



Handlingsplan informationssäkerhet 2026

Utgår från Östhammars kommuns program för informationssäkerhet KF 2024-11-05 § 188

Beslutad av	Digitaliseringschef
Datum	2025-12-18
Ersätter tidigare version	-
Gäller för	Kommunstyrelsen, nämnder
Dokumentansvarig	Informationssäkerhetssamordnare

Om handlingsplanen

Omfattning

Handlingsplanen för informationssäkerhet utgår från programmet för informationssäkerhet. Den innehåller **aktiviteter** för det informations- och cybersäkerhetsarbete som informationssäkerhetsteamet bedömer behöver göras under 2026. Detta för att nå uppsatta mål och leverera i linje med ledningens viljeinriktning.

I tabellen nedan specificeras även vilka **områden** som aktiviteterna inryms inom och vem som har **huvudansvar** för att de genomförs. Observera att det är flera funktioner och roller som behöver samarbeta i respektive aktivitet.

För respektive aktivitet har **tid** för när de kan genomföras uppskattats. I kolumnen **resurser** finns även en uppskattning om vi inom förvaltningen ser att vi kan genomföra aktiviteterna inom ramen för ordinarie budget och bemanning eller om det kan tillkomma kostnader. Slutligen finns en kolumn med **kommentarer** som närmare beskriver aktiviteterna, dess innehåll och syfte.

Avgränsning

Handlingsplanen innehåller inga aktiviteter som informationssäkerhetsteamet gör löpande inom ramen för förvaltningen inom ramen för kommunens etablerade arbetssätt och ledningssystem för informationssäkerhet. Handlingsplanen innehåller inte heller specifika aktiviteter som planeras inom ramen för GDPR- och dataskyddsarbetet, dessa aktiviteter ingår i den handlingsplan som dataskyddssamordnaren ansvarar för.

Samordning

Arbetet med informationssäkerhet, cybersäkerhet och dataskydd samordnas av informationssäkerhets- och dataskyddssamordnare (och kollegor i informationssäkerhetsteamet) för att uppnå synergivinster och underlätta för verksamheternas informationssäkerhets- och dataskyddsarbete.

Samarbeten

Under 2026 kommer skärpta krav att ställas på kommunens informations- och cybersäkerhetsarbete och vi behöver ta höjd för att höja vår förmåga att hantera olika omvärldshot, stärka vår motståndskraft och prioritera säkerhetsåtgärder (utifrån informationsklassning och risk) vid digitalisering, anskaffning och utveckling. Detta genomsyrar hela informations- och säkerhetsarbetet, både i förvaltningen och i handlingsplanen för 2026.

Samarbeten, exempelvis inom Handslaget och mellan kommunen, IT-centrum och samverkanskommunerna, bedöms vara kritiska framgångsfaktorer för att hitta rätt nivå av säkerhet och skydd för känslig information och samhällsviktiga tjänster. Det vi behöver anpassa oss till är:

- Det osäkra omvärldsläget, att kommuner allt oftare blir utsatta för allvarliga cyberhot, attacker och informationspåverkan
- Skärpta lagkrav som ställs på kommuners informations-/cybersäkerhet fr.o.m. 2026 genom den nya cybersäkerhetslagen (NIS2), med tillhörande föreskrifter.
- Externa krav från myndigheter och externa aktörer att vi har ett ändamålsenligt ledningssystem för informations-/cybersäkerhet när vi ska ingå samarbeten.

Handlingsplan för informationssäkerhet 2026

Aktiviteter	Avser område	Huvudansvarig	Tid	Resurser	Kommentar
Informera om vad den nya cybersäkerhetslagen innebär för kommunen, ledningen och våra verksamheters informationssäkerhetsarbete.	Lagefterlevnad Ledningssystem för informationssäkerhet	Informationssäkerhets-samordnare (KS)	Q1	Mantimmar	Information bör utformas målgruppsanpassat för följande roller: kommunstyrelsen, KFLG, kontorschefer/ledningsgrupper, chefer (ev. chefsdialogen), informationsägare, systemägare och medarbetare.
Se över, föreslå och anpassa styrande och stödjande dokument med utgångspunkt i skärpta lagkrav för informations- och cybersäkerhet.	Lagefterlevnad Ledningssystem för informationssäkerhet	Informationssäkerhets-samordnare (KS)	Q1- Q2	Mantimmar	Skärpta krav kommer framför allt med den nya cybersäkerhetslagen (NIS2). Anpassningar kan även bli aktuella när det nya CER-direktivet som träder i kraft senare under 2026.
Rapportera status i informationssäkerhetsarbetet till KFLG och Kommunstyrelsen enligt konceptet ”Ledningens genomgång” och utifrån årsrapport.	Lagefterlevnad Ledningssystem för informationssäkerhet	Informationssäkerhets-samordnare (KS)	Q2	Mantimmar	I cybersäkerhetslagen, föreskrifter och ISO-standards i 27000-serien ställs krav på årlig rapportering till Kommunstyrelsen enligt konceptet ”Ledningens genomgång” som ska ge ett kunskapsunderlag för beslut.
Ta fram en utbildningsplan för 2026.	Kompetensutveckling	Informationssäkerhets-samordnare (KS)	Q1	Mantimmar	Planen ska ge förslag på ändamålsenlig, målgruppsanpassad utbildning. Målgrupper: Förtroendevalda politiker, chefer och medarbetare.
Genomföra kommungemensamma utbildningar i linje med utbildningsplanen för 2026.	Kompetensutveckling	Informationssäkerhets-samordnare (KS)	Q1- Q4	Mantimmar Ev. kostnad	Kostnad för extern utbildare och/eller digital utbildning kan tillkomma.
Utveckla utbildningsmaterial och APT-kitt till stöd för chefer	Kompetensutveckling	Informationssäkerhets-samordnare (KS)	Q1- Q2	Mantimmar	Ett utbildningsmaterial och APT-kitt togs fram under 2025. Det behöver utvecklas under 2026. Önskemål: komplettera med filmer.
Fortsätt dialogen med resp. kontorschef om hur de vill driva informationssäkerhetsarbetet i den egna verksamheten och vilket stöd de behöver för att göra det. Dokumentera förslag och behov.	Ledningssystem för informationssäkerhet	Informationsägare kontor (resp. nämnd)	Q1- Q3	Mantimmar	I enlighet med program för informationssäkerhet. Avser främst planer och återkommande aktiviteter (årshjul), som informationskartläggning, klassning, riskarbete, säkerhetsåtgärder och kravställning. Dokumentation/uppföljning i Security. Planering/rapportering i Stratsys.
Marknadsför internt arbetsätt/stödanvisningar för anskaffning och utveckling som levererades 2025. Bidra i prioriterade upphandlingar i syfte att kvalitetssäkra informationssäkerhetskrav.	Lagefterlevnad Säkerhet och skydd utifrån klassning (KRT) och risk	Informationssäkerhets-samordnare (KS)	Q1- Q4	Mantimmar	Genom att öka kännedomen om och få en bredare användning av det nya arbetsättet och stödanvisningarna kan informationssäkerhets- och dataskyddskrav säkerställas för nya tjänster, verksamhetssystem, välfärdstekniska lösningar, artificiell intelligens (AI), e-tjänster, etc.
Se till att ändamålsenliga kontinuitetsplaner för systembortfall tas fram och kvalitetssäkras. Prio samhällsviktiga och verksamhetskritiska system.	Kontinuitetsplanering	Säkerhetsskydd och beredskap (KS)	Q1- Q4	Mantimmar	Säkerhetsskydd och beredskap driver arbetet. Verksamheterna ansvarar för sin kontinuitetsplanering. Informationssäkerhetsteamet/systemförvaltare har bidragit med koncept/mall för arbetet och stöttar operativt i mån av tid.
Ta fram och öva krisplan för allvarliga IT-störningar och cyberattacker	Cybersäkerhet, IT- och informationssäkerhet	Säkerhetsskydd och beredskap (KS)	Q1- Q4	Mantimmar	Aktiviteten påbörjades under 2025. Utkast till rutin finns, men behöver färdigställas, förankras och övas tillsammans med berörda intressenter.
Säkerställ informationssäkerhet inom ramen för införandet av handslaget (SKR)	Lagefterlevnad Säkerhet och skydd utifrån klassning (KRT) och risk	Informationssäkerhets-samordnare (KS)	Q1- Q4	Mantimmar Ev. kostnader	Aktuella initiativ: Digital post, säker digital kommunikation (SDK), identitets- och behörighetsstyrning och välfärdstekniska lösningar. Projektet kräver fortsatt engagemang från många interna och externa intressenter. Säkerhetsåtgärder kan innebära kostnader.

Säkerställ ändamålsenlig behörighetsstyrning	Lagefterlevnad Säkerhet och skydd utifrån klassning (KRT) och risk	Verksamhetschef DOP (KS)	Q1- Q4	Mantimmar Ev. kostnader	Aktiviteten är komplex och kräver fortsatt engagemang från flera håll: HR, kontorschefer, informationsägare, systemägare, systemförvaltare, IT-centrum, informationssäkerhetsteamet och samverkanskommunerna. Säkerhetsåtgärder kan innebära kostnader.
Minimera glapp och se till att informations, cyber- och IT-säkerhet går hand i hand. Driva på så att samarbeten formaliseras och effektiviseras.	Lagefterlevnad Ledningssystem för informationssäkerhet Säkerhet och skydd utifrån klassning (KRT) och risk	Digitaliseringschef (KS)	Q1- Q4	Mantimmar	Denna aktivitet kräver engagemang från flera håll: Digitaliseringschef, stabschef (DSR), informationsägare, systemägare, systemförvaltare, informationssäkerhetsteamet, IT-centrum och samverkanskommunerna.
Undersök möjligheten att hitta ”ambassadörer” för informations- och cybersäkerhet i verksamheterna.	Systemiserat och riskbaserat arbetssätt	Informationssäkerhets- samordnare (KS)	Q2- Q3	Mantimmar	Medarbetare skulle kunna få intern kompetensutveckling av informations- säkerhetsteamet och vara en länk/ett extra stöd i verksamhetens arbete.
Följ upp, revidera och förankra risk- och sårbarhetsanalys (RSA) för informationssäkerhet	Säkerhetsåtgärder Skyddsåtgärder	Informationssäkerhets- samordnare (KS)	Q2- Q3	Mantimmar	En övergripande RSA för informations- och cybersäkerhet togs fram under 2025. Den ska ses över årligen.
Se till att säkra kommunikationstjänster (säker e-post, säkra digitala möten) och säker lagring införs i kommunen så snart som möjligt.	Lagefterlevnad Säker informationshantering	Informationssäkerhets- samordnare (KS)	Q2- Q4	Mantimmar Medför kostnader	Kravunderlag inför avrop/upphandling har arbetats fram av informations- säkerhetssamordnare. samverkanskommunerna och IT-centrum 2025. Tjänsterna ska införas 2026. Medför kostnader för införande och licenser.
Undersöka om vi kan ansöka om medel kopplade till de skärpta kraven på ökad cybersäkerhet	Lagefterlevnad Ledningssystem för informationssäkerhet	Informationssäkerhets- samordnare (KS)	Q2- Q4	Mantimmar	
Inleda arbetet med att klassa system för att säkerställa att de klarar att hantera skyddsvärd och känslig information (hög informationsklassning).	Lagefterlevnad Säkerhet och skydd utifrån informations- klassning och risk	Systemägare/ systemförvaltare (KS)	Q3- Q4		Informationssäkerhetsarbetet har hittills fokuserat på att klassificera information, men ett arbete behöver också göras för att klassa kommunens befintliga system - även s.k. ”OT-teknik” som t.ex. används i styrsystem, skalskydd, kameror och robotar (t.ex. läkemedelsrobotar)
Ta fram en handlingsplan för 2027	Ledningssystem för informationssäkerhet	Informationssäkerhets- samordnare (KS)	Q4	Mantimmar	Innehållet baseras på status för de aktiviteter som genomförts under året, externa krav, omvärldsläget och verksamhetsbehov för 2026,