Antaget i kommunfullmäktige 2015-01-12, § 17

Riktlinje för användning av Internet, e-post och mobila enheter

Det ökande behovet av mer flexibla arbetsformer ställer ökade krav på säkerhet i informationssystem dels för att kunna uppfylla lagkrav som ställs om sekretess och riktighet dels andra krav som tillgänglighet till information.

1. Inledning

Riktlinjen vänder sig till anställda och förtroendevalda samt annan som verkar inom Huddinge kommun eller använder kommunens verksamhetssystem. Den innehåller information för hur informationssäkerhet ska upprätthållas. Delar av den information som kommunen hanterar omfattas av skyddskrav i lagar och andra författningar samt offentlighets- och sekretesskrav.

Kommunens policy för informationssäkerhet stadgar att kommunen i arbetet med informationssäkerhet ska stödja sig på ISO-standard och Myndigheten för samhällsskydd och beredskaps rekommendationer för informationsklassificering och analys. Alla verksamhetssystem och behandling av information ska uppfylla basnivå för informationssäkerhet.

2. Säkerhetsorganisation

Kommunstyrelsen har det övergripande ansvaret för kommunens säkerhet. Säkerhetssansvaret följer linjeorganisationen och varje chef är ansvarig för att personalen utbildas inom säkerhet och känner till vilka säkerhetsbestämmelser verksamheten omfattas av. Det är av yttersta vikt att anställda får återkommande information och utbildning för att hög säkerhetsnivå ska kunna upprätthållas.

Inom varje förvaltning ska det finnas lokalt utsedda ansvariga som hjälper till med riskanalyser, genomför beslutade säkerhetsåtgärder och är behjälplig med incidentutredningar.

3. Användning av Internet, e-post och sociala medier

Kommunens e-postsystem är ett arbetsverktyg. Det får användas för privat bruk men bara om det inte inkräktar på arbetet, medför kostnader eller på annat sätt skadar kommunen.

E-postadresser tillhörande Huddinge kommun ska inte registreras för eller användas som identifikation för inloggning till applikationer eller system om det inte har anknytning till tjänsten.

Automatisk vidarebefordran från kommunala e-postkonton till externa e-postadresser ska inte ske.

Elektronisk post omfattas av samma regler för offentlighet som gäller för pappershandlingar. I tryckfrihetsförordningen regleras rätten att ta del av allmänna handlingar och det gäller även för e-post. Information som läggs in i e-postsystemets funktion för kalender och kontaktregister omfattas av samma krav.

Regler om öppnade och registrering av allmänna handlingar finns i offentlighets- och sekretesslagen (2009:400).

3.1 Typer av elektroniska brevlådor

Inom kommunen finns olika elektroniska brevlådor kopplade till olika verksamhetsgrenar inom förvaltningar eller för specifika funktioner. För varje brevlåda ska det finnas utsedd informationsägare som beslutar om och följer upp behörigheter till respektive brevlåda samt ansvarar för att inkommande och utgående handlingar hanteras lagenligt. Beslut om att öppna upp ny brevlåda ska fattas av verksamhetschef eller enhetschef.

Myndighetsbrevlådor

Kommunens officiella brevlåda administreras av kommunstyrelsens kansli.

Varje nämnd har också en officiell brevlåda. De administreras av respektive nämnds förvaltning. Andra myndighetsbrevlådor kan finnas hos en förvaltning, en skola eller en särskild grupp av tjänstemän.

Funktionsbrevlådor

Funktionsbrevlådor är knutna till en specifik funktion, exempelvis registrator eller ”Fråga servicecenter”, och administreras av den eller de tjänstemän som ansvarar för denna funktion.

En anställds brevlåda

Anställds brevlåda är knuten till enskild tjänsteman som också ansvarar för administrationen av den.

3.2 Hantering av elektroniska brevlådor

De handlingar som inkommer till eller skickas från kommunala e-postkonton och som utgör allmänna handlingar ska följa Huddinge kommuns rutin för öppning, registrering och hantering av allmänna handlingar.

Öppnande av brevlåda

En elektronisk brevlåda ska som en följd av reglerna i offentlighets- och sekretesslagen öppnas varje arbetsdag. Var och en ska se till att den personliga brevlådan blir öppnad vid frånvaro. Detta kan ske genom att en kollega inom samma förvaltning tilldelas behörighet att läsa och besvara inkomna handlingar.

För att registrator eller en annan anställd på samma förvaltning ska få tillgång till någons personliga brevlåda, om denne inte har getts elektronisk möjlighet att själv logga in, ska ägaren lämna en skriftlig fullmakt att öppna samtliga e-postmeddelanden som är adresserade till tjänstemannen personligen, men som kan antas röra tjänsteangelägenheter. Om medgivande saknas och vidarebefordran inte sker har förvaltningschef rätt att vid behov fatta beslut om öppnande av brevlåda.

Kommunen har enligt offentlighets- och sekretesslagen skyldighet att besvara förfrågningar skyndsamt. Vid planerad frånvaro ska frånvarohanteraren i e-postsystemet aktiveras. Den särskilda mappen för spam ska kontrolleras dagligen för att säkerställa att inga inkommande meddelanden felaktigt hamnat där.

Sekretessbelagd upptagning

E-post/upptagningar, exempelvis dokument, bild- eller filmfiler, vilka bedöms omfattas av sekretess får inte förvaras i en elektronisk brevlåda. Om ett sådant meddelande kommer in till en elektronisk brevlåda i kommunen ska meddelandet omedelbart föras över till avsedd lagringsyta, som specificeras i nämndens dokumenthanteringsplan, och gallras ur den elektroniska brevlådan.

Gallring

E-post i kommunens e-postsystem gallras automatiskt enligt särskilt beslutade anvisningar för Huddinge kommun.

3.3 Internetanvändning

Internet ska primärt användas som ett redskap i arbetet. Privat användning i mindre omfattning accepteras så länge det inte inkräktar på arbetet, medför kostnader eller på annat sätt skadar kommunen.

Det är inte tillåtet att för privata syften besöka webbplatser med extrempolitiskt, pornografiskt eller liknande innehåll. Det är vidare inte tillåtet att skicka kedjebrev.

De temporära filer (cookies) som lagras i mobila enheter vid surfing på Internet är allmänna handlingar och kan komma att lämnas ut om allmänheten begär att få ut information om vilka webbsidor enskilda anställda eller förtroendevalda har besökt.

3.4 Sociala medier

I kommunikationsarbetet ger sociala medier möjlighet till en bredare dialog och ökad delaktighet. Huddinge kommun har fastställda riktlinjer för kommunikation via sociala medier. Riktlinjerna för användning av sociala medier gäller endast medier där det är möjligt att kommunicera, föra en dialog. Om teknisk plattform för sociala medier används utan dialogform omfattas mediet av webbriktlinjerna. Riktlinjerna talar om hur vi som tjänstemän bör uttala oss i tjänsten.

3.5 Kontroll av Internet- och e-postanvändning

All användning av Internet registreras i en logg. Loggningen omfattar uppgifter om användarnamn och namnet på den webbplats som besökts. Om det vid genomgång av loggarna framgår att det förekommer surfing på webbplatser som enligt riktlinjerna inte får besökas, eller om surfing förekommer i onormalt stor omfattning på vissa tillåtna kategorier webbplatser kan administrativa direktören eller förvaltningschef besluta om kontroll av enskilda individers surfing.

Det förs även en logg över all e-post som innefattar uppgifter om avsändare, mottagare, ärendemening, tidpunkt och storlek på meddelandet samt namnet på bifogade filer.

Kommunen utövar normalt ingen kontroll över de anställdas e-postmeddelanden. Kommunen kan komma att ta del av de uppgifter som finns i ett e-postmeddelande om det är nödvändigt för att uppfylla myndighetens skyldigheter om allmänna handlingars offentlighet.

Kommunen kan även komma att ta del av de uppgifter som finns i ett e-postmeddelande om det är nödvändigt med hänsyn till informationssäkerheten, exempelvis vid virus- och hackerangrepp eller för att utreda och förhindra brott.

Beslut om kontroll fattas av administrativa direktören eller förvaltningschef.

4. Distansarbete och mobil användning av IT

Verksamhetssystem som får bearbetas externt utanför kommunens ordinarie tjänsteställen ska ha föregåtts av risk- och sårbarhetsanalys för att säkerställa korrekt informationshantering och tillämpliga säkerhetslösningar. De mobila enheter som kommunen har bedömt får användas i tjänsten får utnyttjas efter att de har försetts med tillämplig säkerhetslösning.

Varje chef ansvarar för att personalen har erforderlig kompetens för mobilt utnyttjande av IT samt att lagar, policys och riktlinjer är kända och följs.

4.1 Informationsklassificering

Information som upprättas, bearbetas, lagras eller distribueras ska hanteras i enlighet med kommunens klassningsmodell för informationstillgångar. Utgör informationstillgången allmän handling finns även legala krav att beakta vilket framgår av Huddinge kommuns rutin för öppning, registrering och hantering av allmänna handlingar.

Information klassas i fyra olika nivåer beroende på konsekvenserna av att informationen kommer i orätta händer, förloras eller inte är tillgänglig vid given tidpunkt:

- *Allvarlig/katastrofal,* där information som kommer i orätta händer kan medföra allvarlig/katastrofal skada (information rörande rikets säkerhet)
- *Betydande,* där information som kommer i orätta händer kan medföra betydande skada (exempelvis information med mycket hög känslighet såsom inom socialtjänst samt hälso- och sjukvårdsuppgifter)
- *Måttlig,* där spridning av information kan medföra måttlig skada (exempelvis personuppgifter och annan verksamhetsinformation)
- *Ingen eller försumbar*, där informationen utgörs av enbart allmän och publik information och där en spridning av informationen endast medför ringa eller ingen skada

Klassificeringen har till syfte att säkerställa att all information ges nödvändigt skydd. Vid bedömning av informationens värde ska förutom legala krav även verksamhetens behov av åtkomstbegränsning, riktighet, tillgänglighet och spårbarhet beaktas.

4.2 Mobil access till informationssystem

Inom Huddinge kommun finns möjlighet att bedriva arbete på distans, vilket innebär att arbete utförs med hjälp av datateknik i andra än arbetsgivarens lokaler. Vid distansarbete gäller samma krav för hantering av information som för ordinarie arbetsplats.

Verksamhetschef respektive systemägare beslutar om ett systems information får bearbetas på distans och med vilken typ av mobil utrustning. Beslut om anslutning som gäller verksamhetskritiska system ska ha föregåtts av dokumenterad risk- och sårbarhetsanalys varvid riskreducerande åtgärder ska ha genomförts. Analysen ska särskilt beakta de risker som finns med behandlingen av känsliga uppgifter i mobila enheter samt integritetsrisker vid samkörning av stora informationsmängder. Riskanalysen utgör grund för att besluta om vilka säkerhetsåtgärder som ska gälla för anslutningen samt hur loggning och analys av tillgången till information ska ske.

Uppkoppling till system som innehåller information som klassats ha mycket hög nivå av känslighet får ske utanför arbetsgivarens ordinarie tjänsteställe om särskilt genomförda säkerhetslösningar finns för ändamålet.

För system som innehåller information som klassats ha hög nivå av känslighet får extern anslutning ske via krypterad förbindelse och efter stark autentisering såsom engångslösenord, e-legitimation, SITHS-kort eller motsvarande. Sådan information får skickas över e-post, internet eller motsvarande om krypterad lösning finns.

Information utgörande nivå hög får endast föras utanför arbetsgivarens lokaler på media som har försetts med krypterade säkerhetslösningar för exempelvis mobil/PDA, surfplatta, USB-minne, bärbar dator/hårddisk. Informationen ska skyddas med avancerat lösenord eller motsvarande.

Uppkopplingar ska följa den av kommunens centrala IT-sektion godkända teknik och standard. Rutiner ska finnas för återkommande uppföljning och logganalys av externa anslutningar samt behörigheter till verksamhetssystem.

Mobil utrustning och annat lagringsmedia som ska kasseras ska hanteras i enlighet med kommunens fastställda rutiner för att säkerställa att ingen känslig information finns kvar på det bärbara mediet. Enheter och annan hårdvara som har innehållit känslig eller sekretessbelagd information ska fysiskt förstöras efter att informationen raderats.

4.3 Extern parts anslutning till verksamhetssystem

Externa parters anslutning till verksamhetssystem ska ha föregåtts av dokumenterad risk- och sårbarhetsanalys samt följa den av kommunens centrala IT-sektion godkända teknik och standard för anslutningen.

4.4 Risk- och sårbarhetsanalys

Varje beslut om mobil access till information i verksamhetssystem ska ha föregåtts av risk- och sårbarhetsanalys. Syftet med analysen är att säkerställa verksamhetens kontinuitet och informationstillgångarnas säkerhet. Analyserna ska dokumenteras och föreligga varje beslut som medger access till informationen i verksamhetssystemen.

Riskanalysen ska fokusera på varje verksamhets viktigaste mål och uppgifter. Analys ska göras inför varje beslut som innebär större förändrade strategiska inriktningar för hur information ska behandlas eller lagras, exempelvis övergång till e-arkiv, delning av eller tillgång till myndighetsinformation eller annan övergång till nya typer av kommunikationslösningar. Den skyddsnivå som beslutas ska stå i proportion till det som ska skyddas.

Analysen ska omfatta de krav som ställs med avseende på:

- Sekretess (skydd mot obehörig åtkomst av information)
- Riktighet (åtgärder för att åstadkomma rätt kvalitet på information, att information inte obehörigen, av misstag eller på grund av funktionsstörning har förändrats)
- Tillgänglighet (åtgärder för att säkra drift och funktionalitet)
- Spårbarhet (möjligheten att fastställa vem som gjort vad eller att kunna verifiera orsaken till en händelse)

4.5 Personuppgiftsbiträdesavtal

Avtal ska finnas med leverantör eller annan som på uppdrag av kommunen lagrar eller behandlar information innehållande personuppgifter. Personuppgiftsombudet för förteckning över vilka biträdesavtal som finns i kommunen.

5. Tekniska säkerhetsåtgärder

Det finns en risk för vidarespridning av kommunens information vid anslutning och synkronisering mot externa system eller applikationer varför tekniska begränsningar eller skydd måste finnas. Spårbarhet ska finnas för information som det råder sekretess för eller annars betraktas som känslig eller verksamhetskritisk. Information som bedöms vara särskilt skyddsvärd eller känslig ska vara säkrad genom kryptering och får endast synkroniseras externt efter föregående stark autentisering.

Information som innehåller personuppgifter får endast synkroniseras med tjänster eller applikationer som kommunen har ett personuppgiftsbiträdesavtal med.

Information från verksamhetssystem som synkroniserats till mobila enheter ska arkiveras eller i förekommande fall raderas när informationen inte längre behövs. Enheter ska återställas till fabriksinställning innan annan övertar enheten.

5.1 Synkronisering av e-post och kalender till mobil enhet

Synkronisering får endast ske till enheter som har försetts med Huddinge kommuns valda säkerhetslösning.

5.2 Lagring och delning av information

Allmänna handlingar, sekretessbelagd information eller annan verksamhetskritisk information ska hanteras i enlighet med kommunens informationssäkerhetspolicy, dokumenthanteringsplaner samt Huddinge kommuns rutin för öppning, registrering och hantering av allmänna handlingar. Sådana handlingar får endast lagras på mobila enheter eller extern lagringsplats som kommunen har slutit avtal med och därmed kan styra tillgången till informationen. Originalet ska i förekommande fall lagras Huddinge kommuns verksamhetssystem. Information som ska mellanlagras för att senare överföras till förvaring i arkiv ska stödja de format som gäller för slutlig förvaring i e-arkiv och som anges i Riksarkivets författningssamling (RA-FS 2009:1 och 2009:2 eller senare upplagor).

Allmänna molntjänster där enskilda själva sluter avtal gällande lagring ska inte användas annat än efter dokumenterat beslut av administrativa direktören eller förvaltningschef och efter samråd med IS/IT-strateg om inte rätten finns att ingå avtal eller särskild fullmakt finns för detta.

Säkerhetskopiering sker av information som lagras i verksamhetssystemen. Information ska med jämna mellanrum sparas ned i verksamhetssystem samt arkiveras, gallras eller raderas när den inte längre behövs. Lagring på andra lagringsutrymmen än verksamhetssystemen ska betraktas som endast temporära.

5.3 Mobila applikationer

Mobila applikationer medger ett effektivt arbetssätt för mobila enheter. Applikationer med låg säkerhetsnivå eller virus utgör samtidigt en specifik risk för avsiktlig eller oavsiktlig spridning av information. Mobila applikationer får endast laddas ned och användas på de mobila enheter som har utrustats med Huddinge kommuns valda säkerhetslösning.

5.4 Incidenthantering

En incident är en handling eller händelse som påverkar informationstillgångars sekretess, riktighet eller tillgänglighet på ett negativt sätt som innebär skada för verksamheten. Det är inte incidenten i sig som är negativ för tillgången utan den eller de skador, konsekvenser, som incidenten leder till. Virusangrepp, identitetsstölder och skadlig kod ökar varför det är viktigt att följa kommunens vid var tid gällande säkerhetsföreskrifter. Vid inträffad incident ska kommunens rutiner för incidenthantering följas.

6. Uppföljning

Elektroniskt lagrad information ska vara skyddad mot förlust, förstörelse och förvanskning. Rutiner ska finnas som säkerställer läsbarheten av elektroniskt lagrad information under hela dess bevarandeperiod. Kommunarkivet kan hjälpa till med vilka format och vilken teknik som är lämplig att använda. För informationsmängder innehållande personuppgifter eller annars känslig information ska spårbarhet finnas som i logg utvisar på individnivå vem som har haft access till informationen, eventuella förändringar som har gjorts och när det skedde. För särskilt känslig information ska logguppföljning ske var tredje månad. Loggarna ska vara skyddade mot obehörig insyn och förändring.

Uppföljning ska ske fortlöpande för att säkerställa att verksamheten lever efter gällande lagar och fastställda policys och riktlinjer. Skyddsåtgärder ska följas upp i syfte att kontrollera att de ger avsedd effekt och verkar för att förbättra säkerheten. De ska fortlöpande kontrolleras och anpassas.

Respektive verksamhetschef, informations- och systemägare har ansvar för att se till att kontrollerna finns och genomförs.