SVENLJUNGA KOMMUN

riktlinje

Riktlinjer för informationssäkerhet, cybersäkerhet och dataskydd

Beslutat av	Kommunfullmäktige
Beslutandedatum	2025-06-16 § 71
Ansvarig	Kommunchef
Revideras	Vid behov
Följas upp	Årligen

Innehållsförteckning

1. Inledning

Invånarna förväntar sig i allt högre grad att snabbt, enkelt och säkert kunna sköta sina ärenden, få tillgång till information och ha möjlighet till inflytande genom digitala kontaktvägar. Att information är korrekt som kommunen hanterar i relationer med kommuninvånare, företag och organisationer såväl som inom vår egen organisation utgör en grund för tillit och förtroende. Det är även viktigt att information i alla externa och interna relationer är tillgänglig när det behövs och att känslig information skyddas för att vi ska kunna fullgöra vårt uppdrag i samhället. Informationens säkerhet är därför en mycket viktig aspekt för alla verksamheter (informationsägare) inom kommunen.

Informationssäkerhets- och dataskyddsarbetet är en del i kommunens ledning- och kvalitetsarbete och omfattar alla informationstillgångar och personuppgifter utan undantag.

Riktlinjerna konkretiserar och operationaliserar Svenljunga kommuns policy för informationssäkerhet, cybersäkerhet och dataskydd. De anger krav, ansvar och tillvägagångssätt som ska tillämpas i den dagliga verksamheten för att säkerställa en korrekt hantering av information, system och personuppgifter.

Riktlinjerna riktar sig till samtliga organisatoriska enheter och funktioner och omfattar tekniska, administrativa och organisatoriska åtgärder. De utgör därmed ett styrande ramverk för hur säkerhetsarbetet ska genomföras i praktiken, i enlighet med gällande lagstiftning (t.ex. dataskyddsförordningen, säkerhetsskyddslagen och NIS2), interna regelverk och etablerade standarder som återfinns inom 27000-serien.

Tillämpning av riktlinjerna är föreskriven inom ramen för det systematiska informationssäkerhetsarbetet och följs upp genom intern kontroll, revision och efterlevs genom att följa ledningssystemet för informationssäkerhet, cybersäkerhet och dataskydd.

1.1 Syfte

Riktlinjerna betraktas som ett mer konkret stöd utifrån policyn för informationssäkerhet, cybersäkerhet och dataskydd. Den utgör sålunda grunden och beskrivningen för hur verksamheterna ska kunna uppnå en god säkerhet. Kommunfullmäktiges beslut av riktlinjerna medför konkreta tillämpningar av hur den utformas i granulärare guider, instruktioner, anvisningar och rutiner av informationssäkerhetssamordnare (CISO) eller informationsägare i respektive

förvaltning. Den hierarkiska strukturen för styr-och stöddokument är konstruerad enligt följande:

1. Unionsrättslig reglering och nationella lagstiftning
2. Policy för informationssäkerhet, cybersäkerhet och dataskydd
3. Riktlinjer för informationssäkerhet, cybersäkerhet och dataskydd
4. Ledningssystem för informationssäkerhet och dataskydd
5. Lokala guider, instruktioner, anvisningar och rutiner

2. Informationstillgångar

Med informationstillgångar avses all information och relaterade resurser/tillgångar som behövs för att hantera information. Exempel på resurser som används för att hantera information är IT-system, IT infrastruktur, pärmar och papper. Oavsett om informationen behandlas manuellt eller automatiserat och oberoende av dess form eller miljö den förekommer i ska informationstillgångarna ha rätt skydd. Perspektivet med informationssäkerhet och dataskydd är en naturlig del vid utformning av våra arbetssätt och en del av vårt dagliga arbete.

2.1 Informationssäkerhet

Informationssäkerhet definieras i enlighet med SIS-TR 50:2015 som bevarandet av informationens konfidentialitet, riktighet och tillgänglighet. Det innebär:

- Information finns endast tillgänglig för de som är behöriga (Konfidentialitet)
- Information skyddas mot oavsiktlig eller avsiktlig förvanskning (Riktighet)
- Information skall kunna nås och användas när den behövs (Tillgänglighet).

Arbetet med informationssäkerhet omfattar att införa och förvalta administrativa regelverk som policys och riktlinjer, tekniskt skydd med bland annat brandväggar och kryptering samt fysiskt skydd med till exempel skal- och brandskydd. Det handlar om att ta ett helhetsgrepp och skapa ett fungerande långsiktigt arbetssätt för att ge organisationens information det skydd den behöver.

Informationssäkerhet är teknikneutralt och omfattar skydd av såväl muntlig, pappersbunden som digital information. Utgångspunkten för kommunens informationssäkerhetsarbete är att följa den etablerade standarden inom området, SS-ISO/IEC 27000, cybersäkerhetslagen (i unionen känd som NIS-2 och CER-direktiven) Dataskyddsförordningen (GDPR) och övriga tillämpliga lagar inom

dataskydd. Detta stämmer väl överens med Myndigheten för samhällsskydd och beredskaps (MSB) rekommendation om hur informationssäkerhetsarbetet ska bedrivas inom offentlig förvaltning.

2.2 Cybersäkerhet

Cybersäkerhet avser skyddet av information, system, nätverk och digital infrastruktur mot hot och angrepp som uppstår genom eller via cyberspace. Arbetet omfattar tekniska och organisatoriska åtgärder för att förebygga, upptäcka, hantera och återhämta sig från incidenter såsom intrång, skadlig kod, dataintrång, överbelastningsattacker och andra former av cyberhot.

Cybersäkerhet är en del av det övergripande informationssäkerhetsarbetet men fokuserar särskilt på det digitala hotlandskapet och angripares metoder. Arbetet utgår från både nationella och internationella strategier och regelverk, såsom NIS2-direktivet (Cybersäkerhetslagen), Säkerhetsskyddslagen och MSB:s föreskrifter. Det är särskilt relevant för samhällsviktig verksamhet och digitala tjänster där kontinuitet, tillgänglighet och motståndskraft mot attacker är avgörande.

2.3 Dataskydd

Dataskydd handlar om att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Dataskyddsförordningen (The General Data Protection Regulation, GDPR) gäller i hela EU och har till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras. Vidare finns den nationella regleringen, SFS lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, även benämnd som dataskyddslagen. Dataskydd finns även reglerat i flera andra lagstiftningar som alltid ska beaktas i verksamheternas arbete.

2.4 LISD

Kommunens arbete med informationssäkerhet, cybersäkerhet och dataskydd bedrivs utifrån ett systematiskt och långsiktigt angreppssätt genom ett ledningssystem (LISD). Syftet är att möjliggöra en strukturerad styrning, uppföljning och förbättring av säkerhetsarbetet inom hela organisationen.

LISD bygger på principerna i standardserien SS-ISO/IEC 27000 och tillämpas utifrån kommunens behov och förutsättningar. Som stöd för utformning och implementering används Myndigheten för samhällsskydd och beredskaps (MSB) metodstöd för systematiskt informationssäkerhetsarbete.

2.5 Informationsklassning

Grunden för att kunna ge informationstillgångar rätt skydd är att inventera, värdera och klassificera informationstillgångarna.

Kommunens samtliga informationstillgångar ska finnas förtecknade i kommunens informationshanteringsplan (IHP), därmed utgör IHP en grund för värdering och klassificering av informationen utifrån informationssäkerhet och dataskydd.

För att underlätta informationshanteringen med externa aktörer utgår kommunens klassningsmodell från myndigheten MSB:s klassningsmatris med anpassning av definitioner av konsekvens- och skyddsnivåer utifrån kommunens förutsättningar. Varje informationstillgång värderas sedan inom varje säkerhetsaspekt tillgänglighet, riktighet och konfidentialitet.

Genom att klassa informationstillgångar utifrån de tre säkerhetsaspekterna identifieras vilken effekt otillräckligt skydd av informationstillgångarna får och utifrån det säkerställs att kraven på informationssäkerhet och dataskydd är på rätt nivå. En viss information kan exempelvis vara mycket kritisk när det gäller tillgänglighet och riktighet, men mindre känslig när det gäller konfidentialitet. Klassning syftar främst till att ge tillräckligt skydd för kritiska informationstillgångar, men också till att undvika överskydd med onödigt höga kostnader som följd.

Klassningsmodellens roll är att skapa en organisationsgemensam ram så att klassning sker på ett enhetligt sätt i hela organisationen och att samma skyddsnivå ges till likvärdiga informationstillgångar.

Själva informationen är den primära tillgången som klassas, resurser som används för att hantera informationen ska sedan utformas så att de möter de krav som klassningen av informationen medför enligt de skyddsåtgärder som klassningsmodell beskriver.

För att kunna bedöma att informationstillgångar har rätt skydd ska SKR:s (Sveriges kommuner och regioner) klassningsverktyg KLASSA användas för att göra självskattning och ta fram åtgärdsplan.

Tabell – säkerhetsaspekter och skyddsnivåer

Informationsklass	**Konfidentialitet**	**Riktighet**	**Tillgänglighet**
4. Av betydelse för Sveriges säkerhet	Säkerhetsskydds-klassificerad Säkerhetsskydds-klassificerade upp-gifter. Information som rör Sveriges säkerhet.		
3. – Allvarlig skada	Information med Stark sekretess -som innehåller uppgift som omfattas av -stark eller absolut sekretess eller uppgift som hänför sig till 18 kap OSL, eller en mycket stor mängd känsliga -personuppgifter som inte omfattas av stark eller absolut sekretess, där spridning kan medföra allvarliga konsekvenser för kommunen eller annan part.	Information som om den inte är riktig och fullständig medför allvarlig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funktion som om den inte är tillgänglig medför allvarlig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.
2. – Betydande skada	Sekretess Information som omfattas av svag sekretess enligt OSL eller känsliga	Information som om den inte är riktig och fullständig medför betydande konsekvens för kommunen eller	Information eller funktion som om den inte är tillgänglig medför betyd-ande konsekvens för

	personuppgifter enligt GDPR, där spridning kan medföra betyd-ande konsekvenser för kommunen eller annan part.	annan part, t.ex. externa aktörer eller medborgare.	kommunen eller annan part, t.ex. externa aktör-er eller medborgare.
1. – Måttlig skada	Intern Information som är avsedd att och utan konsekvenser kan spridas till medarbetare inom kommunen och till externa aktörer som behöver informationen.	Information som om den inte är riktig och fullständig medför måttlig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funktion- som om den inte är tillgänglig medför måttlig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.
0. – Ingen eller försumbar skada	Öppen Information som är avsedd att och utan konsekvenser kan spridas fritt inom och utom kommunen.	Information som om den inte är riktig och fullständig medför ingen eller lindrig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.	Information eller funktion som om den inte är tillgänglig medför ingen eller lindrig konsekvens för kommunen eller annan part, t.ex. externa aktörer eller medborgare.

3. Målsättning

För att kunna åstadkomma de strategiska målsättningarna i policyn för informationssäkerhet, cybersäkerhet och dataskydd har ett antal målsättningar inom olika områden identifierats.

Tabell – målsättning genom område och delmålsättning

Område	Delmålsättning
Organisation	Organisationen ska ha ett högt riskmedvetande och informationssäkerhetsarbetet ska vara organiserat så att det finns tydligt mandat och ansvar.
Riskhantering	Risker som kan påverka kommunens informationssäkerhet ska identifieras, analyseras och hanteras.
Styrning av informationstillgångar	Alla informationstillgångar ska vara kopplade till en informationsägare som har ansvar för att informationen och resurserna klassificeras och skyddas på rätt sätt.
Åtkomst till information	Användare ska ha tillgång till rätt information på rätt sätt för sin arbetsuppgift och vara medveten om sitt personliga ansvar.
Personal och säkerhet	Alla medarbetare som hanterar informationstillgångar ska ha kännedom om kommunens styrdokument och regelverk och tillräcklig kompetens för att kunna utföra sina arbetsuppgifter på ett säkert sätt.
Fysisk säkerhet	Kommunens information, samt övriga informationstillgångar, som exempelvis lokaler och den utrustning som används för informationshantering, ska skyddas på en tillräcklig nivå.
Drift och kommunikation	Drift och kommunikation av IT-miljö, system och tillhörande resurser ska ske utifrån fastställda rutiner för gemensam infrastruktur och de specifika säkerhetskrav som ställs av verksamheten.
Dataskydd	Organisationen ska ha ett systematiskt arbete gällande dataskydd för att uppnå ett högt personligt integritetsskydd för anställda och innevånare.
Hantering av incidenter	En process för rapportering när det gäller informationssäkerhets- och personuppgiftsincidenter ska finnas. Detta för att mildra effekter, förhindra upprepande och

	underlätta återgång till verksamhet på normal nivå om någon form av incident skett.
Kontinuitetsplanering	Det ska finnas en kontinuitetsplanering för att säkerställa den tillgång till information och funktioner som krävs för att upprätthålla verksamhet.
Uppföljning	Informationssäkerheten ska, som en del av den ordinarie verksamhetsredovisningen, regelbundet följas upp på central nivå och inom respektive nämnd, styrelse och bolag.

4. Principer och arbetssätt

Arbetet med informationssäkerhet, cybersäkerhet och dataskydd ska vara normerande, stödjande och kontrollerande. Arbetet ska bedrivas riskbaserat vilket innebär att hot, risker och sårbarheter identifieras och reduceras.

Principer för arbetet med informationssäkerhet och dataskydd:

- bygger på en helhetssyn som har informationen som utgångspunkt men även omfattar organisation, arbetssätt, processer, människor och teknik
- är systematiskt och bygger på den vedertagna standardserien ISO/IEC 27000 samt på rekommendationer från MSB
- aktiv samverkan med det förvaltningsarbete som finns i kommunen och där det är möjligt använda samma dokumentationsmodell
- integreras i arbetet med upphandling och avtalsuppföljning
- uttrycks i relevanta och uppdaterade styrdokument
- är förebyggande men ska även kunna hantera incidenter, allvarliga störningar och kriser när det gäller såväl säkerhets- som personuppgiftsincidenter
- förbättras och anpassas löpande i en föränderlig omvärld
- är väl kommunicerat i verksamheterna där medarbetare genom utbildning och information får en säkerhetsmedvetenhet med syfte att leva upp till denna policy och tillhörande styrdokument

5. Roller, ansvar och befogenheter

Ansvaret för kommunfullmäktige, kommunstyrelsen, nämnder med förvaltning och kommunala bolag fastslås i informationssäkerhet, cybersäkerhet och dataskyddpolicyn. För att kunna upprätta ett gott informations- och dataskydd krävs ytterligare utpekade roller, ansvar och befogenheter inom kommunen.

Kommunchef ansvarar på uppdrag av kommunstyrelsen för att informationssäkerhet, cybersäkerhet och dataskyddsarbetet bedrivs så effektivt som möjligt så att områdena uppnås enligt kommunstyrelsen och kommunfullmäktiges beslut.

Chef/VD ansvarar för informationssäkerhets- och dataskyddsarbetet inom sin verksamhet. Chef/VD ansvarar för att medarbetare inom den egna verksamheten har tillräcklig kunskap och förståelse för att erforderlig informationssäkerhet, cybersäkerhet och dataskydd i verksamheten ska uppnås.

Informationsägare formellt är tillika nämnderna. Det innebär att nämnden har det övergripande ansvaret för att bedöma informationens skyddsvärde och säkerställa att lämpliga skyddsåtgärder vidtas. Informationsägaren ansvarar även för att planera, genomföra och följa upp informationssäkerhetsarbetet inom sitt ansvarsområde. I praktiken kan dock ansvaret för operativa informationssäkerhetsåtgärder och riskhantering delegeras till tjänstepersoner, såsom förvaltningschef, verksamhetschef eller enhetschef. Den som innehar det faktiska ansvaret för en verksamhetsinformation är då också att betrakta som riskägare, med ansvar för att identifiera, värdera och hantera informationsrisker på en nivå som motsvarar verksamhetens behov och förutsättningar. Det är således viktigt att tydliggöra både det formella informationsägarskapet och det delegerade ansvaret för riskhantering, så att informationssäkerheten kan styras effektivt i hela organisationen.

Medarbetare är ansvariga för att följa kommunens styrdokument (policy, riktlinjer och guider) för informationssäkerhet och dataskydd. Medarbetare har också ansvar att uppmärksamma brister och incidenter rörande informationssäkerhet, cybersäkerhet och dataskydd och rapportera dessa till närmaste chef.

Dataskyddsombud (DSO) utses av varje nämnd och bolagsstyrelse. Dataskyddsombuden bevakar att personuppgiftsansvarig lever upp till dataskyddsförordningen och annan relevant lagstiftning. Detta görs genom rådgivning, utbildning och vägledning samt genom olika former av granskningar.

Informationssäkerhet och Dataskyddskontakt (IDSK) är den funktion som är kontaktperson gentemot dataskyddsombud och jobbar strategiskt och operativt med dataskydd i kommunen. Dataskyddskontakten sitter med i ISG.

Informationssäkerhetsgruppen (ICSG) samordnar och följer upp informationssäkerhet, cybersäkerhet och dataskyddsarbetet.

CISO/Informationssäkerhetssamordnaren har det samordnande och strategiska ansvaret för kommunens informations- och cybersäkerhet samt dataskydd. Rollen är rådgivande gentemot både verksamhet och ledning och verkar för att säkerställa ett systematiskt och långsiktigt informationssäkerhetsarbete i hela organisationen. Det operativa säkerhetsarbetet utförs i nära samverkan med informationsägare, systemförvaltare, verksamhetsutvecklare, IT och dataskyddsombud. CISO är även sammankallande till ICSG.

IT-chef ansvarar för kommunens interna tekniska IT-miljö och säkerställer att IT-miljön är tillförlitlig och motsvarar interna och externa krav gällande informationssäkerhet och dataskydd. Har ett övergripande ansvar för att säkerställa ett grundskydd för information hanterad i IT-verksamheten.

IT-säkerhetsansvarig ansvarar för att säkerheten i den interna IT-miljön, såsom tjänster, processer, system, infrastruktur, verktyg etcetera är tillräcklig och uppfyller verksamheters krav, legala krav samt policyn för informationssäkerhet och dataskydd med underliggande styrdokument. Verka för höjande av säkerhetsmedvetande inom IT. Ansvarar för att samordna och stödja informationsägare i val av relevanta säkerhetsåtgärder och deltar vid informationsklassningar och kravställande i upphandlingar. IT-säkerhetsansvarig sitter med i ISG.

Upphandlare stödjer med att i samband med upphandlingarna hänvisa verksamheter till de informationssäkerhetsprocesser som finns.

6. Informationssäkerhetsprocesser

För en effektiv och hållbar informationssäkerhetsverksamhet ska ett antal grundläggande processer för informationssäkerhet etableras och implementeras i kommunernas verksamheter. Processerna är utformade i enlighet med ISO-27000 serien och är anpassade till kommunens organisatoriska förutsättningar och specifika behov.

Processerna tar sikte på att skapa en robust och flexibel ram för informationssäkerhet, cybersäkerhet och dataskyddsarbetet som kan möta de krav

och utmaningar verksamheterna står inför. I det ljuset ska nedanstående processer med tillhörande anvisningar som specificeras i kommunens LISD skapas för och tillämpas av verksamheterna i den verksamhetsnära förvaltningen:

- Informationsklassningsprocess för identifiering och tilldelning av lämpliga skyddsbehov.
- Identifiera verksamheternas personuppgiftsbehandlingar.
- Riskhanteringsprocess för identifiering och hantering av informationssäkerhetsrelaterade risker.
- DPIA när verksamheterna hanterar känsliga personuppgifter.
- Incidenthanteringsprocess som reglerar hantering och uppföljning av informationssäkerhets/dataskydds relaterade incidenter. (se nedanstående avsnitt, incidentrapportering för mer utförlig information).
- Behörighetshanteringsprocess som reglerar arbetet med tilldelning, upprätthållande och avveckling av behörigheter till kommunens information.
- Personalsäkerhetsprocess för informationssäkerhetsrelaterade moment innan anställning, under eller vid förändrad anställning och vid anställningens upphörande.
- Process för anskaffning, utveckling och avveckling av tjänster/system avseende informationssäkerhetsrelaterade moment i arbetet med anskaffning, utveckling och avveckling av tjänster och system.
- Kontinuitetsplaneringsprocess som reglerar hur tillgång till kommunens information ska kravställa och optimeras utifrån verksamheternas behov.
- Säkerhetsmedvetandeprocess som anger hur medvetenheten om informationssäkerhet ska förmedlas och vidmakthållas.
- Uppföljningsprocess som anger hur uppföljning av informationssäkerhetsarbetet ska ske i verksamheten samt hur efterlevnaden ska säkerställas.
- Ledningsprocess som reglerar hur styrningen av informationssäkerhetsarbetet ska ledas och återkopplas till verksamheten.

7. Risk och sårbarhetsanalys

Risk-och sårbarhetsanalysen ingår i den process som föreligger vid nyanskaffning eller nyförvärv av nya system, eller större förändringar av digitala system eller tjänster. Analysen säkerställer att informationstillgångar skyddas på en ändamålsenlig nivå och att regelefterlevnaden i NIS-2, CER-direktiven, GDPR med flera efterlevs och att de tekniska och organisatoriska skyddsåtgärderna dimensioneras utifrån riskbild.

Analysen genomförs i enlighet med policyn och är ett obligatoriskt moment för informationsägaren.

7.1 Analysens beståndsdelar

- I analysen ska informationsresurserna och tillgångarna ha identifierats, det inbegriper vad som hanteras i systemet, exempelvis personuppgifter, känslig information och samhällskritiska funktioner.
- En beskrivning av hot-och sårbarheter, exempelvis intern/extern hotbild, teknisk miljö, beroenden till tredje part eller dylikt.
- Riskbedömning som består av sannolikhet och konsekvens och en bedömning av dessa.
- Beslut om skyddsåtgärder som inbegriper tekniska, organisatoriska eller juridiska sådana.
- Avvägning och dokumentation av eventuella kvarstående risker

7.2 Ansvar

Arbetet genomförs i samverkan mellan informationsägare, systemförvaltare, CISO, IT och verksamhetsrelevanta parter. CISO ansvarar för att kvalitetssäkra metod och analys för att ge vägledning om relevanta krav och åtgärder och betraktas som risksamordnare.

Resultatet ska dokumenteras.

8 Incidenthantering

En incident är en oönskad eller oplanerad händelse som påverkar eller riskerar påverka kommunens information, IT-miljö eller behandling av personuppgifter. Det skulle kunna vara:

- Felaktig eller obehörig åtkomst till information
- IT-avbrott eller cyberangrepp (exempelvis virus eller ransomware)
- Utskick av information till fel mottagare
- Borttappad bärbar dator eller USB
- Misstänkt dataintrång eller phishingförsök
- Läckta personuppgifter

Roll	**Ansvar**
Alla medarbetare	Ska omedelbart rapportera incidenter vid var tid gällande angiven kanal.
Närmaste chef	Ska stötta rapportering, eskalera och delta i utredningen vid behov.
CISO/informationssäkerhetsansvarig	Leder bedömning och hantering av incidenten. Dokumenterar och koordinerar åtgärder.
ICSG	Vid behov deltar vid utredningen.
Dataskydsdombud (DSO)	Blir kallad av CISO vid behov av bedömning av personuppgiftsincidenter och eventuell anmälan till Integritetsskyddsmyndigheten
IT-funktionen	Utreder vid behov tekniska orsaker, återställer system och implementerar skyddsåtgärder

8.1 Rapportering av incident

Utgångspunkten är att incidenter ska rapporteras så snart som möjligt.

Inrapporteringen sker vid var tid aktuell angiven kanal.

Telefon eller e-postmeddelande till IT eller CISO vid akuta incidenter.

Rapporteringen består av följande delar:

- Vad som hänt (så tydligt som möjligt)
- När det upptäcktes
- Vem som upptäckte det
- Vilken information/system/personuppgifter som påverkats

8.2 Vad händer efter en anmäld incident

1. Bedömning
    a) ICSG/CISO/IT-driftsledare tillsammans med beroende på art och karaktär på incidenten relevanta parter genomför en bedömning.
    b) Fastställer om det är en informations, cybersäkerhet eller personuppgiftsincident.
    c) Om incidenten omfattas av rapporteringsplikt till aktuell myndighet såsom IMY eller MSB.
    d) Om nämnd/ledning/verksamhet, enskild eller externa parter drabbas till den graden att de informeras. Sålunda en kommunikationsplan vid aktualitet.
2. Åtgärder
    a) Stoppa pågående skada (exempelvis stänga av konto, isolera system)
    b) Återställa till normal verksamhet
    c) Dokumentera händelser samt vidtagna åtgärder
3. Eventuell rapportering till myndigheter
    a) IMY (inom 72 timmar) vid personuppgiftsincident
    b) MSB (inom 24 timmar) vid allvarlig incident enligt Cybersäkerhetslagen
4. Uppföljning och förbättring
    a) Analys av grundorsak
    b) Uppdatering av rutiner
    c) Återkoppling till berörda parter (kan vara chef, verksamhet, enskild eller dylikt)

8.3 Ansvar

Chefer ansvarar för att säkerställa medarbetarens kunskap kring hur incidenter hanteras och är en stödjande funktion i en snabb hantering vid incidenter i samverkan med säkerhetsfunktionerna.

CISO/Informationssäkerhetssamordnare ansvarar för samordning av incidenthanteringen, följer upp det årligen med statisk och genomför kompetenshöjande insatser inom området.