STRATEGI
PROGRAM
PLAN
POLICY
RIKTLINJER
REGLER

REGLER FÖR INFORMATIONS-SÄKERHET

HÖGANÄS KOMMUN

Fastställt av: Kommunfullmäktige
Datum: 2022-04-24
För revidering ansvarar: Informationssäkerhetsansvarig
För eventuell uppföljning och tidplan ansvarar: Informationssäkerhetsansvarig
Dokumentet gäller för: Samtliga förvaltningar och kommunala bolag
Dokumentet gäller till och med: Tills vidare

Innehållsförteckning

1 OMFATTNING

Reglerna konkretiserar bestämmelserna i *policy för informationssäkerhet och personuppgiftshantering (KS/2019/255)* och *riktlinjer för informationssäkerhet (KS/2022/100)* som gäller för Höganäs kommunkoncern.

Kompletterande regler och rutiner finns i verksamheten för specifika IT-stöd eller i genomförd informationsinventering. Informationens klassning (öppen, grundläggande, utökad eller hög) är det som tillsammans med säkerhetsåtgärderna avgör hur informationen får hanteras.

Som medarbetare ansvar du för information du hanterar eller kommer i kontakt med i din anställning/uppdrag. I ansvaret ingår att

- delta i utbildningar i informationssäkerhet
- i eget arbete följa policy, riktlinjer och regler för informationssäkerhet samt personuppgiftshantering.
- vid användning av IT-stöd ta del av instruktioner om hur dessa resurser ska hanteras, vilka villkor och vilket ansvar som gäller
- rapportera informationssäkerhetsrelaterade brister och incidenter.
- vid tillgång till information som du inte borde ha tillgång till snarast informera närmaste chef eller uppdragsgivare.

1.1 INFORMATIONSHANTERING

Se Riktlinjer för Informationssäkerhet 1.3 Introduktion – vad är informationssäkerhet

Följande regler gäller vid informationshantering.

- Du lagrar information enbart i avsett IT-stöd eller på avsedd lagringsplats, vilket anges i verksamhetens dokumenthanteringsplan.
- Du lagrar inte information längre än nödvändigt vilket innebär att du regelbundet går igenom och rensar arbetsanteckningar och tillfälliga dokument.
- Du använder e-posten som en kommunikationsväg och inte som en lagringsplats.
- Du hanterar enbart information du har behörighet att hantera. Vid tillgång till information som du inte borde ha tillgång till ska du snarast informera närmaste chef eller uppdragsgivare.

1.1 UTBILDNING OCH INFORMATION

Se riktlinjer för informationssäkerhet 2.7 Medarbetaren
Som medarbetare ska du

- Delta i verksamhetsspecifik utbildning och information om lagringsplats och regler för användning av verksamhetens IT-stöd.
- Ta del av grundläggande utbildning i informationssäkerhet för alla medarbetare
- ta löpande del av information om informationssäkerhet som delges via intranätet, APT eller andra informationskanaler inom verksamheten.

1.2 AVVIKELSER

Se riktlinjer för informationssäkerhet 3.2 Incidenter

- Som medarbetare är du skyldig att rapportera brister eller incidenter så snart du upptäcker dem.

1.3 SÄKERT BETEENDE

Se riktlinjer för informationssäkerhet 3.6 säkert beteende

Som medarbetare ansvarar du för att

- den information du hanterar i offentliga miljöer har skyddsnivå öppen.
- Information med hög skyddsnivå inte kommuniceras muntligt i offentliga miljöer
- telefonsamtal inte kan höras av obehöriga om du är på en publik plats eller till exempel lämnar ett möte för att besvara ett samtal.
- Information på datorskärm eller mobila enheter är skyddad och inte kan läsas av obehöriga
- Låsa skärm på dator eller mobil enhet när du lämnar dem utan uppsikt.
- informationen inte oavsiktligt kan läsas eller höras av någon annan när du arbetar i en publik miljö som tåg, flygplats eller utbildningstillfällen.

1.4 LAGRING OCH SÄKERHETSKOPIERING

Se riktlinjer för informationssäkerhet 3.4 lagring och säkerhetskopiering

Som medarbetare ansvarar du för att

- enbart lagra information i avsett IT-stöd eller på avsedd lagringsplats, vilket anges i verksamhetens dokumenthanteringsplan.
- inte dubbellagrar, vilket innebär att du tar bort eventuella arbetskopior eller e-postmeddelande när informationen är överförd till IT-stödet.
- inte lagrar information längre än nödvändigt vilket innebär att du går igenom och rensar arbetsanteckningar och tillfälliga dokument. Gallringsintervall av allmänna handlingar anges i verksamhetens dokumenthanteringsplan.
- lagrar enbart information med skyddsnivå ***öppen*** på USB-minne, extern hårddisk, skrivbordet på datorn eller mobila enheter
- Fysiska dokument som innehåller annan information än öppen skyddsnivå ska förvaras inlåsta.

1.5 ANVÄNDNING AV KLIENTENHETER

Se riktlinjer för informationssäkerhet 5.2.2 certifiering av hårdvara och 5.4.2 underhåll, reparation och avveckling av hårdvara.

Klientenheter är samlingsnamnet för enheten du använder i ditt arbete för att ta del av eller skapa information, till exempel dator, Chromebooks smarta mobiler och surfplattor. Vid användning av klientenheter gäller att

- Klientenheter så som datorer, mobiler och surfplattor är kommunens egendom och ska enbart användas av behörig användare.
- Enheterna är personliga arbetsredskap och får inte lånas ut eller överlåtas om det inte är gemensamma enheter som delas av flera.
- Enheterna ägs av Höganäs kommun och det gäller även informationen som lagras i dessa.
- Uppsatta säkerhetsinställningar i enheter får inte ändras.
- Endast godkända programvaror får installeras på enheten.
- För alla klientenheter gäller att du enbart får lagra information i avsedda system och baserat på informationens klassning och skyddsåtgärder. Det är informationen som avgör användningen, inte enhetens förmåga.
  Var försiktig vid anslutning till externa eller okända nätverk då nätverkstrafiken kan avlyssnas.
- Vid avslut av anställning eller vid byte till en annan avdelning ska klientenheter hanteras i enlighet med de rutiner som finns och får inte behållas privat.
- För installation av system och applikationer som inte finns i ”Höganäs appkatalog” ska arbetsprocess för detta följas. Se mer information på arbetsnätet under Systemförvaltningsmodellen och IT-avdelningens supportsida frågor och svar.
- Vid förlust av klientenhet **omedelbart** låsa eller radera klientenheten samt polisanmäla förlusten. *Instruktion hur detta görs finns på IT-avdelningens supportsida på kommunens intranät.*
- att klientenheten placeras och skyddas mot stöld, extern påverkan samt miljörelaterade hot som värme, kyla och vätska. Speciellt utsatt är mobila enheter där risk för förlust, stöld eller skada är större.
- Att du inte kopplar in utrustning som manipulerar eller påverkar säkerheten i kommunens nätverk – en sådan handling betraktas som försök till intrång och kan leda till rättslig påföljd.

1.6 ANVÄNDNING AV IT-STÖD

Se riktlinjer för informationssäkerhet 2.1.4 medarbetarens ansvar

Som medarbetare ansvarar du för att

- inte använda program och applikationer som kan lyssna av, manipulera eller påverka kommunens IT-miljö – en sådan handling betraktas som försök till intrång och kan leda till rättslig påföljd.

- Vid kopiering eller distribution av upphovsrättsligt/skyddat material säkerställa att detta är tillåtet, det vill säga att rättighetsinnehavaren medger detta.
- vid användning av IT-stöd ta del av instruktioner om hur dessa ska hanteras, vilka villkor och vilket ansvar som gäller.

1.7 ANVÄNDARNAMN OCH LÖSENORD

Se riktlinjer för informationssäkerhet 3.8 användarnamn och lösenord

Som medarbetare ansvarar du för att

- aldrig dela ditt/dina lösenord med någon annan
- Inte utför något med någon annans inloggning.
- lösenord inte är synliga. De ska hanteras som en värdehandling.
- aldrig skriva ner ditt/dina lösenord eller spara det i webbläsare eller din hemdator.
- aldrig använda samma lösenord i arbetet och privat.
- aldrig använda ett användarnamn eller e-postadress från arbetet i privata sammanhang.
- använda olika lösenord för olika tjänster på webben även om de är jobbrelaterade. På så vis minskas riskerna att någon kommer åt information.
- Om du arbetar i system där lösenordsbyte inte är tvingande, ska du ändå byta ut ditt lösenord för att hålla hög säkerhet.
- alltid byta ditt/dina lösenord om du förlorat din dator, surfplatta eller mobil eller om du tror att någon har kännedom om ditt/dina lösenord.
- Inte använda automatisk minnesfunktion för lösenord. Om du loggar in på webbsidor så ska du inte låta webbläsare spara lösenordet, utan alternativet ”Nej” ska väljas om du får en sådan fråga.
- ditt lösenord är - svårt att gissa för någon annan. Det ska därför inte kunna förknippas med dig som person, och dessutom ha en viss längd och komplexitet.
- Skydda mobila enheter med en låskod som inte får motsvara någon del i ditt telefonnummer, ditt personnummer eller relaterade personnummer.
- Låskoderna inte är enkla såsom 000 000, 123 456, 987 654 eller motsvarande. Du ska inte ha en kod som du använder i andra sammanhang, till exempel till passage eller din privata e-legitimation.

1.8 SKYDD MOT SKADLIG KOD

Se riktlinjer för informationssäkerhet 5.5.2 skydd mot skadlig kod

Som medarbetare ansvarar du för att

- aldrig stänga av eller på annat sätt påverka installerat skydd mot skadlig kod.
- enbart ansluta godkänd utrustning till kommunens nätverk, anslut till exempel inte ett USB-minne som du använder privat eller du fått av någon annan.

- Vara ”sunt” -misstänksam, undvik att klicka på länkar i e-post eller på webbsidor om du inte är säker på avsändaren.
- Du endast öppnar bifogade filer i e-post om de kommer från en känd avsändare och en bilaga är förväntad.
- Vara observant på om klientenhet beter sig långsamt eller konstigt. Vid misstanke om skadlig kod kontakta kommunens IT-support

1.9 INTERNET OCH SOCIALA MEDIER

Som medarbetare ansvarar du för

- nedladdning och installation av upphovsrättsligt material som film, musik, med mera inte sker utan stöd i lag, avtal eller skriftligt tillstånd från rättighetsinnehavaren.
- Enbart publicera eller dela öppen information på internet
- inte besöka webbplatser med till exempel brottslig verksamhet, rasism, diskriminering, extrempolitiskt eller pornografiskt innehåll.
- Du använder internet i tjänsten och eventuellt annat användande av internet inte stör ordinarie arbetsuppgifter eller innebär merkostnader som inte arbetsrelaterade för kommunen.
- Om du är ansvarig för ett konto i någon av våra sociala medier ansvarar du även för informationen i dessa.
- Kommentarer/frågor i sociala media ska bemötas/besvaras inom 24 timmar förutom över helger, då svar ges snarast möjligt kommande arbetsdag. Du behöver kontrollera innehållet och ta bort informationen om den inte kan anses ha öppen skyddsnivå.
- Innan du raderar en kommentar eller meddelande ska innehållet samt information om dess avsändare sparas. Såväl avpublicerad som raderad kommunikation ska bevaras och hållas ordnad.
- Inlägg från utomstående som innehåller sekretessbelagda uppgifter ska tas bort från mediet och tas om hand för registrering.

1.10 KOMMUNIKATION OCH DELNING AV INFORMATION

Se riktlinjer för informationssäkerhet 2.3 ledningssystem för informationssäkerhet

Som medarbetare ansvarar du för att följa informationens klassning med tillhörande skyddsnivåer och säkerhetsåtgärder vid kommunikation och delning av information, internt eller externt.

Viss information omfattas av sekretess och tystnadsplikt vilket innebär att det är förbjudet att lämna ut sekretesskyddade uppgifter, vare sig det görs muntligen eller skriftligen. Den

som röjer en sådan uppgift kan dömas till böter eller fängelse för brott mot tystnadsplikt enligt brottsbalken.

1.11 E-POST

E-post är en kommunikationskanal och din brevlåda är inte en lagringsplats. Du ansvarar för att gå igenom din e-postbrevlåda och ta bort information som inte är aktuell. Det finns några generella regler för e-post som du måste följa. Detta gäller även gemensamma funktionsbrevlådor eller förvaltningsbrevlådor.

- Du använder inte din @hoganas.se-e-post för privata syfte, du använder din privata e-postadress för privat kommunikation.
- Det finns en särskild koncernövergripande dokumenthanteringsplan för e-post som du ska följa. Den anger vad du ska rensa direkt, till exempel besvarade inbjudningar, information för kännedom och annan information som bedöms som inaktuell när du läst den.
- För intern kommunikation har vi i de flesta fall andra kanaler än e-post (till exempel intranät, Teams i M365, meddelandefunktion i verksamhetssystem).
- Du får i din e-post aldrig förvara information som
  - omfattas av sekretess enligt OSL,
  - känsliga personuppgifter enligt artikel 9 i Dataskyddsförordningen eller
  - information som omfattas av NIS-direktivet om skydd för samhällsviktiga funktioner.
- Får du skickat sådan information till dig ska du
  - Överföra informationen till korrekt IT-stöd
  - Radera meddelandet och tömma papperskorgen i e-postbrevlådan
  - Svara/vidarebefordra i ett nytt meddelande så att du inte sprider känsliga uppgifter.
- Du får inte klicka på länkar i e-post från avsändare du inte kan verifiera
- Du får inte lämna ut uppgifter om användarnamn eller lösenord via länkar i e-post
- Det är inte tillåtet att automatiskt vidarebefordra e-post till externa e-postadresser.

1.12 FAX

Faxmeddelande är en kommunikationsväg som fortfarande används i vissa verksamheter. Om du använder fax för att skicka information som omfattas av sekretess eller känsliga uppgifter gäller följande

- Du ska säkerställa att det är rätt mottagare – du behöver alltså först ringa till mottagaren för att kontrollera faxnumret.
- Du ska skicka ett ”kontrollfax” med begäran om att mottagaren ska bekräfta vem hen är och att kontrollfaxet är mottaget.

- När du fått det faxet returnerat och är säker på avsändaren kan du skicka informationen till mottagaren. Hen ska stå vid faxen och ta emot utredningen direkt och omedelbart efter sändning bekräfta att hen mottagit rätt antal sidor och att utredningen är upphämtad från faxen.
- Du ska ”din” fax radera informationen i minnet så att den inte kan återskapas och mottagaren ska göra samma sak.

1.13 DISTANSARBETE

Se riktlinjer för informationssäkerhet 2.5.1 skyddsnivå och skyddsåtgärder

Idag när de flesta enheter vi har är mobila och medger arbete på annan plats än det fysiska kontoret kan det vara lätt att tro att det är enheten som avgör om vi kan ta med informationen utanför kommunens lokaler. Det är klassningen och skyddsåtgärderna som avgör om du kan arbeta med informationen på distans eller inte.

- Vid distansarbete måste godkänd säker utrustning och anslutning användas
- Försiktighet ska iakttas vid arbete i publika miljöer, exempelvis kan skärmen skyddas med sekretesskydd.
- Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme.
- Arbete med information med högt skyddsvärde får inte ske i publika miljöer.
- Du ansvarar för att säkerställa att den information du hanterar är godkänd för distansarbete och för att informationen skyddas på rätt sätt.

1.14 FYSISK SÄKERHET

Som medarbetare ansvarar du för att

- låsa skärmen när du lämnar datorn för en kort stund. Du ska även låsa ditt kontorsrum när du lämnar det.
- logga ut och stänga av datorn vid arbetsdagens slut.
- Skriftligt material som innehåller annan information än skyddsnivå öppen ~~får~~ inte ligger framme så att obehöriga kan ta del av den. Materialet ska låsas in i godkända skåp när du lämnar arbetsplatsen, även för kortare stunder.
- Vid utskrift av dokument omgående hämta~~s~~ upp det ur skrivare. Vid utskrift av konfidentiell information ska utskriften övervakas så att du är säker på att ingen obehörig kan läsa informationen.
- Pappersdokument som innehåller konfidentiell information vid gallring strimlas eller kastas i godkända säkerhetskärl.
- Besökare inte vistas utan uppsikt i lokaler där konfidentiell information kan finnas. Obekanta personer i sådana lokaler ska tillfrågas vem de söker och hjälpas tillrätta. All personal i kommunkoncernen ska kunna identifiera sig med tjänstekort (fysiskt eller digitalt) med bild och titel.

- Mottagare av besök ansvarar för besökare så länge de befinner sig i kommunens lokaler.

1.15 NÄR DU AVSLUTAR DIN ANSTÄLLNING ELLER UPPDRAG

se riktlinjer för informationssäkerhet 2.7.3 avslut eller ändring av anställning

När din anställning eller ditt uppdrag upphör har du inte längre rätt att ha tillgång till den information du tidigare haft i ditt uppdrag. Det innebär att all information ska återlämnas eller lämnas över till kollega. Detta gäller såväl fysisk som digital information. All information som inte ska bevaras, alltså arbetsmaterial eller tillfälliga anteckningar, ska kastas, den information som ska bevaras ska finnas i avsett IT-system. Har du arbetsmaterial i din e-post, eller i personliga lagringsytor som till exempel Mina dokument eller Onedrive, ska du gå igenom dessa och identifiera eventuell information som efterträdare kan behöva. Informationen ska sparas ner i avsett system eller gemensamt identifierad arbetsyta och därefter raderas från din personliga lagringsyta.

Som medarbetare ansvarar du för att

- Fysisk information lämnas över till ansvarig chef
- arbetsmaterial i e-post eller i personliga lagringsytor ska identifieras och sparas ner i avsett system eller gemensamt identifierad arbetsyta och därefter raderas från din personliga lagringsyta.
- meddela din chef eller efterträdade vilken information som är överlämnad och var den är lagrad.
- personliga lagringsytor och e-post inte innehåller någon information när du avslutar din anställning eller uppdrag.
- Återlämnar taggar, kort för passage och nycklar
- Återlämnar enheter och annan hårdvara som du haft i din tjänst

Om du byter uppdrag inom kommunkoncernen ansvarar du för att den information du haft tillgång till i ditt tidigare uppdrag lämnas över och att din e-post inte innehåller någon information av vikt.

Regler för informationssäkerhet baseras på riktlinjer för informationssäkerhet, beslutade av Kommunfullmäktige med diarienummer KS/2022/100.