Informationssäkerhet

Stödanvisning HubS

säkra digitala kommunikationstjänster och säker lagring

Östhammars kommun

Målgrupp	Användare av HubS, alla kontor och verksamheter
Avsändare	Kommunledningskontoret, Digitalisering och projektledning
Dokumentansvarig	Informationssäkerhetssamordnare
Framtagen	2026-06-18
Reviderad	-

ÖSTHAMMARS KOMMUN
– EN DEL AV ROSLAGEN

Innehåll

Innehåll

Innehållet i stödanvisningen utgår från kommunens program och vägledning för informationssäkerhet och ger instruktioner för användning av HubS – kommunens sammanhållna system för säkra digitala kommunikationstjänster och säker fildelning/lagring.

Mål och syfte

Ambitionen är att skapa förutsättningar för medarbetare som hanterar skyddsvärd och känslig information att kommunicera, dela information och samarbeta på ett säkert sätt.

HubS säkra tjänster

HubS är en plattform som är byggd för säkra verktyg inom digital kommunikation. I HubS kan du dela information och kommunicera på ett säkert sätt via:

- **Säkra digitala möten med chatt** – trygga möten med interna och externa deltagare
- **Säkra meddelanden med säker e-post** – meddelanden som skickas till/från säkra personliga brevlådor och/eller gruppbrevlådor – internt och externt.
- **Säkra meddelanden med säker digital kommunikation (SDK)** – meddelanden som skickas mellan myndigheter – bygger på adressböcker som anslutits till SDK.
- **Säkra filer/säker lagring** – filhantering, lagring och delning av dokument.

Plattformen bygger på modern säker teknik och är kravställd så att informationen behandlas inom EU/EES, det betyder att ingen tredjelandsöverföring sker. Det gör att HubS har en högre säkerhetsnivå än vanlig e-post, Teams och andra generella samarbetsverktyg. Informationen hanteras i en kontrollerad miljö med starkare styrning av åtkomst, autentisering och spårbarhet. ”Tillitsnivåer” lägger på ett extra säkerhetslager. De avgör hur mottagaren eller mötesdeltagaren behöver identifiera sig innan personen får åtkomst.

Även att HubS ger en hög teknisk grundsäkerhet är det viktigt att som användare välja rätt verktyg, tillitsnivåer och mottagare. Det är också viktigt att hålla behörigheter aktuella.

Information som ska hanteras säkert

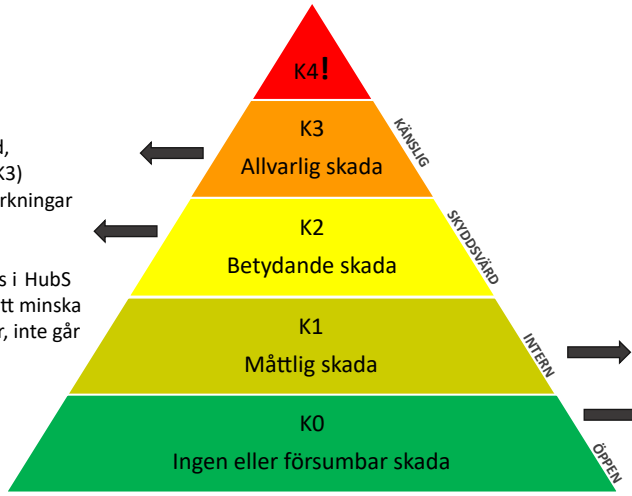
Den mesta information kommunen hanterar är öppen eller intern, men vi har också sekretessbelagd och känslig information som behöver ett extra skydd och hanteras säkert.

HubS är främst avsedd för hantering av skyddsvärd och känslig information. Vid osäkerhet om informationens känslighet och skyddsvärde, ta det säkra före det osäkra och använd HubS.

Vilken information ska hanteras i HubS?

HubS
- Information bedömd, högt klassad, konfidentialitetsnivå 2 och 3 (K2, K3)
- Betydande eller allvarliga skadeverkningar
- Skyddsvärd och känslig

… ska ges ett extra skydd och hanteras i HubS (och i säkra verksamhetssystem) för att minska risken att den kommer i orätta händer, inte går att nå, manipuleras eller förstörs.



Teams, Outlook, etc.
Den mesta information vi hanterar är öppen (K0) eller intern (K1).
Den behöver sällan något förstärkt skydd och ska hanteras som vanligt.

Konfidentialitet nivå 4 (K4) – synnerligen allvarlig skada – säkerhetsskyddsklassad
Exempel: Rikets säkerhet (hanteras av Säkerhetsskyddschef enl. separat rutin).

Konfidentialitet nivå 3 (K3) – allvarlig skada – hög skyddsnivå
Exempel: Känsliga personuppgifter[1], kartskikt, risker, sårbarheter, incidentrapporter, anbud upphandling (pågående), sekretessbelagda bygglovshandlingar.

Konfidentialitet nivå 2 (K2) – betydande skada – utökad skyddsnivå
Exempel: Skyddsvärda personuppgifter[2], samlade beredskaps- och kontinuitetsplaner.

Konfidentialitet nivå 1 (K1) – måttlig skada - grundläggande skyddsnivå
Exempel: Avtal, bygglov, ansökningar, icke-känsliga personuppgifter (t.ex. kontaktuppgifter).

Konfidentialitet nivå 0 (K0) – ingen eller försumbar skada – låg skyddsnivå
Exempel: Allmän information, rekryteringsannonser, nyheter på kommunens webbplatser.

Läs mer om hur information klassas och bedöms som skyddsvärd eller känslig: Informationssäkerhet

Tillitsnivåer i HubS

Level Of Assurance (LoA) betyder tillitsnivå. Med tillitsnivå avses grad och säkerhet och tillförlitlighet. Det anger hur säkert mottagaren behöver identifiera sig innan personen får ta del av informationen. Det är den som skickar/delar information via HubS som i praktiken väljer vilken tillitsnivå mottagaren ska använda för att ta del av informationen. Tillitsnivån anger hur säkra vi behöver vara på att informationen verkligen når rätt person. Ju högre

[1] Kan t.ex. vara utredningar om barn, elevdata- och omdömen, uppgifter om brukare, personliga förhållanden, hälsa, allergier, vård, omsorg, journaler, religiös och politisk åskådning, sexuell läggning, genetiska uppgifter och biometriska uppgifter som används för att entydigt identifiera en person. Se IMY https://www.imy.se/
[2] Kan t.ex. vara mötesbokningar med personliga uppgifter personuppgifter kopplade till fler uppgifter om individer/grupper, löner, lagöverträdelser, värderande uppgifter och information som rör någons privata sfär.

tillitsnivå, desto starkare kontroll krävs innan mottagaren får åtkomst till informationen eller kan delta i ett möte. Det är viktigt att välja rätt tillitsnivå utifrån informationens klassning och skyddsvärde - och vilka konsekvenser det kan få om fel person får tillgång till den.
En för låg tillitsnivå kan innebära att känslig information når fel person. En för hög tillitsnivå kan istället skapa onödiga hinder, till exempel genom att mottagaren behöver ange telefonnummer, använda SMS-kod eller identifiera sig med e-legitimation, trots att det inte behövs.

Grundfrågan är: ”Hur allvarligt skulle det vara om fel person fick tillgång till informationen?”

Välj tillitsnivå utifrån informationens klassning, skyddsvärde och risk
I HubS finns tre tillitsnivåer:

- LoA 1 – kan användas för öppen och intern information (K0- och K1-klassad)
- LoA 2 – kan användas för skyddsvärd information (K2-klassad)
- LoA 3 – ska användas för känslig information (K3-klassad).

Det som styr valet av tillitsnivå är också om du behöver veta exakt vem mottagaren är eller om det räcker att informationen når rätt e-postadress, rätt funktion eller rätt organisation.

LOA-nivå	Vad nivån innebär	När LOA-nivån används
LoA 1	Grundläggande åtkomst. Ingen särskild verifiering av mottagarens identitet krävs.	När risken är låg och det räcker att informationen går till rätt adress eller att deltagaren har fått rätt möteslänk.
LoA 2	Extra kontroll genom SMS-kod.	När risken är högre och åtkomsten behöver skyddas bättre, men det inte är nödvändigt att identifiera mottagaren med e-legitimation. Det kan t.ex. gälla större mängder personuppgifter eller information som skulle kunna orsaka olägenhet om den hamnar fel.
LoA 3	Mottagaren identifierar sig med e-legitimation, t.ex. BankID.	När det är viktigt att säkerställa att mottagaren eller mötesdeltagaren är en viss identifierad person. Det kan t.ex. gälla känsliga och sekretessbelagda uppgifter som ska lämnas till den enskilde själv.

Exempel: Val av tillitsnivå för hantering av handlingar
I HUBS bör tillitsnivån väljas utifrån utlämnandets risk och om mottagaren måste vara en viss identifierad individ. LoA 1 bör vara standard för offentliga handlingar där mottagaren inte behöver identifieras. LoA2 kan användas när man vill minska risken för fel mottagare, till exempel vid större mängder personuppgifter. LoA3 bör reserveras för de fall där utlämnandet förutsätter säker identifiering, till exempel sekretessbelagda uppgifter till den enskilde själv, partsrelaterade utlämnanden eller villkorade utlämnanden.

Säkerhetsmedveten användare

Den tekniska säkerheten och tillitsnivåer och är bara en del av säkerheten. Minst lika viktigt är det att vara säkerhetsmedveten som användare av plattformen. Kom ihåg att alltid kontrollera att det är rätt kontaktuppgifter och att endast rätt personer får åtkomst. Vid digitala möten behöver man även kontrollera deltagarlistan och tänka på om obehöriga kan höra samtalet eller se skärmen. Vid delade lagringsytor behöver behörigheterna följas upp och tas bort när de inte längre behövs.

Om något går fel… Anmäl incident när den riskerar att påverka eller påverkar informationssäkerheten och/eller skyddet av personuppgifter: Incidentanmälan informationssäkerhet - Östhammars kommun.

Allmänna handlingar

Se bilaga Tillämpningsanvisningar till allmänna handlingar och gallring

Gallring

Gallring handlar om att välja ut vilka dokument/uppgifter som ska bevaras och vilka som kan tas bort. Det är en nödvändig och viktig aktivitet för att skapa ordning, effektivitet och säkerhet i vår informationshantering.

Dokument/uppgifter som inte utgör allmänna handlingar men rymmer personuppgifter måste rensas ut då de blivit inaktuella. Att gallra skyddsvärd och känslig information är nödvändbart för att skydda enskilda individers integritet, minimera skador vid eventuella dataläckor och efterleva lagar och regler. Enligt dataskyddsförordningen (GDPR) får personuppgifter inte sparas längre än nödvändigt och det gäller även i HubS. Personuppgifter får bevaras längre för arkivändamål av allmänt intresse (men detta gäller *inte* i HubS), utan bevarandehandlingar ska då överföras till verksamhetssystem eller diarium. En rekommendation är därför att ta för vana att alltid gallra information/dokument manuellt när ett ärende är avslutat.
Kom ihåg att spara uppgifter som hör till ett specifikt ärende enligt verksamhetens rutin och i det/de säkra verksamhetssystem som används för ändamålet. Uppgifter om gallring ska framgå av kommunens dokumenthanteringsplaner.

Notera att information och dokument som skickas/tas emot med säkra digitala meddelanden eller kommuniceras i säkra digitala möten/säker chatt gallras automatiskt var tredje månad!
För tjänsten säker lagring sker ingen automatisk gallring, utan gallringen görs manuellt. Gallringen ska göras så snart ett dokument är inaktuellt.

För mer information, se bilaga Tillämpningsanvisningar till allmänna handlingar och gallring.

Kontakt

Informationssäkerhetsteamet nås vardagar via infosäkerhet@osthammar.se

Mer information och stöddokument

Bilaga: Tillämpningsanvisningar till allmänna handlingar och gallring
Informationssäkerhetsrelaterade stödanvisningar finns på Ines:

- https://ines.osthammar.se/service-support-och-stod-i-arbetet/informationssakerhet/
- Hantera information säkert
- Klassa information
- Skyddsvärt och känsligt
- GDPR och dataskyddsarbete

Utbildningsfilmer och guider finns i den digitala läroplattformen InfoCaption:

- Säkra digitala kommunikationstjänster (HUBS)