Kungsbacka

Regler för informationssäkerhet

För medarbetare och förtroendevalda

Innehållsförteckning

Inledning

Kungsbacka kommuns *Säkerhets- och beredskapspolicy* är ett övergripande dokument i vilket kommunledningen uttrycker sitt stöd för och sin syn på informationssäkerhet.

Detta dokument – *Regler för informationssäkerhet för medarbetare och förtroendevalda* – konkretiserar Säkerhets- och beredskapspolicyn med mer detaljerad information och regler.

De här reglerna för informationssäkerhet gäller för alla medarbetare och förtroendevalda i Kungsbacka kommun. Reglerna gäller även extern personal, leverantörer och övriga externa aktörer som har tillgång till kommunens information.

Kungsbacka kommun är en stor organisation med många skilda verksamheter. Kompletterande regler till detta dokument kan därför finnas verksamhetsvis. Avvikelser från dessa kommungemensamma regler får dock aldrig göras utan särskilt tillstånd.

Reglerna för informationssäkerhet är baserade på den svenska och internationella standarden SS-ISO/IEC 27002/2014 och på Myndigheten för Samhällsskydd och beredskaps (MSB) metodstöd för informationssäkerhetsarbete.

1.1 Struktur och läsanvisning

Reglerna är uppdelade i avsnitt. Varje avsnitt består av informativa delar och regler som är obligatoriska. Samtliga regler är dessutom numrerade och presenterade i tabellform.

1.2 Vad är informationssäkerhet?

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för all information som vi hanterar. Detta gäller information i alla dess former; text, ljud, bild, film osv, och oavsett hur informationen lagras, bearbetas och kommuniceras. Det kan vara med stöd av IT, dokument eller direkt av oss människor i form av tal. Medan IT-säkerhet fokuserar på säkerhet i IT-baserad informationshantering handlar informationssäkerhet alltså om all information, oavsett form.

Information och de resurser som används för att hantera information benämns informationstillgångar. Målet är att upprätthålla nödvändig nivå på skyddet av kommunens informationstillgångar avseende;

- konfidentialitet - att information skyddas för obehörig insyn
- riktighet - att information är tillförlitlig, korrekt och fullständig
- tillgänglighet - att information är nåbar vid rätt tillfälle
- spårbarhet - att specifika aktiviteter som rör information kan spåras

Vad som är lämplig nivå av skydd för en viss informationsmängd beror på dessa krav, hotbilden och i vilka situationer informationen hanteras – hur den lagras, bearbetas och kommuniceras.

1.3 Medarbetarens ansvar för informationssäkerhet

Information är en viktig resurs för kommunen och är av stor betydelse för alla våra verksamheter. I kommunen hanterar vi varje dag mängder av information som berör allt vad vi gör inom våra olika verksamheter. Information kan förekomma i olika former, den kan vara muntlig, skriftlig eller finnas i IT-system. Information finns främst i form av texter men även bilder, symboler, filmer och ljud utgör information.

Medarbetarens kunskap och medvetenhet är ett viktigt skydd, till exempel att arbeta på rätt sätt med pappersdokument och IT-system, och att vara försiktig med konfidentiell information.

Säkerhet är inte bättre än den svagaste länken och det är viktigt att alla typer av skydd fungerar på ett bra sätt tillsammans. En stor del av kommuns informationssäkerhet beror därför på hur den enskilde medarbetaren hanterar informationen. Kungsbacka kommun ställer krav på att medarbetare, förtroendevalda, extern personal, leverantörer och andra externa aktörer (samtliga benämns fortsättningsvis i detta dokument som *medarbetare*) följer reglerna för informationssäkerhet beskrivna i detta dokument.

Utbildning och information om informationssäkerhet ska vara obligatorisk för alla nyanställda och utgöra en del av introduktionsprogrammet. Löpande ska dessutom alla anställda erbjudas utbildningar inom informationssäkerhet.

Om du som medarbetare har tillgång till känslig information ska du skriva under en tystnads- och sekretessförbindelse. En sådan förbindelse gäller även efter att anställningen eller avtalet har upphört.

Vid underlåtenhet att följa regler för informationssäkerhet följer kommunen rådande lagar och avtal. Lagbrott polisanmäls.

1.4 Informationsklasser

Viss information är mer känslig än annan. Behovet av skydd skiljer sig därför mellan olika typer av information och i olika situationer. Skyddsbehovet beror på legala krav och vilka konsekvenser det skulle få för verksamheten eller för enskilda individer om informationen sprids till obehöriga.

Kungsbacka kommun har en modell för att klassa hur känslig en informationsmängd är och hur den ska hanteras utifrån det. Modellen beskrivs i dokumenten *Rutin för klassificering av informationstillgångar* och *Protokoll för klassificering av informationstillgångar.*

Behöver du som medarbetare hjälp med att klassa en informationsmängd så kontakta kommunens specialist informationssäkerhet.

1.4.1 Konfidentiell information

Det viktigaste är att vi hanterar konfidentiell information på rätt sätt. Konfidentiell information är information som kräver att vi vidtar extra säkerhetsåtgärder på grund av legala krav och tänkbara konsekvenser för våra verksamheter och för enskilda individer. Exempel på konfidentiell information är känsliga personuppgifter enligt dataskyddsförordningen (GDPR) och information som omfattas av sekretess enligt offentlighets- och sekretesslagen (OSL). Även skyddade personuppgifter (skyddad identitet) är konfidentiell information.

Du kan läsa mer om personuppgifter och information som omfattas av sekretess och hur du hanterar den typen av information i ***Regler för hantering av information i Kungsbacka kommuns digitala samarbetsplattform och Office 365***

https://kungsbackakommun.sharepoint.com/sites/verksamhetsstyrning/ODMPublished/1263/Regler%20for%20hantering%20av%20information%20i%20Kungsbacka%20kommuns%20digitala%20samarbetsplattform%20och%20Office%20365.pdf

Det finns annan speciallagstiftning som reglerar hur konfidentiell information får hanteras. Exempel på sådan speciallagstiftning är patientdatalagen, lagen om informationssäkerhet för samhällsviktiga och digitala tjänster, och säkerhetsskyddslagen. Är du som medarbetare osäker på vilken lagstiftning som gäller för den information du hanterar, prata med din chef.

1.5 Skyldighet att rapportera incidenter och brister

Alla medarbetare har skyldighet att rapportera incidenter eller brister som misstänkts kunna medföra negativ påverkan på kommunens information. Det kan röra sig om till exempel:

- IT-angrepp/intrång
- Skadlig kod
- Oskyddad känslig information
- Brister i efterlevnad av regler för informationssäkerhet

IT- och informationsrelaterade incidenter och brister ska rapporteras enligt kommunens rutin för incidentrapportering. Medarbetare som har upptäckt incidenter eller svagheter där brott misstänks föreligga ska dock inte själva försöka bevisa sådana då det kan försvåra framtida utredningar.

1.6 Informationssäkerhet i praktiken

I detta avsnitt beskrivs de informationssäkerhetsregler som gäller i Kungsbacka kommun och som bidrar till en högre nivå av informationssäkerhet.

1.6.1 Lösenord

För att logga in till de flesta av kommunens IT-system används användar-ID och lösenord. Lösenorden är personliga och får inte göras kända för andra. Om en obehörig kommer över ditt lösenord och får tillgång till ditt användar-ID, kan den personen utföra aktiviteter i ditt namn.

Användar-ID och lösenord används för att skydda information som kan vara känslig och det är därför viktigt att följa nedanstående regler för skapande och hantering av lösenord.

Ett lösenord ska vara så kallat starkt, det vill säga svårt att gissa för någon annan. Det ska därför inte kunna förknippas med dig som person och dessutom ha en viss längd och komplexitet.

Regler för utformning av lösenord	
1.6.1.1	Lösenordet måste vara minst **8 tecken** långt. Det får inte vara något av dina tidigare 24 använda lösenord för IT-användarkonto.

Tips på bra lösenord som är enkla att minnas är att tänka ut en mening. Variera sedan mellan stora och små bokstäver och bilda lösenordet. Exempel:

Mening: ”Klockan 10 går två bilar till Norrköping"

Lösenord: K10g2btN

Användar-ID och lösenord är i sig viktig information där användar-ID är information medan lösenord är konfidentiell information och ska hanteras på ett säkert sätt:

Regler för hantering av lösenord	
1.6.1.2	Lösenord ska inte vara synliga. Lösenordet ska hanteras som en värdehandling och inte ligga framme uppskriven på en lapp. Bäst är att förvara lösenord endast i minnet.
1.6.1.3	Olika lösenord ska användas. Samma lösenord ska inte användas privat

	och i jobbet. Olika lösenord ska dessutom användas för olika tjänster på webben även om de är jobbrelaterade. På så vis minskar riskerna att någon kommer åt information.
1.6.1.4	Lösenord ska bytas regelbundet. Byte av lösenord ska ske var 180e dag.
1.6.1.5	Lösenord får inte delas. Lösenord är personliga och ska inte delas mellan kollegor. I de fall en dator delas av flera, ska ändå personliga inloggningar göras. Detta är viktigt för spårbarheten och för att kunna veta vem som har gjort vad i systemen.
1.6.1.6	Automatisk minnesfunktion för lösenordet ska inte användas. Om man loggar in på webbsidor så ska man inte låta webbläsare spara lösenordet. Alternativet ”Nej” ska väljas om man får en sådan fråga. Detta är särskilt viktigt då en dator delas av flera. Webbläsare har funktioner för att i efterhand ta bort webbhistorik/ta bort lösenord vilken kan användas om man är osäker på om lösenord har lagrats.

1.6.2 Mobila enheter

Den IT-utrustning som tillhandahålls av kommunen kan vara stationär eller bärbar, en så kallad mobil enhet. Mobil enhet avser bärbar dator (laptop), USB-minne, CD/DVD-skiva, extern hårddisk samt smart telefon och surfplatta.

Regler för hantering av mobila enheter	
1.6.2.1	Mobila enheter som tillhandahålls av Kungsbacka kommun är personliga arbetsredskap som inte får lånas ut eller överlåtas om det inte är enheter som delas av flera.
1.6.2.2	Förinställda säkerhetsinställningar i enheter får inte ändras.
1.6.2.3	Endast godkända programvara får installeras på enheterna. Programvara upplagda i Software Center är godkända.
1.6.2.4	Installerad programvara får inte kopieras eller installeras på annan enhet.
1.6.2.5	Mobila enheter ska låsas med lösenord eller biometrisk autentisering, till exempel fingeravtryck.
1.6.2.6	Konfidentiell information måste vara krypterad på mobila enheter. Mobila enheter med operativsystemet iOS (iPhone och iPad) är krypterade som standard och du som användare behöver inte göra något. På en Android-enhet med Android 4.1 eller senare som inte är krypterad som standard ska du välja att kryptera data. På de flesta Android-enheter trycker du på Inställningar › Säkerhet › Kryptera telefonen.
1.6.2.7	Viktig information bör inte lagras enbart på en bärbar enhet, i så fall ska den snarast kopieras över till OneDrive eller SharePoint så att informationen säkerhetskopieras.
1.6.2.8	Endast av kommunen godkända enheter och programvara får anslutas till kommunens nät. Godkänd utrustning är enheter inköpta via e-

	handel, och eventuellt andra enheter efter samråd med Digitalt center. För programvara se 1.8.2.3
1.6.2.9	Privat utrustning kan anslutas till kommunens gästnätverk
1.6.2.10	Mobila enheter får enbart anslutas till trådlösa nätverk som är kända och lösenordskyddade.
1.6.2.11	Vid distansarbete måste godkänd säker utrustning användas. Godkänd utrustning är enheter inköpta via e-handel, och eventuellt andra enheter efter samråd med Digitalt center.
1.6.2.12	Vid distansarbete ska åtkomst till information ske över en säker förbindelse, exempelvis VPN.

Regler för fysisk hantering av mobila enheter	
1.6.2.13	Försiktighet ska iakttas vid arbete i kontorslandskap och aktivitetsbaserad arbetsyta så att obehöriga inte kan ta del av konfidentiell information via dator- eller telefonskärm.
1.6.2.14	Arbete med konfidentiell information får inte ske i publika miljöer, exempelvis på ett kafé, på tåget, mm.
1.6.2.15	Mobila enheter ska alltid låsas innan de lämnas utan uppsikt.
1.6.2.16	Förlust av enhet ska omedelbart anmälas till Service Direkt. Detta ska göras innan polisanmälan. I vissa fall finns möjligheter att fjärradera information.
1.6.2.17	Vid avslut av anställning eller vid byte till en annan enhet ska mobila enheter återlämnas i enlighet med de rutiner som finns, och får inte behållas privat.

Särskilda regler för smarta telefoner, bärbara datorer och surfplattor

Förutom de regler som gäller allmänt för mobila enheter gäller även följande vid användning av smarta telefoner och surfplattor.

Kungsbacka kommun är som arbetsgivare generellt sett ägare till de smarta telefoner, bärbara datorer och surfplattor som används i tjänsten, och även till den information som finns i dessa. Man bör därför som medarbetare vara medveten om att arbetsgivaren har rätt att ta del av exempelvis sms, foton och kalenderanteckningar om det är nödvändigt för att uppfylla myndighetens skyldigheter om allmänna handlingars offentlighet. Arbetsgivaren kan även komma att ta del av denna information om det är nödvändigt utifrån ett informationssäkerhetsperspektiv, till exempel vid virus- och hackerangrepp, eller för att utreda och förhindra brott. Detta gäller självklart även stationär dator.

Regler för hantering av smarta telefoner, bärbara datorer och surfplattor	
1.6.2.18	I syfte att minska risken för skadlig kod är det endast tillåtet att ladda ned appar från Kungsbacka kommuns interna appkatalog, App Store eller Google Play.
1.6.2.19	Pinkoder, fingeravtryck eller annan autentisering måste användas till smarta telefoner och surfplattor. Då pinkoder används ska ej enkla pinkoder som 0000, 1234 etc. användas och inte samma pinkod som

	används i andra sammanhang, till exempel pinkod till bankomatkort.

1.6.3 Skadlig kod

Skadlig kod är ett samlingsbegrepp för oönskade datorprogram som virus, trojaner, spionprogram och maskar. Dessa kan installeras på alla enheter eller i ett nätverk, ganska obemärkt för den vanlige användaren. Den har utvecklats i syfte att störa IT-system, för att samla in information eller för att utnyttja datorkraft eller minneskapacitet i IT-utrustning.

Skadlig kod är ett växande problem och den blir mer och mer sofistikerad och ”intelligent”.

Exempel på idag förekommande skadlig kod:

- Vissa trojaner, keyloggers, kan avlyssna lösenord och skicka dessa vidare
- Det finns trojaner som skapar bakdörrar i datorer så att andra personer får tillgång till dessa utan ägarens vetskap, exempelvis med syfte att lagra olaglig information
- Ett ökande problem är Ransomware, en skadlig kod som krypterar dina filer. När krypteringen skett får man sedan erbjudande att betala till de kriminella för att de ska låsa upp filerna

Spridning av skadlig kod

Skadlig kod kan spridas till din dator eller mobila enhet om du öppnar bilagor i e-post, importerar filer eller surfar på internet och klickar på fel länkar, inklusive sådana som finns i sociala medier.

Avsändare till e-post kan vara falska och webbsidor är inte alltid de som de utger sig för att vara. Identiteter kan kapas. Vid så kallad phishing (nätfiske) luras mottagaren att klicka på en länk som leder till en sida där man ombeds fylla i koder, lösenord eller bankkonton. Var observant på detta och fyll aldrig i sådana uppgifter! Seriösa myndigheter, företag och andra organisationer ber aldrig om uppgifter på detta sätt.

IT-utrustning som drabbats av skadlig kod, även ett smittat USB-minne, kan om det kopplas upp i kommunens nätverk, sprida sig vidare i nätverket och orsaka stor skada.

Kommunens datorer är utrustade med skydd mot skadlig kod. Det innebär inte fullständig säkerhet då utvecklingen inom detta område är oerhört snabb. Alla medarbetare och förtroendevalda kan också bidra till ett bra skydd mot skadlig kod genom att följa dessa regler:

Regler för skydd mot skadlig kod	
1.6.3.1	Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod.
1.6.3.2	Anslut endast godkänd IT-utrustning till kommunens nätverk. Godkänd utrustning är enheter inköpta via e-handel, och eventuellt annan utrustning efter samråd med Digitalt center. Privat utrustning får enbart anslutas till kommunens gästnätverk, se 1.8.2.9
1.6.3.3	Var misstänksam och undvik att klicka på konstiga länkar eller fylla i irrelevanta uppgifter.
1.6.3.4	Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga är förväntad.
1.6.3.5	Var observant på om IT-utrustning beter sig långsamt eller konstigt. Vid misstanke om skadlig kod kontakta Service Direkt.

1.6.4 Internet och sociala medier

Användning av Internet och sociala medier kan vara till stor nytta, privat såväl som på arbetet. Internet för dig som medarbetare i Kungsbacka kommun ska främst användas som ett arbetsverktyg och inte störa ordinarie arbetsuppgifter eller innebära merkostnader eller risker för informationssäkerheten i Kungsbacka kommun.

De regler som gäller i samhället i övrigt gäller självklart även inom Kungsbacka kommun. Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt dataskyddsförordningen (GDPR) är exempel på lagar som ibland måste beaktas när du som medarbetare använder Internet.

Förutom de regler som är kopplade till skadlig kod i avsnitt 1.8.3, finns här särskilda regler för användning av internet och sociala medier.

Regler för internetanvändning	
1.6.4.1	För material på internet som ska användas i tjänsten, får nedladdning och installation av upphovsrättsligt material (datorprogram, film, musik med mera) inte ske utan stöd i lag, avtal eller med skriftligt tillstånd från rättighetsinnehavaren.
1.6.4.2	I begränsad omfattning får internet användas för privata syften.
1.6.4.3	Utrymmeskrävande filtyper inklusive filmer, program och spel får inte för privat bruk laddas ned, strömmas, lagras eller spridas i eller via kommunens nätverk.
1.6.4.4	Internet är ett öppet nätverk och ingen information som omfattas av sekretess, personuppgifter eller känsliga personuppgifter får publiceras där utan stöd i lag.

1.6.5 E-post

E-post är för många medarbetare det vanligaste och viktigaste sättet att kommunicera både internt och externt.

Som medarbetare kan det vara svårt att veta vilken information som är ok att skicka med e-post. Innan du skickar information med e-post ställ dig själv frågan vilken sorts information det rör sig om och vem mottagaren är; innehåller materialet konfidentiell information såsom känsliga personuppgifter eller information som omfattas av sekretess, eller är informationen helt öppen? Ditt svar avgör hur du ska hantera informationen.

Du kan läsa mer om hantering av personuppgifter och information som omfattas av sekretess i e-post i ***Regler för hantering av information i Kungsbacka kommuns digitala samarbetsplattform och Office 365***

https://kungsbackakommun.sharepoint.com/sites/verksamhetsstyrning/ODMPublished/1263/Regler%20for%20hantering%20av%20information%20i%20Kungsbacka%20kommuns%20digitala%20samarbetsplattform%20och%20Office%20365.pdf

I övrigt gäller följande regler för e-post:

Ansvar	
1.6.5.1	Den enskilde medarbetaren som är kontoinnehavare för ett personligt e-postkonto är alltid ansvarig för den e-post som skickas från kontot.
1.6.5.2	E-postkonton som delas av flera, till exempel myndighetsbrevlådor och funktionsbrevlådor, ska ha utsedda ansvariga.

Privat e-post	
1.6.5.3	Håll isär arbetsrelaterad och privat kommunikation när du kommunicerar via e-post. Använd inte heller ditt e-postkonto i Kungsbacka kommun för privata ändamål, t. ex för att öppna ett konto på Facebook eller Instagram.
1.6.5.4	Det är inte tillåtet att automatiskt vidarebefordra e-post som innehåller konfidentiell information till externa e-postadresser eller att vidarebefordra e-post som innehåller konfidentiell information till din private e-postadress.

1.6.6 Lagring och säkerhetskopiering

Det är viktigt att information lagras på ett säkert sätt och säkerhetskopieras så att den kan återskapas i händelse av exempelvis diskkrasch eller oavsiktlig radering.

Regler för lagring	
1.6.6.1	Information ska lagras på nätverket så att den säkerhetskopieras. Det kan göras till den personliga lagringsytan OneDrive eller till den gemensamma lagringsytan SharePoint (samarbetsrum).
1.6.6.2	Om information i undantagsfall behöver lagras på lokal hårddisk, se till att regelbundet kopiera över informationen till nätverket.

1.6.6.3	Om information har gått förlorad, exempelvis om man av misstag råkat radera ett dokument, är det i OneDrive och SharePoint (samarbetsrum) möjligt att inom 30 dagar återställa informationen från papperskorgen på egen hand. I övriga fall ska Service Direkt kontaktas för att försöka återskapa den senaste säkerhetskopian.
1.6.6.4	Konfidentiell information såsom känsliga personuppgifter och information som omfattas av sekretess ska i första hand lagras i avsedda och godkända verksamhetssystem och lagringsytor som har begränsad åtkomst, både vad gäller användare och administratörer av systemet eller lagringsytan.
1.6.6.5	Lokal lagring av konfidentiell information, t.ex. på en persondator, får endast ske om lagringsenheten eller filerna är skyddade med godkänd metod för kryptering. Om du är osäker på om din enhet är krypterad kontakta Service Direkt.
1.6.6.6	I de fall information behöver föras över till ett USB-minne så ska USB-minnet krypteras. Som medarbetare kan du själv kryptera USB-minnet enligt nedan, alternativt kontakta Service Direkt. Hur du som användare krypterar ditt USB minne: 1. Sätt i USB-minnet i datorn. 2. Högerklicka på USB-minnet och välj ”Turn Bitlocker on” 3. Välj lösenord eller smartcard som authenticering 4. Spara din ”recovery key” förslagsvis i din Onedrive eller skriv ut den. 5. Klicka Next. 6. Klicka Next 7. Klicka Start encrypting Klar
1.6.6.7	Fysiska dokument som innehåller konfidentiell information ska förvaras inlåsta i utrymmen där enbart behöriga medarbetare har tillgång till informationen.

1.6.7 Lagring i molntjänster

Det finns idag flera molntjänster som vi använder dagligen, inte minst för att dela filer och lagra information. Molntjänster är sådana tjänster som nås via nätverk, till exempel Internet och som ger möjlighet till resursdelning, snabb skalbarhet och självbetjäning.

För medarbetare i en offentlig myndighet gäller det att tänka på vilken information som kommuniceras till och från molntjänsten och hur den behandlas där. Detta är särskilt viktigt för information med särskilda hanteringsregler, såsom känsliga personuppgifter och information som omfattas av sekretess.

För lagring i Office 365 molntjänst se regeldokumentet ***Regler för hantering av information i Kungsbacka kommuns digitala samarbetsplattform och Office 365***
https://kungsbackakommun.sharepoint.com/sites/verksamhetsstyrning/ODMPublished/1263/Regler%20for%20hantering%20av%20information%20i%20Kungsbacka%20kommuns%20digitala%20samarbetsplattform%20och%20Office%20365.pdf

För övriga molntjänster gäller följande:

Regler för lagring i molntjänster	
1.6.7.1	Endast molntjänster som lever upp till Kungsbacka kommuns krav på säkerhet för att skydda aktuell information får användas för lagring. Kontakta kommunens specialist informationssäkerhet för en bedömning av informationstillgången och molntjänsten innan du börjar lagra information i en molntjänst.
1.6.7.2	Konfidentiell information får i normalfall inte lagras i molntjänster. Kontakta kommunens specialist informationssäkerhet för en bedömning av om en molntjänst i undantagsfall kan användas för lagring av en konfidentiell informationsmängd.

1.6.8 Spårning och loggning

Loggning sker i kommunens datorer och nätverk. Loggarna används för felsökning och för utredning av incidenter eller för skydd av vår information ur ett IT- och informationssäkerhetsperspektiv. Loggarna lagras under en viss tid och är åtkomliga endast för en begränsad grupp administratörer.

Spårbarhet innebär att man genom loggning kan identifiera vem som har gjort vad och när samt följa förloppet för olika händelser på datorn.

All internettrafik, e-post och Skype loggas centralt. Kungsbacka kommun har som arbetsgivare rätt att gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning och regelverk. Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättskipande myndighet utan att du som kontoinnehavare meddelas. Loggarna är även allmän, och oftast offentlig, handling enligt Tryckfrihetsförordningen. Loggarna kan därför komma att lämnas ut till enskilda eller massmedia om de begär att få ta del av dem.

1.6.9 Säkert beteende

En stor del av kommunens information hanteras muntligt, på fysiskt papper och på dataskärmen. Vi kommunicerar dagligen informellt och formellt på detta sätt och vi måste vara särskilt försiktiga då vi hanterar känslig information. Tänk på att det alltid finns informell information som inte i förhand är definierad, utan som skapas i det ögonblick det uttalas eller skrivs. Det kan till exempel vara information om en oförutsedd händelse, till exempel ett brott. Sådan information kan vara känslig eller till och med belagd med sekretess.

Regler för muntlig information	
1.6.9.1	Konfidentiell information ska hållas inom en begränsad krets av behöriga. Detta måste beaktas så att inte obehöriga kan höra sådan information på arbetsplatsen, både i arbetssituationer men även i informella sammanhang som till exempel vid fikabordet. Man ska enbart tala i stängda utrymmen och även försäkra sig om att fysiska samtal eller telefonsamtal inte hörs i intilliggande rum.
1.6.9.2	Konfidentiell information får överhuvudtaget inte kommuniceras muntligt i publika miljöer.

Regler för information på skärmar och i pappersform	
1.6.9.3	Skriftligt material som innehåller konfidentiell information får inte ligga framme så att obehöriga kan läsa den. Materialet ska låsas in i godkända skåp när man lämnar arbetsplatsen och även för kortare stunder.
1.6.9.4	Konfidentiell information på datorskärmen ska vara skyddad från obehöriga. Datorn ska låsas när man lämnar den, även för kortare stunder.
1.6.9.5	Besökare får inte vistas utan uppsikt i lokaler där konfidentiell information kan finnas. Mottagare av besök ansvarar för besökare så länge de befinner sig i kommunens lokaler. Obekanta personer i sådana lokaler ska tillfrågas vem de söker och hjälpas tillrätta.
1.6.9.6	Vid försändelse av intern fysisk post ska förslutna kuvert användas. För fysisk post som skickas externt ska i första hand rekommenderade försändelser användas om brevet innehåller konfidentiell information såsom känsliga personuppgifter och information som omfattas av sekretess.
1.6.9.7	Då konfidentiell information överförs via fax ska man försäkra sig om att man har rätt nummer (till exempel använda sig av kortnummer) och att mottagarens fax är övervakad under överföringstillfället. Man ska inte lämna faxen innan överföringen är klar.
1.6.9.8	Vid utskrift ska dokument omgående hämtas upp ur skrivare. Vid utskrift av konfidentiell information ska utskriften övervakas så att man är säker på att ingen obehörig kan läsa informationen.
1.6.9.9	Pappersdokument som innehåller känslig eller sekretessbelagd information måste vid kassering strimlas eller kastas i godkända säkerhetskärl.

Beslutad av: Biträdande kommundirektör, 2019-11-06 KS/2019:637

Gäller från: 2019-11-15

Ansvarig förvaltning: Kommunstyrelsen

Kontakt: Kungsbacka direkt 0300-83 40 00, info@kungsbacka.se

Kungsbacka kommun, 434 81 Kungsbacka
kungsbacka.se