedriva kontinuitetsarbete inom respektive område. Det finns mallar för kontinuitetsplaner med operativ vägledning för verksamheterna. I kommunens "Riktlinje för krisberedskap framgår krav på kontinuitetsarbetet, riktlinjen är antagen av Kommunfullmäktige.

Skellefteå kommun arbetar enligt förvaltningsmodellen PM3, där verksamheten och IT-komponenter delas in i förvaltningsobjekt med utsedda objektägare och objektledare. Dessa ansvarar för informationssäkerhet, teknisk drift och utveckling av objekten. Kommunen har en informationssäkerhetspolicy som kravställer identifiering, klassning och förteckning av processer och IT-system. I kommunens *Förvaltningsmodell för IT-stöd* ställs

krav på dokumentation, leverantörskrav och informationssäkerhetsklassning av system. All dokumentation uppges ske i kommunens systemstöd, Infokollen, som innehåller en samlad kravkatalog för kommunens IT-system.

Vid anskaffning av ny IT-leverantör ansvarar objektägaren och objektledaren för kravställning. Kraven baseras både på det framtagna IT-kravbiblioteket och informationssäkerhetsbiblioteket. Intervjuade nyckelpersoner uppger att anskaffade system dokumenteras och klassas i Infokollen, och klassningen ligger till grund för de krav som ställs på respektive informationssystem. Enligt *Förvaltningsmodell för IT-stöd* ska kravställning och avtal med IT-leverantörer följas upp, vid granskningstillfället noteras däremot att kommunen inte genomfört regelbunden uppföljning av de system som levereras av Miljödata före den inträffade attacken. Vidare noteras att central kravställning för hur ofta IT-leverantörsavtal ska följas upp saknas vid granskningstillfället. Kommunen har tecknat ett ramavtal samt ett personuppgiftsbiträdesavtal (PUB) med Visma, i vilket kommunen kravställer skyndsam rapportering till personuppgiftsansvarig vid misstänkt personuppgiftsincident. Miljödata är en underleverantör till Visma och omfattas därmed av det befintliga ramavtalet. Detta innebär att Miljödata är bunden av samma villkor och krav som huvudleverantören. Vid granskningstillfället saknar PUB-avtalet en tillräckligt tydlig definition av tidsfrister för när leverantören ska återrapportera incidenter till kommunen.

Det finns en beslutad utbildnings- och övningsplan för krisberedskap (*Skellefteå kommuns Utbildning-och övningsplan 2023 – 2026*) som främst riktar sig till politiska och operativa krisledningsfunktioner. Säkerhetschefen ansvarar för planering och genomförande av utbildningar och praktiska övningar, där IT-relaterade scenarier ingår. Enligt kommunens utbildningsplaner uppges samtliga medarbetare genomgå en grundläggande utbildning inom informationssäkerhet och dataskydd, där exempelvis utbildning inom dataskyddsförordningen (GDPR) ingår. Vid tid för granskningen görs inga riktade utbildningsinsatser, däremot uppges kommunen arbeta med att ta fram ett nytt utbildningspaket med befattningsbaserade utbildningar. Vidare uppger intervjuade nyckelpersoner att man i praktiken bedriver ett arbete med personuppgiftshantering i enlighet med dataskyddsförordningen (GDPR). Det finns detaljerade processbeskrivningar för rapportering av informationssäkerhetsincidenter, dokumentationskrav vid incidenthantering samt kravställning på rapportering till berörda myndigheter inom 72 timmar. Kommunen arbetar enligt principen om lagringsminimering. Vid granskningstillfället saknar Skellefteå kommun styrande dokument som kravställer hur kommunen ska hantera personuppgifter i enlighet med dataskyddsförordningen (GDPR). Detta innebär att det inte finns fastställda rutiner för centrala delar som dokumentation av behandlingar, gallringsrutiner och lagringsfrister.

2.1.2 Bedömning

Mot bakgrund av det förändrade omvärldsläget och genomförda cyberattacker inom både offentlig som privat sektor är bedömningen att kommunstyrelsen delvis har skapat tillräckliga förutsättningar för att hantera cyberattacker och dess konsekvenser. Vi noterar att kommunen bedriver ett övergripande riskarbete och har identifierat bristande IT-säkerhet hos leverantörer som en potentiell risk. Däremot bedöms förberedande åtgärder för att minimera denna risk ha varit otillräckliga vid tiden för attacken. Vi noterar vidare brister i kravställning för IT-leverantörshantering och avsaknad av systematisk uppföljning av leverantörsavtal under avtalstiden. Dessutom saknas tillräckligt tydligt definierade

tidsfrister för incidentrapportering i gällande IT-leverantörsavtal. Dessa brister ökar risken för bristande regelefterlevnad och försämrad säkerhetsnivå vid förändringar i hotbild eller lagstiftning.

Vidare bedöms att nuvarande styrdokument inte täcker alla områden som krävs för effektiv hantering av en cyberattack och dess konsekvenser. Vi konstaterar även att kommunen brister i arbetet med personuppgiftshantering, då det saknas tydlig kravställning för arbetet med personuppgiftshantering samt etablerade rutiner för gallring av personuppgifter. Detta innebär att kommunen saknar tillräckliga förutsättningar för att ändamålsenligt hantera och minimera mängden känsliga uppgifter som lagras i system som driftas av extern leverantör. Vid granskningstillfället pågår ett arbete med att upprätta och utveckla styrdokument inom informationssäkerhet, arbetet är initierat men inte ännu färdigställt.

Vidare konstateras att Skellefteå kommun erbjuder grundläggande utbildningar inom informationssäkerhet och dataskydd. Däremot saknas utbildningsinsatser anpassade för befattningar som hanterar stora mängder känslig information, för att säkerställa att medarbetarnas kompetens och riskmedvetenhet är i nivå med den information de hanterar. Detta ökar risken för felaktig hantering av personuppgifter och informationssäkerhetsincidenter. Kommunen uppger att ett arbete med att ta fram ett nytt utbildningspaket med befattningsbaserade utbildningar pågår. Sammantaget bedömer vi att identifierade brister ökar risken att känsliga data exponeras vid en fullbordad cyberattack.

2.2 Revisionsfråga 2: Agerade kommunstyrelsen i enlighet med fastställda riktlinjer och rutiner i samband med den genomförda cyberattacken?

För att effektivt hantera en pågående cyberattack krävs att korrekt information når berörda parter och att ansvar och mandat är tydliga och kända. Det är även av vikt att kommunen agerar skyndsamt för att minimera konsekvenserna av attacker.

2.2.1 Iakttagelser

Cyberattacken mot systemleverantören Miljödata inleddes den 20 augusti och upptäcktes av Miljödata den 23 augusti. Attacken drabbade tre system hos Skellefteå kommun: Stella, Adato och Novi. Miljödata uppger att ingen dataförlust eller läckage av personuppgifter skedde från kommunen, men berörda system stängdes ner och var obrukbara under en vecka medan attackens omfattning utreddes. Information om attacken nådde Skellefteå kommuns systemförvaltare för HR-systemen via mejl den 25 augusti kl. 08:18. Systemförvaltaren kontaktade omedelbart närmsta chef. Tjänsteperson i Beredskap (TiB) larmades och kallade till bedömningsmöte samma dag som kommunen informerades. Inledningsvis bedrevs ett arbete för att ta fram en lägesbild, förstå attackens omfattning samt besluta om initiala åtgärder. Kommunen gick in i förstärkningsläge, men krisorganisationen aktiverades inte, då attacken bedömdes ha måttlig påverkan. Kommunen stängde omedelbart integrationen och möjligheten att logga in till de drabbade systemen.

Den 26 augusti publicerade kommunen ett pressmeddelande om att känslig information gällande medarbetare och tidigare medarbetare kan ha läckt, vilket ledde till medial uppmärksamhet. Kommundirektören och personalnämndens ordförande fick löpande information, och förhandlingschefen rapporterade vid personalnämndens sammanträde. Informationsflödet till politiken var begränsat på grund av händelsens endast bedömdes ha måttlig påverkan. Skellefteå kommun rapporterade incidenten till Integritetsskyddsmyndigheten (IMY) den 27 augusti, två dygn efter att kommunen fått kännedom om attacken och fyra dygn efter att personuppgiftsbiträdet, Miljödata, upptäckte den.

Innan attackens omfattning var fastställd höll bedömningsgruppen löpande möten för lägesuppdateringar, som dokumenterades enligt etablerade mallar. Kommunen genomförde workshops för att ta fram omfallsscenarier och prioriterade åtgärder. Kontinuitet, förtroende och korrekt information identifierades som centrala mål, och kommunikation och krisstöd pekades i Omfallsplanen ut som potentiellt viktiga åtgärdsområden i samband med omfall. Bedömningsgruppen och IT-ansvariga skapade även chattgrupper för snabb informationsspridning. Systemen återtogs i drift den 1 september och den 5 september bekräftade Miljödata att inga personuppgifter hade läckt. Den 12 november beslutade IMY att inga ytterligare åtgärder skulle vidtas. Kommunen tog inget formellt beslut om återgång till normalläge, vilket noteras i kommunens interna uppföljning av incidenthanteringen. Kommunen uppger att beslut fattades i beredskapsgruppens interna chattgrupp, efter besked från Miljödata om att inga uppgifter läckt från kommunen.

2.2.2 Bedömning

Vi bedömer att kommunstyrelsen till viss del hanterade cyberattacken mot Miljödata i enlighet med etablerade riktlinjer och processer. Bedömningen grundar sig i att kommunen agerade utan dröjsmål och i enighet med framtagna rutiner och riktlinjer så snart de fick kännedom om attacken. Vid granskning noteras även att kommunen arbetat proaktivt med riskbedömning innan omfattningen av attacken hade klarlagts. Däremot bedöms att återställningsfasen saknade motsvarande struktur som den initiala hanteringen. Det saknas formellt beslut om återgång till normalläge.

Vi konstaterar att rapporteringen till Integritetsskyddsmyndigheten (IMY) inte har skett utan onödigt dröjsmål. Enligt dataskyddsförordningen (GDPR) ska personuppgiftsansvarig anmäla en personuppgiftsincident till tillsynsmyndigheten inom 72 timmar från det att denne blivit medveten om incidenten. I det aktuella fallet informerades kommunen av personuppgiftsbiträdet, Miljödata, först två dagar efter att incidenten upptäckts. Vår bedömning är därför att anmälan till IMY som skedde fyra dagar efter att personuppgiftsbiträdet identifierade incidenten inte rapporteras tillräckligt skyndsamt. Kommunen bör säkerställa att leverantörsavtal tydligt reglerar tidsramar för när personuppgiftsbiträdet ska underrätta personuppgiftsansvarig vid misstanke om personuppgiftsincident, så att kravet på anmälan inom 72 timmar kan uppfyllas. Personuppgiftsansvarig har rapporterat inom 72 timmar från att man blev informerad om attacken, däremot har incidenten inte rapporterats inom 72 timmar från dess att incidenten upptäcktes. Generellt är avsikten i dataskyddsförordningen (GDPR) att ansvar

inte kan skjutas över på biträde vid behandling eller incidenter relaterat till personuppgifter.

Det bedöms även kvarstå oklarhet om en tidigare notifiering från Miljödata hade påverkat utfallet då mottagaren, systemförvaltare för HR-systemen, inte ingår i beredskapsgruppen och således inte har beredskap. Varje nämnd i Skellefteå kommun är personuppgiftsansvarig för de uppgifter som hanteras inom nämndens verksamhet. Eftersom attacken berörde flera nämnder har kommunstyrelsen det övergripande ansvaret för rapporteringen.

2.3 Revisionsfråga 3: Har kommunstyrelsen följt upp och utvärderat konsekvenserna av cyberattacken i tillräcklig omfattning?

Att följa upp och utvärdera konsekvenserna av en cyberattack är avgörande för att stärka kommunens framtida beredskap. Genom att identifiera orsaker och sårbarheter som möjliggjorde attacken kan kommunen vidta riktade åtgärder för att förbättra säkerheten och minska risken för liknande incidenter. Utvärderingen ger underlag för att utveckla rutiner, tekniska skydd och kompetens som gör organisationen mer motståndskraftig.

2.3.1 Iakttagelser

Kommunen genomförde initialt löpande översiktliga utvärderingar för att bedöma attackens omfattning och konsekvenser. Kommunen har i sin utvärdering av cyberattacken främst granskat incidenthanteringens inledande faser. Enligt IT-avdelningens ”Process vid särskild IT-händelse ITVU 1.0” ska kommunikation och hantering utvärderas efter varje incident i lärande syfte, med fokus på IT-avdelnings agerande och efterlevnad av process, snarare än utvärdering av händelsen i sig. Objektägaren ska sedan genomföra ett efterarbete där händelsen utvärderas. Kommunen har färdigställt en utvärdering av incidenthanteringen där förbättringsområden som informationsflöde och tydlighet i återgångsprocessen identifierades. Intervjuade nyckelpersoner framhåller det interna samarbetet, informationsflödet och responstiden som styrkor. Utvärderingarna har dokumenterats enligt mallar och lagrats av TiB. Minnesanteckningar visar att kommunen tidigt bedömde att bristen på åtkomst inte innebar verksamhetskritiska konsekvenser, givet ett kortare avbrott. I dagsläget saknas däremot retrospektiv analys av potentiella konsekvenser som systemens otillgänglighet medförde.

Det efterarbete som objektägare för system levererade av Miljödata ansvarar för har påbörjats. Efterarbetet förväntas innefatta en mer omfattande utvärdering av attacken, dess konsekvenser samt åtgärder som ska vidtas för IT-systemen. Vi noterar att de berörda IT-objektens kravställning har uppdaterats i Infokollen efter attacken samt att en rutin för incidenthantering tagits fram specifikt för IT-system levererade av Miljödata. Vid granskningstillfället saknas estimerad tidsplan för när arbetet förväntas färdigställas och det saknas även kravspecifikation avseende vad efterarbetet ska innefatta.

Cyberattacken som drabbade Miljödata, och således Skellefteå kommun, klassades som en särskild händelse med medelhög påverkan på verksamheterna. Kommunens

krisledningsplan definierar tydligt krav på återrapportering och efterarbete för händelser som definieras som kris men motsvarande riktlinjer för hur kommunen och kommunstyrelsen ska hantera händelser av lägre prioritet är mindre tydliga. Intervjuade nyckelpersoner uppger att återrapportering till kommunstyrelsen skett i viss utsträckning, men att formell återrapportering främst görs vid händelser som klassas som verksamhetskritiska. EY har inte tagit del av styrelseprotokoll som bekräftar att återrapportering gjorts. Kommunikation mellan verksamhet och kommunstyrelsen innan, under och efter attacken har skett via informella kanaler.

2.3.2 Bedömning

Vi bedömer att kommunstyrelsen till viss del har följt upp och utvärderat konsekvenserna av cyberattacken i tillräcklig omfattning. Bedömningen grundar sig i att en utvärdering av kommunens agerande har genomförts där förbättringsåtgärder har identifierats i syfte att dra lärdom samt utveckla redan etablerade rutiner och arbetssätt. Dessa utvärderingar är centrala för att minimera risken att drabbas av liknande attacker i framtiden samt för att utveckla kontinuitetshanteringen. Vi bedömer att kommunen hittills främst har utvärderat sitt agerande utifrån attackens faktiska utfall. Däremot anser vi att en fullständig utvärdering även bör omfatta alternativa scenarier för att identifiera och implementera proaktiva åtgärder inför framtida incidenter med potentiellt större och mer allvarlig påverkan på verksamheten. Sådana scenarier kan exempelvis utreda hur kommunens agerande hade påverkats vid ett scenario där leverantörens rapportering fördröjts ytterligare på grund av otydliga tidskrav i avtalen. En sådan utvärdering stärker kommunens förmåga att vidta åtgärder för att bättre förbereda sig på framtida, mer omfattande attacker.

Kommunstyrelsen bedöms inte ha ställt tillräckligt tydliga krav på tidsplan för när det uppföljande efterarbetet för drabbade IT-systemen ska färdigställas samt vad det ska omfatta, vilket riskerar att fördröja en fullständig utvärdering och åtgärdsplan. Efterarbete är avgörande för att identifiera orsaker, ändamålsenligt hantera sårbarheter och förhindra upprepning av incidenter. Vidare noteras att kommunens krisledningsplan tydligt definierar tillvägagångsätt för att hantera situationer som klassificeras som kris men att riktlinjer för efterarbete vid händelser av lägre prioritet är otydliga. Detta kan leda till variation i hantering och uppföljning.

Med hänsyn till den kommande implementeringen av NIS-2 direktivet, i form av cybersäkerhetslagen, som mest sannolikt träder i kraft 15 januari 2026, kommer kraven gentemot styrelsens ansvar vid cybersäkerhetsincidenter att öka. Den nya cybersäkerhetslagen ställer högre krav på återrapportering och att en formell slutrapport med analys av orsak och vidtagna åtgärder vid betydande incidenter som påverkar verksamheten slutförs och rapporteras till styrelsen inom en månad. Även MSB:s kommande förslag på föreskrifter och allmänna råd om säkerhetsåtgärder och utbildning 8 § betonar ledningens ansvar att följa upp säkerhetsåtgärder, inklusive leverantörers cybersäkerhet. Med hänvisning till kommande regelverk och föreskrifter bedöms att kommunstyrelsen för närvarande inte säkerställer att den är tillräckligt informerad om cybersäkerhetsincidenter, samt att rapportering sker inom fastställda tidsramar.

3. Samlad bedömning och rekommendationer

Vår sammanfattande bedömning är att kommunstyrelsen *delvis* hanterade konsekvenserna av cyberattacken på systemleverantören Miljödata på ett ändamålsenligt sätt. EY har utifrån granskningsresultatet identifierat övergripande rekommendationer för att åtgärda brister och stärka det förebyggande arbetet, i syfte att minska risken för liknande incidenter framöver. Utifrån granskningsresultatet rekommenderar EY kommunstyrelsen att:

Tabell 1: Svar på revisionsfrågor

Revisionsfråga	Svar	
► Har kommunstyrelsen skapat tillräckliga förutsättningar för att hantera cyberattacker och dess konsekvenser?	Delvis tillfredställande Ett strukturerat risk- och incidenthanteringsarbete där IT-säkerhet i leverantörskedjan ingår har bedrivits. Däremot saknas tillräckligt skärpta och aktuella informationssäkerhetskrav i leverantörsavtalen, samt rutiner för uppföljning ändamålsenliga utbildningar och rutiner för gallring samt personuppgiftshantering.	
► Agerade kommunstyrelsen i enlighet med fastställda riktlinjer och rutiner i samband med den genomförda cyberattacken?	Delvis tillfredställande Agerandet har varit skyndsamt och i enlighet med etablerade riktlinjer och processer. Däremot bedöms att rapportering till IMY i samband med cyberattacken inte gjorts utan onödigt dröjsmål.	
► Har kommunstyrelsen följt upp och utvärderat konsekvenserna av cyberattacken i tillräcklig omfattning?	Delvis tillfredställande Utvärdering av cyberattacken har genomförts och efterarbetet har inletts. Hittills har utvärderingen i huvudsak baserats på det faktiska utfallet, med begränsad hänsyn till att alternativa scenarier som kan motivera ytterligare åtgärder. Attacken bedömdes som en incident med måttlig påverkan, vilket har medför otydlighet kring tidsramar och omfattning för det pågående efterarbetet som ska vidare utreda orsaker, konsekvenser och möjliga åtgärder. Kommunstyrelsen saknar etablerade och tydliga kravställningar för återrapportering och uppföljning anpassade till bedömd incidenttyp och risknivå.	

Utifrån granskningsresultatet rekommenderar vi kommunstyrelsen att:

- Ta fram relevanta styrdokument, rutiner och riktlinjer
- Säkerställa robusta säkerhetskrav och uppföljning av leverantörsavtal
- Implementera befattningsanpassade utbildningsinsatser
- Säkerställa kontinuerlig insyn i incidenthantering

Skellefteå december 2025

Ingrid Gunnarsson, projektmedarbetare

Tilda Mosséen, projektmedarbetare

Magnus Andersson, projektledare

Mårten Trollin, kvalitetssäkrare

Per Stålberg, certifierad kommunal yrkesrevisor, uppdragsledare

Bilaga 1: Förtydligande av rekommendationer

- **Ta fram relevanta styrdokument, rutiner och riktlinjer**

Kommunstyrelsen rekommenderas tillse att relevanta styrdokument fastställs för att stödja ett heltäckande informationssäkerhetsarbete. Detta inkluderar krav på hantering av personuppgifter och gallring, tydliga rutiner för både känsliga och mindre känsliga händelser samt kontinuerlig uppdatering av styrdokument.

- **Säkerställ robusta säkerhetskrav och uppföljning av leverantörsavtal**

Kommunstyrelsen rekommenderas att säkerställa att leverantörsavtal innehåller tydliga och ändamålsenliga säkerhetskrav, inklusive specifika tidsfrister för incidentrapportering samt säkerställa att rutiner för uppföljning och revidering av leverantörskrav görs regelbundet under avtalstiden.

- **Implementera befattningsanpassade utbildningsinsatser**

Kommunstyrelsen rekommenderas att stärka informationssäkerhetsutbildningen genom att införa befattningsanpassade insatser för medarbetare som hanterar känsliga uppgifter.

- **Säkerställ kontinuerlig insyn i incidenthantering**

Kommunstyrelsen rekommenderas att tillse att den har god kännedom om säkerhetsåtgärder genom att tydliggöra vilken information som ska rapporteras vid incidenthantering samt säkerställa att återrapportering sker för händelser med potentiellt betydande omfattning. Rekommendationen riktas delvis mot framtida hantering av incidenter med hänvisning till kommande cybersäkerhetslagen.

Bilaga 2: Intervjuade

- Redovisningschef
- Säkerhetschef
- Dataskyddsombud
- Chef verksamhetsnära IT
- IT-ansvarig

Bilaga 3: Dokumentförteckning

- Risk och sårbarhetsanalys ITVU (RSA) IT
- Krisledningsplan ITVU ver 1.0
- Bilaga_Prioriterade åtgärder beredskapsplan Ransomware.xlsx
- Process vid särskild IT-händelse ITVU 1.0
- Kontinuitetsplan vid IT-händelse
- Åtgärdshantering vid särskild IT-händelse
- Kontaktlista Åtgärdsteam
- Kontaktlista vid Särskild IT-Händelse
- Innehållsförteckning Krispärm
- Krisposter
- Mall Lägesbild Bedömningsmöte
- 202405 Bilaga 1 Omfattning och Pris version 1
- Avtal version 4.0
- Bilaga 2 - Leverans + Ub 1-4 version 4.0
- Bilaga 3 - Underhåll version 4.0_nytt
- Bilaga 5 - Tjänster + U 1-2 version 4.0
- Checklista inför återgång till normalläge
- Driftavtal Adato Miljödata – Adato
- Driftsavtal Lisa med Miljödata 180704
- Instruktioner för Informationssäkerhet - För dig som medarbetare - Insidan Skellefteå kommun
- Instruktioner informationssäkerhet - Insidan Skellefteå kommun
- KOM-Backup - Databas backup-policy-131125-131231
- Kravbibliotek IT.xlsx
- Rutin vid incident hos leverantör
- Skellefteå Kommun - Novi tilläggsavtal 20230320
- Skellefteå Kommun Personuppgiftsbiträdesavtal Bilaga B 20230314 Uppdatering
- Skellefteå kommun PuBavtal
- SKEN-2023-10-20 Spegling produktionsdata till testmiljö-131125-124539
- Status utbildning medarbetare Informationssäkerhet Lärande Skellefteå

- Tilläggsavtal Visma – Adato
- Tilläggsavtal Visma – Lisa
- Cyberattack
- 2025-05-20 Utbildning krisberedskap och stabsmetodik, steg 1 av 2
- 2025-05-22 Öva stabsmetodik på IT-relaterad händelse, steg 2 av 2
- 2025-09-12 Utvärdering cyberattack mot systemleverantör Miljödata
- Information insidan informationssäkerhetsincidenter
- Informationssäkerhetspolicy_fastställd av KF 190618 § 208
- MALL Första bedömningsmöte
- MALL Fortsatta bedömningsmöten
- Mötesbokning 2024-10-01 och 2024-10-02 utbildning
- Omfall Läckta uppgifter_Cyberattack_250826
- Plan för kriskommunikation
- Prioriterade åtgärder innan omfall Läckta uppgifter_Cyberangrepp_250826.xlsx
- Protokollsutdrag Kommunfullmäktige 2025-04-29 § 145
- PUI dok 1 Tjänsteskrivelse
- PUI dok 2 delegationsbeslut
- PUI dok 3 Anmälan Miljödata IMY 2025-08-27
- PUI dok 4 Mottagningsbekräftelse
- PUI dok 5 Information från Miljödata avseende personuppgiftsincident
- PUI dok 6 Slutrapport personuppgiftsincident
- PUI dok 7 Komplettering PUA ej exfil
- PUI dok 8 E-post Information gällande Miljödata incident
- PUI dok 9 Beslut om incident(885605)
- Riktlinjer för styrande dokument, fastställda kommunfullmäktige 2025-04-29 § 145
- Skellefteå kommuns Plan för hantering av extraordinära händelser (krisledningsplan) 2023 - 2026 reviderad
- Skellefteå kommuns Riktlinjer för krisberedskap 2023-2026 reviderad
- Skellefteå kommuns Risk- och sårbarhetsanalys 2023 - 2026 (reviderad)
- Skellefteå kommuns Utbildnings- och övningsplan 2023- 2026 reviderad
- Utbildning och övning 2023.png

- Utbildning och övning 2024.png
- Alla informationssäkerhetskrav.xlsx
- Anskaffning av IT-system – Process
- HR-objektet - Uppdrag och organisation
- Incidentnotis
- Objektplan HR-objektet 2025
- Skellefteå kommuns Förvaltningsmodell för IT-stöd
- Utbildning IT-säkerhet 2025
- Vidmakthållande aktiviteter IT
- Insidan hantering av personuppgiftsincident

Bilaga 4: Definitioner

Cyberattack: En cyberattack är ett samlingsnamn för olika typer av brott som utförs på IT-system. Attackerna kan utföras för att få tillgång till hemlig information, begränsa tillgången till IT-systemen, samt förstöra data eller IT-system.

IT-miljö: En IT-miljö avser all hårdvara, mjukvara, nätverk och data som utgör verksamhetens resurser för informationsteknik.

IT-infrastruktur: De grundläggande komponenter inom IT-miljön som behövs för att mer användarnära delar, som persondatorer, mobiltelefoner och applikationer, ska fungera. Infrastrukturen omfattar vanligtvis nätverk, servrar och säkerhetsutrustning. Enligt vissa definitioner ingår även databaser, vissa operativsystem och liknande. IT-infrastrukturen är en förutsättning för att en verksamhets IT-miljö ska fungera.

Kontinuitetsplan: Kontinuitetsplan är ett viktigt dokument i en organisations riskhanteringsstrategi. Kontinuitetsplaner upprättas i syfte att säkerställa att kritiska funktioner inom en organisation fortsatt bedrivs och upprätthålls på en tolerabel nivå, under och efter en störning.

Säkerhetskopia: En säkerhetskopia eller backup är en kopia av lagrad information som skapas för att förhindra att originaldata går förlorad. Säkerhetskopian kan användas för att återställa originalinformationen vid dataförlust i samband med exempelvis en cyberattack. Säkerhetskopior som lagras offline innebär att viktig data sparas på medier som inte är uppkopplade mot något nätverk, vilket skyddar dem från cyberattacker.