Införande av Cybersäkerhetslagen och NIS2 i Nacka kommun

Nuläge, rekommendationer och handlingsplan

Leverans från uppstartsprojektet december 2025

Diarienummer: KSKF-2025-01265

NACKA KOMMUN

Innehåll

1. Inledning 2

1.1. Bakgrund och syfte 2

1.2. Sekretessbedömning 2

1.3. Ansvar och roller 2

2. Leverabel 1: Gap-analys 2

3. Leverabel 2 och 3: Rekommendationer och handlingsplan 5

3.1. Analys och hantering av anmälningsplikt 7

3.2. Organisatoriska säkerhetsåtgärder 7

3.3. Tekniska och driftrelaterade säkerhetsåtgärder 10

3.4. Fysiska säkerhetsåtgärder 14

3.5. Sektorsspecifika säkerhetsåtgärder: offentlig förvaltning 14

4. Leverabel 4: Plan för utvärdering 15

5. Bilagor 15

1. Inledning

1.1. Bakgrund och syfte

Syftet med detta dokument är att sammanställa de centrala leverablerna från uppstartsprojektet för implementeringen av Cybersäkerhetslagen (CybSäkL) och NIS2 i Nacka kommun. Dokumentet riktar sig till kommunens ledning och beslutsfattare och utgör ett beslutsunderlag inför fortsatt arbete. Ambitionen är att förmedla en överskådlig bild av nuläge, behov, åtgärdsförslag och förslag till hur arbetet bör organiseras.

Den 14 november 2025 tog styrgruppen fram ett projektdirektiv och startade därmed detta uppstartsprojekt.

Syftet med uppstartsprojektet är att utvärdera behovet av åtgärder och ta fram ett stöd till kommunens ledning utifrån hur cybersäkerhetslagen kommer påverka organisationen, vilket innefattar konkreta åtgärder och prioriteringar för att implementera lagstiftningen.

Detta dokument utgör leveransen från uppstartsprojektet i enlighet med projektdirektivet.

1.2. Sekretessbedömning

Projektgruppens bedömning är att dokumentet per den 16 december 2025 inte innehåller några uppgifter som omfattas av sekretess eftersom det är så övergripande att konkreta sårbarheter eller andra skyddsvärda bedömningar inte föreligger. Undantaget är den mer detaljerade gap-analysen, som inte läggs in i detta dokument utan ligger i avsett system.

1.3. Ansvar och roller

För uppstartsprojektet har följande ansvar och roller varit gällande:

- **Uppdragsgivare:** Stadsledningskontoret
- **Projektledare för projektgruppen:** Magnus Lindqvist
- **Deltagare i projektgruppen:** Emelie Rohdin, Emelie Sunnliden Ceder, Anni Ström
- **Styrgrupp:** Henrik Ahl, Henrik Palmblad-Wennergren, Louise Hult

2. Leverabel 1: Gap-analys

Nacka kommun bedriver idag ett riskbaserat systematiskt och fortlöpande arbete för att stärka säkerhetsmedvetandet i organisationen Utredningen ser ett behov av bland annat tydligare styrning och förbättrade rutiner för incidenthantering, uppföljning och dokumentation.

Trots begränsade resurser bedriver stadsledningskontoret ett arbete för att informera verksamheterna om kommunens höga krav på informations- och cybersäkerhet samt tillhandahåller stöd för hur verksamheterna ska säkerställa detta genom administrativa, tekniska och fysiska åtgärder, vilka enligt utredningen bör utvecklas och kompletteras. För att effektivt motverka cyberhot och incidenter, öka nivån på kommunens cyber- och informationssäkerhet samt optimera resursanvändning krävs en utökad koncernövergripande samordning av cybersäkerhets- och informationssäkerhetsarbetet baserat på noggranna riskbedömningar.

Fysiska utbildningsinsatser har genomförts och anpassats efter olika målgrupper, samt verksamhetsstöd för systematiskt informationssäkerhetsarbete i Stratsys har införskaffats för att säkerställa en tydligare dokumentation av informationssäkerhetsarbetet. Deltagandet i utbildningar har hittills varit otillräckligt och ännu inte omfattat samtliga medarbetare, vilket bidrar till skillnader i säkerhetsmedvetenhet och grundläggande förståelse för vikten av digital säkerhet inom organisationen. Säkerhetsstaben har, med regelbundenhet, arrangerat öppna hus för att erbjuda stöd till verksamheterna i deras informationssäkerhetsarbete, vilket fortsatt bedöms vara av stor betydelse under 2026. Arbetet fortgår dock men verksamheternas tillgång till resurser för att bland annat klassificera information skiljer sig åt, vilket gör det svårt att skapa en fullständig överblick av kommunens behov av säkerhetsåtgärder och sårbarheter eftersom informationsklassning är absolut grundläggande för ett systematiskt cyber- och informationssäkerhetsarbete.

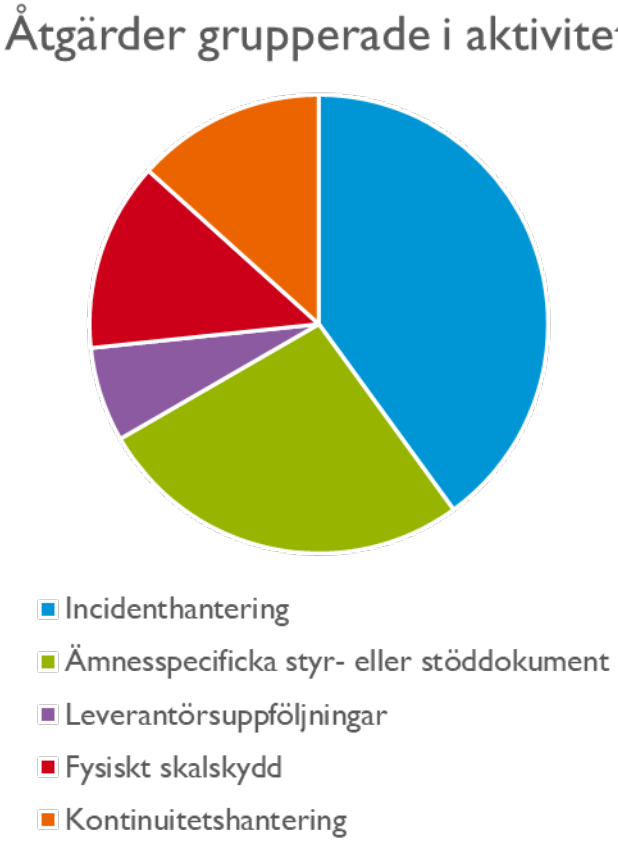
En gap-analys för kommunstyrelsen (inte övriga nämnder eller produktionen) baserad på kontrollpunkter i ISO 27002 är genomförd (bilaga 1). Gap-analysen indikerar positiva effekter av de genomförda tekniska säkerhetsåtgärderna inom ramarna för objektförvaltningen. Objektledare IT och objektledare verksamhet har det operativa ansvaret för inventering och prioritering av kritiska IT-system och komponenter, inklusive analys av systemsäkerhet, leverantörsdialog kring backup-rutiner samt systemsäkerhetsbedömningar. Utredningen påvisar även att vissa riskanalyser genomförts för både kritiska och övriga system, men att kvalitet och nivå på dessa analyser varierar.

Vad utredningen dock inte kunnat skapa sig en uppfattning om är hur det systematiska informationssäkerhetsarbetet i förhållande till ISO 27002 bedrivs i kommunens produktionsenheter då dessa till stor del bedriver sin IT-förvaltning inom ramen för sin verksamhet och inte ingår i objektförvaltningen. Den styrning och utveckling vars resultat som ovan nämnda Gap-analys ligger till grund för är alltså exklusive produktionens IT-förvaltning. Detta bör särskilt uppmärksammas då eventuella brister kommer påverka hela kommunens cybersäkerhet och vid en tillsyn som påvisar brister kommer Nacka kommun som juridisk person hållas ansvarig, inte enskilda verksamheter.

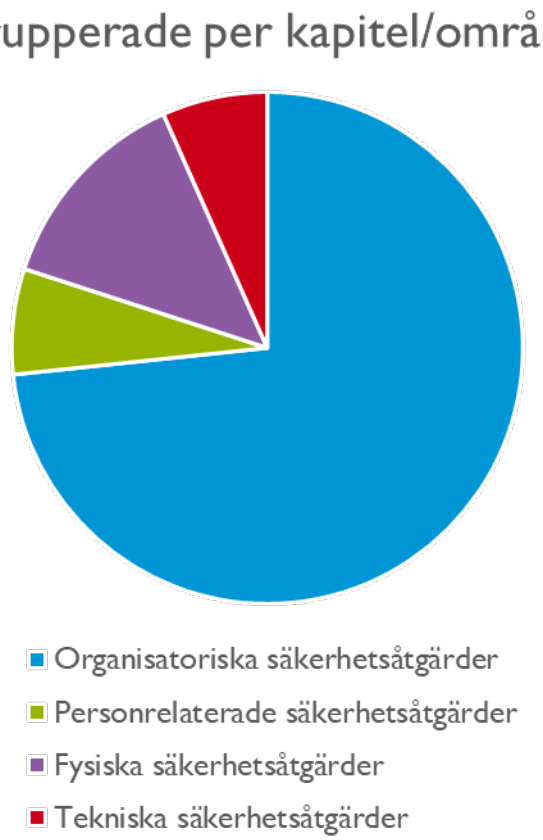
Under 2025 har kommunen genomfört mätningar och utvärderingar av det systematiska informations- och säkerhetsarbetet. Analys av data från Cybersäkerhetskollen samt gap-analysen enligt ISO 27002 har identifierat följande prioriteringsområden kopplade till cybersäkerhetslagen: brister i incident- och kontinuitetsplanering, tydligare styrning av det systematiska informationssäkerhetsarbetet genom interna regler, behov av

kompetenshöjande insatser samt förstärkt uppföljning och leverantörsuppföljning för att minska sårbarheter. Dessa områden överensstämmer med den nationella Cybersäkerhetsstrategin, där kommunernas ansvar för Sveriges cybersäkerhet och motståndskraft är centralt för att nå en förbättrad lägesbild nationellt.

Nedanstående två cirkeldiagram visar sammanfattande statistik över de åtgärder som identifierats i gap-analysen.



Av ovanstående cirkeldiagram kan utläsas att de flesta säkerhetsåtgärder som behövs införas för att kommunen ska uppnå önskat läge rör incidenthantering följt av en tydligare styrning genom interna regler för det systematiska informationssäkerhetsarbetet.



Av ovanstående cirkeldiagram kan utläsas att nästan tre fjärdedelar av de säkerhetsåtgärder som behövs för att kommunen ska uppnå önskat läge är relaterade till organisatoriska säkerhetsåtgärder. I många fall handlar detta om tydligare styrning och ledning genom beslutade mål, interna regler eller policys samt definierade roller och ansvar. Endast knappt vart tionde kontrollpunkt gäller tekniska säkerhetsåtgärder, så i den kategorin har kommunen redan kommit långt.

Det föreligger också ett fortsatt behov av att verksamheterna bedriver ett mer aktivt och strukturerat arbete med både säkerhetsåtgärder, övning och dokumentation inom ramen för kontinuitetsplaneringen.

3. Leverabel 2 och 3: Rekommendationer och handlingsplan

Mot bakgrund av kommunens aktuella situation bedömer uppstartsprojektets utredning att samtliga säkerhetsåtgärder enligt kategorierna i gap-analysen bör implementeras och regleras i kommunens styrdokument för att uppfylla gällande lagkrav. Flera styrdokument saknas fortfarande eller föreligger enbart som stöddokument, och omfattningen samt innehållet i dessa dokument behöver utvecklas för att möjliggöra en fullständig efterlevnad av cybersäkerhetslagen.

NIS2-direktivet ålägger ledningen ett särskilt strategiskt och personligt ansvar för uppföljning och övervakning av kommunens cybersäkerhetsarbete. Enligt SOU 2024:18 s. 374[1] jämställs ledningen med kommunstyrelsen, vilket är vägledande i utformningen av dessa rekommendationer.

Uppstartsprojektets utredning förordar att kommunledningens ansvar tydliggörs under införandefasen, samt att styrdokument med kommunövergripande strategi för incidenthantering, uppföljning och definiering av nyckelroller tas fram under första halvåret 2026. Vid implementeringen av NIS2 rekommenderas att Nacka kommun i stor utsträckning utgår från befintlig styrmodell med övergripande ledningsansvar, informationssäkerhetsstrategin samt digitaliseringsstrategin.

Uppstartsprojektets strategiska handlingsplan bygger på de huvudområden som anges i MSB:s förslag till föreskrifter om anmälningsplikt, förslag till föreskrifter om säkerhetsåtgärder och utbildning samt förslag till föreskrifter om incidenthantering och informationsplikt:

- Analys och hantering av anmälningsplikt
- Organisatoriska säkerhetsåtgärder
- Tekniska och driftrelaterade säkerhetsåtgärder
- Fysiska säkerhetsåtgärder
- Sektorsspecifika säkerhetsåtgärder: offentlig förvaltning

Eftersom det kan vara utmanande att hantera samtliga områden samtidigt, rekommenderas att prioritering sker baserat på resultatet av gap-analysen. Därefter planeras och utvärderas ytterligare säkerhetsåtgärder. Utredningen har tagit fram en övergripande strategisk handlingsplan, men detaljerade aktiviteter såsom utbildningsinsatser och framtida avtalskrav får hanteras under införandeprojektet. En specifik gap-analys mot cybersäkerhetslagen bör göras tidigt i införandeprojektet eftersom tidsbrist och att cybersäkerhetslagen inte beslutades förens den 10 december 2025 gjorde det omöjligt att genomföra den i uppstartsprojektet.

Den övergripande identifierade ambitionsnivån är att Nacka kommun når nivå 3[2] enligt Cybersäkerhetskollen inom fyra år, vilket ger tid för strukturerat arbete och utvärdering. Enligt underlag från MSB publicerat i samband med genomförande av Cybersäkerhetskollen 2025 är 3,3 nivån för att nå upp till minst föreskriftskraven (MSBFS 2020:6). Det ska också uppmärksammas att organisationen mäts på sitt långsiktiga systematiska cyber- och informationssäkerhetsarbete. Systematiskt arbete uppnås inte utan att både ha implementerat arbetssättet, arbetat med det och utvärderat arbetet minst en gång. Dessutom genomförs Cybersäkerhetskollen enbart vartannat år. Av dessa

[1] Se även prop. 2025/26:28 Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag, s. 99 som hänvisar till nämnda SOU

[2] Nivå 3 är strax under miniminivå kraven för att uppfylla föreskriften MSBFS 2020:6. Vi har inte de nya föreskrifterna ännu att jämföra med, men enligt MSB ska Cybersäkerhetskollen omarbetas mot nya föreskrifterna när de är beslutade och då kommer hygiennivån för dessa föreskriftskrav motsvara samma miniminivå enligt utsago från MSB.

anledningar anser utredningen att en rimlig genomsnittlig nivå på 3 är en tillräckligt god ambition att ha som mål för mätningen 2028/2029.

Implementering
Två initiativ föreslås: dels ett incidenthanteringsprojekt (20 jan–1 oktober 2026) som utvecklar en gemensam incidentprocess och rutiner samt säkerställer en förankring i organisationen, och dels ett införandeprojekt (20 jan–20 dec 2026) där kraven i cybersäkerhetslagen, förordning och föreskrifter analyseras och därav konstaterade behov av åtgärder genomförs. Nedan summeras åtgärdsområden enligt föreskrifter med förslag på insatser och tidsramar.

3.1. Analys och hantering av anmälningsplikt

NIS2-direktivet kräver att alla organisationer anmäler sig. Kommunen ska kontrollera om den omfattas av flera sektorer och ange detta i anmälan, vilket kan innebära tillsyn från flera myndigheter. MSB lanserar en anmälningstjänst i februari 2026.

Åtgärd: Utse ansvarig för att analysera berörda sektorer

Ansvarig: Införandeprojektet utser ansvarig person.

Deadline: 1 februari 2026 eller när det digitala formuläret öppnas.

3.2. Organisatoriska säkerhetsåtgärder

1. **Systematisk riskbaserat arbete**

Kommunerna ska arbeta systematiskt och allriskbaserat med cybersäkerhet enligt lag, förordning och relevanta föreskrifter.

Åtgärd: Genomför årlig informationssäkerhetsutvärdering på nämndnivå[3].

Ansvarig: Samordnaren rapporterar till KS, verksamheterna ansvarar för rapportering enligt direktiv från samordnaren.

Deadline: Starta nu, verksamheterna ska rapportera till KS senast november 2026.

[3] Det är svårt att uppnå de krav som ställs i 2 kap. 8 och 24 §§ förslag till föreskrift om säkerhetsåtgärder och utbildning om inte varje nämnd enskilt följer upp sitt arbete och kan rapportera på varje punkt uppåt så det sedan kan sammanställas till KS med fokus på de mest prioriterade säkerhetsåtgärderna och riskerna som har en kommungemensam bäring.

2. **Interna regler och arbetssätt, omvärldsbevakning, infoklassning, riskhantering**

Uppdatera och säkerställ tillräcklig styrning genom interna dokument gällande kommunens systematiska informations- och cybersäkerhetsarbete. Projektet ska förankra och informera organisationen om förändringar. Genomför en omvärldsanalys vid behov och uppdatera kommunens riskbild. Stöd kontinuerlig klassificering av information och riskhantering samt informationsbevarande och gallring.

Ansvarig: Informationssäkerhetssamordnare har ansvar för informationssäkerhetsstrategin inklusive ytterligare styrdokument, JKE för delegationsordningen och arkivet för stöd till verksamheterna med revidering av informationshanteringsplaner. Chefer och medarbetare är ansvariga för att ta emot information och be om stöd om man inte förstår informationen. Arbetet behöver inkludera kommunens arkiv för att säkerställa korrekt informationshantering enligt externa och interna krav.

Deadline: Juni 2026 för delegationsordningen samt löpande för övriga styrdokument.

3. **Ledningens ansvar för säkerhetsarbete** (utnämna roller, riskacceptans, mål och inriktning)

Kommunstyrelsen ansvarar för riktlinjer, roller, beslut som krävs enligt föreskrifter och säkerhetsuppföljning.

Åtgärd: Ta fram en årsprocess som säkerställer utbildning, och presentation av årsrapport till högsta ledningen. Årlig rapportering krävs enligt lag.

Ansvarig: Införandeprojektet

Deadline: Genomgång av styrdokument och delegationsordning senast första halvåret 2026.

4. **Ledningens utbildning om säkerhetsåtgärder**

Ledningen ska utbildas i enlighet med cybersäkerhetslagen, med en etablerad process för förtroendevalda i ledningen.

Åtgärd: Ta fram utbildningspaket för ledningen, on-boarding för nya ledare och utse ansvarig för att hålla utbildningarna. Säkerställ att utbildningarna anpassas till ledarens roll och ansvar, samt vilket skyddsbehov (klassning) informationen i verksamheten har.

Ansvarig: Införandeprojektet

Deadline: Oktober 2026

5. Personalsäkerhet

NIS2 och cybersäkerhetslagen kräver att ledning och medarbetare har tillräcklig kunskap om cyber- och informationssäkerhet för att organisationen ska uppnå en säker informationshantering.

Åtgärd: Säkerställ obligatorisk utbildning för ledning, styrelse och andra relevanta funktioner samt integrera detta i on-/offboardingprocessen för tjänstemän och politiker.

Ansvarig: Införandeprojektet

Deadline: December 2026

6. Incidenthantering

NIS2-direktivet och cybersäkerhetslagen kräver att den första inledande incidentrapporteringen sker inom 24 timmar och därefter med ytterligare rapportering efter 72 timmar och 30 dagar. Tydliga processer, rutiner, definierade roller med ansvar (t.ex. incidentansvarig och incidentmanager) och strukturerad dokumentation behövs för att säkerställa efterlevnad. Rutiner för rapportering till CERT-SE samt eventuellt andra myndigheter där det finns externa regelkrav på detta ska vara tydliga och förankrade.

Säkerhetsstaben har tillsammans med kundserviceenheten påbörjat ett arbete med en kommungemensam incidentprocess. Projektet föreslår att ett separat projekt startas som kan bistå och ta detta arbete vidare för att säkerställa förankring och etablering i samtliga kommunens verksamheter.

Ansvarig: Incidentprojektet

Deadline: 16 juni 2026 som milstolpe för första leveransen och återrapportering av läget i december 2026

7. Kontinuitetshantering och krishantering

Kontinuitetsplanering och krishantering ska säkerställa att kommunens samhällsviktiga tjänster upprätthålls vid störningar eller cyberincidenter enligt cybersäkerhetslagen.

Åtgärd: Genomför en inventering av befintliga kontinuitetsplaner och uppmana till att upprätta nya där sådana saknas under det första kvartalet 2026. Genomför analys om det

finns anledning att revidera krishanteringsplan och riktlinjer för kommunens TIB[4]-funktion med anledning av krav i föreskriften om säkerhetsåtgärder och utbildning samt förskriften för incidenthantering och informationsplikt.

Ansvarig: Kommunstyrelse/kommundirektör[5]: Övergripande ansvar för planer och resurser; beslutar om prioriteringar.

Säkerhetsdirektör/Säkerhetschef och Digitaliseringsdirektör och IT driftschef: Utarbeta, driva och testa planer; verksamhetschefer anger kritiska beroenden

Deadline: Juni 2026

8. **Uppföljning och utvärdering**

Kommuner måste systematiskt följa upp och utvärdera cybersäkerhetsarbetet enligt cybersäkerhetslagen för att säkerställa att säkerhetsåtgärderna är proportionerliga, lämpliga och effektiva.

Åtgärd: Genomföra årliga revisioner, mätningar (t.ex. Cybersäkerhetskollen), tester av säkerhetsåtgärder och incidenthantering; rapportera status, brister och framsteg till ledningen. Varje verksamhetschef ska årligen följa upp det systematiska informations- och cybersäkerhetsarbetet inom sin verksamhet.

Utvärdera efterlevnad av policy, riskanalyser och åtgärdsplaner med KPI:er, och justera baserat på resultat från övningar och analyser av inträffade incidenter.

Ansvar: Kommunstyrelse/kommundirektör[6]: Övergripande uppföljning och beslut om förbättringsåtgärder.

Informationssäkerhetssamordnare/IT-säkerhetssamordnare: Driva operativa utvärderingar, samla data och föreslå korrigeringar; verksamhetschefer bidrar med lokal input.

Deadline: December 2026 första rapporten, därefter löpande på årlig basis.

3.3. Tekniska och driftrelaterade säkerhetsåtgärder

1. **Förvärv, utveckling och underhåll av system**

[4] Tjänsteman I Beredskap
[5] Med anledning av kraven på bl.a. extern samverkan i 2 kap, 21 § förslag på föreskrifter om säkerhetsåtgärder och utbildning så antar utredningen att ett beslut om dessa interna regler vill nog stadsdirektör och kanske även KS ha varit delaktiga i. När vi når ett sådant läge så kommer varje moment vi gör och inte gör granskas och troligen även få medial uppmärksamhet.
[6] 2 kap. 8 § förslag på föreskrifter om säkerhetsåtgärder och utbildning, och i synnerhet punkt 8

NIS2 och cybersäkerhetslagen ska stärka verksamhetens skydd mot cyberhot och minska risken för incidenter. Brister i leveranskedjor är idag ett av de största cyberhoten. Som mottagande organisation i de digitala leveranskedjorna måste Nacka kommun samarbeta med leverantörer för att upprätthålla hög säkerhet och ett effektivt skydd för sina nätverk och informationssystem.

Åtgärd: Utredningen rekommenderar att inköps- och digitaliseringsenheten samarbetar för att ta fram krav på säkerhetsåtgärder i framtida upphandlingar. Dessa krav ska även gälla befintliga avtal och kan kräva extra resurser och planering. Därutöver bör utvärderas om controllerenheten också bör medverka i de delar som berör leverantörsuppföljningar under pågående avtalsperiod.

Ansvarig: Införandeprojektet informerar om behovet.

Inköps-/upphandlingsansvarig och enhetschef på digitaliseringsenheten: Säkerställa krav i avtal och leverantörskedjor. Dialog bör även föras med enhetschef på controllerenheten.

IT- och informationssäkerhetssamordnare: Införa tekniska säkerhetsåtgärder i utveckling och underhåll efter beslut från objektägare; ledningen godkänner strategiska beslut.

Deadline: Juni 2026

2. **Driftrelaterad dokumentation**

Driftrelaterad information ska följa kraven i föreskriften samt vara aktuell och beskriva befintlig arkitektur, informationsflöden, nät, systemkomponenter, beroenden, driftprocesser, rutiner vid störningar och incidenter, samt ansvarsfördelning.

Ansvar: enhetschef på digitaliseringsenheten/driftansvarig tillsammans med IT-säkerhetssamordnare ansvarar för att inventera och se till att dokumentationen har upprättats. Beslut om nivå och omfattning fattas av ledningen. Objektledare IT upprättar dokumentationen och kontaktuppgifter till leverantörer.

Deadline: Ge första rapport i juni 2026, därefter uppdateras löpande, minst årligen eller vid större förändringar.

3. **Segmentering och filtrering**

Åtgärder: Undersöka behovet av att dela upp nät i zoner (t.ex. drift, klient, gäst, OT/industri), införa brandväggar och filtrering mellan zoner, begränsa trafik till minsta nödvändiga, samt särskilt skydda system för samhällsviktiga tjänster.

Ansvar: enhetschef på digitaliseringsenheten/IT-säkerhetssamordnaren; verksamhetsansvariga anger vilka system och informationsklasser som kräver högre skyddsnivå.

Deadline: Riskbaserat införande så snart som möjligt; segmentering av kritiska system ska utvärderas och planeras in senast december 2026.

4. Behörighetshantering och autentisering

Behörighetsstyrning och autentisering avser rutiner som beskriver tydliga roller och behörigheter, principen minsta behörighet, regelbunden behörighetsgranskning, stark autentisering (t.ex. multifaktor) till känsliga system, loggning av misslyckade inloggningsförsök och central identitetshantering

Åtgärd: Inventera nuläget och ta fram en rapport med ska- och bör-krav på säkerhetsåtgärder, tidplan samt kostnadskalkyl. Revidera interna regler och uppdatera dessa vid behov.

Ansvar: enhetschef på digitaliseringsenheten i samverkan med HR och verksamhetschefer; ledningen/ objektägare beslutar om krav på behörighetsstyrning och stark autentisering. Verksamhetschef ansvarar för att säkerställa att informationsklassning är genomförd och att medarbetare endast har behörighet till information som krävs för utförande av aktuell arbetsuppgift/roll.

Deadline: Sammanställ en rapport och redovisa för ledningen förslag om åtgärder senast december 2026.

5. Säkerhetsloggning och logganalys; robust och spårbar tid

Kommunen behöver både logga säkerhetshändelser och ha gemensam, spårbar tid i alla viktiga system.

Åtgärder: Aktivera loggning i kritiska system, nät- och säkerhetskomponenter, skydda loggar mot manipulation, fastställa vad som loggas och hur länge, och införa rutin eller verktyg för analys av säkerhetsloggar. Interna regler för regelbunden loggranskning måste upprättas gällande behörighet till loggarna samt skydd och bevarande av loggarna.

Ansvar: enhetschef på digitaliseringsenheten/IT-säkerhetsanssamordnare ansvarar för teknisk loggning, loggskydd, logg granskning och tidsinfrastruktur. IT-säkerhetssamordnare sätter krav på vad som ska loggas, hur länge och vilka system som måste ha spårbar och synkroniserad tid för incidentutredning.

Deadline: Redovisa åtgärder, planerade åtgärder och behov av ytterligare säkerhetsåtgärder december 2026

6. Skydd mot skadlig kod och kryptering

Kommunen behöver både grundläggande skydd mot skadlig kod och riskbaserad kryptering av känslig information.

Åtgärd: Genomför riskanalys utifrån informationsklassningen för relevant information därefter implementeras kryptering om behov finns utifrån genomförd riskanalys. Utöver detta ska rutiner för säker nyckelhantering upprättas och krypteringen i kritiska system ska dokumenteras.

Vid behov förstärks skyddet mot skadlig kod samt skapas eller revideras rutiner för att hålla systemen och rutinerna vid misstänkta infektioner uppdaterade.

Ansvar: enhetschef på digitaliseringsenheten/IT-säkerhetssamordnare: tekniskt skydd mot skadlig kod, klient- och serverskydd, epost/webbfilter, krypteringslösningar i infrastruktur och system.

Informationssäkerhetssamordnare: policy och krav för när kryptering ska användas (i vila/vid överföring) utifrån informationsklassning, samt uppföljning av efterlevnad.

Deadline: ska vara på plats senast december 2026 och därefter utvärderas löpande.

7. Säkerhetskonfigurering, säkerhetstester, säkerhetskopiering, övervakning av system samt ändringshantering

Kommunen behöver ha grundläggande styrning avseende hur system sätts upp, ändras, testas, övervakas och säkerhetskopieras för att identifiera brister i cybersäkerheten och minska risken för cyberhot. Interna regler för bland annat säkerhetskopiering och ändringshantering behöver upprättas.

Åtgärd: Inventera säkerhetsinställningar, införa standardkonfigurationer och patchrutiner samt genomföra återkommande tester på kritiska system. Säkerställ backup med testad återläsning, granska larm och driftövervakning, och förbättra ändringshantering med dokumentation och riskanalys. Mjukvara som leverantören inte längre tillhandahåller säkerhetsuppdateringar för ska omedelbart bytas ut eller uppgraderas.

Ansvar: enhetschef på digitaliseringsenheten/IT-drift: Praktisk säkerhetskonfigurering, patchning, säkerhetskopiering, övervakning och genomförande av tester.

IT-säkerhetssamordnare och systemägare: Ställa krav (vilka system, vilken nivå) samt godkänna större ändringar efter riskbedömning.

Deadline: Löpande arbete, lägesrapportering december 2026

3.4. Fysiska säkerhetsåtgärder

1. **Lokaler, system och tekniska försörjningssystem**

Lokaler, system och tekniska försörjningssystem behöver skyddas fysiskt, miljömässigt och driftsmässigt baserat på informationsklassning och riskanalys för att skydda lokaler där informationsbehandling genomförs och för att upprätthålla kommunens samhällsviktiga tjänster.

Åtgärd: Med informationsklassningen som grund genomförs en riskanalys om Nacka kommuns relevanta fysiska utrymmen är i behov av åtgärder. Arbeta aktivt med rutiner som avser clean desk, låsa skåp, särskild sektion för externa besökare, lokalers utformning med mera. Genomför en behovsanalys med allriskperspektiv och genomför nödvändiga säkerhetsåtgärder utifrån identifierade risker.

Ansvarig: Införandeprojektet

Deadline: December 2026.

3.5. Sektorsspecifika säkerhetsåtgärder: offentlig förvaltning

1. **RAKEL och SGSI**

Åtgärd: identifiera om användningen av RAKEL (Radio Kommunikation för Effektiv Ledning) behöver utökas i kommunen med hänvisning till nya krav i cybersäkerhetslagen och i samband med en ny utformning av en incidenthanteringsprocess.

Utred om SGSI (Swedish Government Secure Intranet) behöver användas alternativt kan vara en kostnadseffektiv lösning för att möta delar av kraven som följer av cybersäkerhetslagen samt dess förordning och föreskrifter. Lämna över utredningen till högsta ledningen.

Kontrollera en gång per kvartal funktionen för intern och extern kriskommunikation hos systemen.

Ansvarig: Införandeprojektet

Deadline: Q2 2026 för resultatet av identifieringen huruvida det föreligger ett behov av utökad användning av RAKEL. Q4 2026 för rapport av utredning om Nacka kommuns behov av SGSI.

4. Leverabel 4: Plan för utvärdering

Nacka kommuns införandeprojekt för cybersäkerhetslagen bör utvärdera vidtagna åtgärder vid tre fasta milstolpar: efter sex månader (ca juli 2026), efter ett år (jan 2027) samt slutligen i samband med den första årliga rapporteringen till kommunstyrelsen som rekommenderas ske i april 2027. Därefter sker årlig rapportering enligt kraven i cybersäkerhetslagen med rekommenderad tidpunkt i april varje år. Rekommendationen grundar sig på att resultat från Cybersäkerhetskollen som genomförs vartannat år kan börja sammanställas efter februari 2026. Samt relevanta beredskapsmyndigheters årsrapporter brukar publiceras i början av varje år i vilka relevant information för prioriteringar av säkerhetsåtgärder kan framgå.

När:

Q2 2026 (efter 6 mån): Grundläggande efterlevnad (t.ex. anmälan, riskanalys, prioriterade åtgärder).

Jan 2027 (efter 1 år): Utvärdering av implementeringen av alla projektet prioriterade säkerhetsåtgärder, inklusive tester och planer.

Årlig (april): Årsrapportering till kommunstyrelsen enligt krav i cybersäkerhetslagen, förordning och föreskrifter.

Hur:

Använd gap-analys i Stratsys, NIC Platform (Nordic Information Control) för analys av olika datakällor, Cybersäkerhetskollen MSB:s Mognadsdialogen och interna checklistor för självutvärdering av riskhantering, incidentrutiner och ledningsstöd.

Genomför revisioner med KPI:er (t.ex. % system med MFA, loggningstäckning, % av informationen som är klassad), övningar och externa granskningar; rapportera till kommunstyrelsen med åtgärdsplan

5. Bilagor

Nr	Namn	Länk
1	Gap-analys för KS (exkl. Produktionsenheter)	Finns i Stratsys. Sekretess.