Kumla kommun

Riktlinjer för Användare

Informationssäkerhet Kumla kommun

Beslutande	Kommunstyrelsen
Datum och paragraf	Klicka här för att välja datum., § 999
Dokumentansvarig	Informationssäkerhetssamordnare
Revideras	Vid behov
Gäller till	2025-04-01

Innehåll

Inledning **4**

Medarbetares ansvar för informationssäkerhet 4

Informationsklasser 5

Personuppgifter 6

Allmänna handlingar och sekretess 7

1. Lösenord **8**

2. Mobila enheter och utanför arbetsplatsen **9**

Särskilda regler för smarta telefoner och surfplattor 12

3. Skadlig kod och Granska avsändaren **12**

Spridning av skadlig kod 13

Granska avsändaren 13

4. Internet och sociala medier **14**

5. E-post **15**

Övrig hantering av e-post 17

6. Lagring, säkerhetskopiering och molntjänster **17**

7. Spårbarhet och loggning **18**

8. Säkert beteende och När det blir fel **18**

Skyldighet att rapportera incidenter och brister 19

Inledning

Detta kapitel vänder sig till alla medarbetare vid Kumla kommun. Riktlinjerna gäller även extern personal som har åtkomst till Kumla kommuns information, exempelvis inhyrda konsulter.

Riktlinjerna beskriver det ansvar man som medarbetare har vid hantering av information i Kumla kommun och vilka regler som gäller.

Kumla kommun är en stor organisation med många skilda verksamheter. Kompletterande regler och rutiner till riktlinjerna kan därför finnas lokalt. Avvikelser från dessa riktlinjer får dock aldrig göras utan särskilt tillstånd. Kontakta ansvarig chef vid osäkerhet om vad som gäller.

Riktlinjerna följer i stort en struktur framtagen av Myndigheten för samhällsskydd och beredskap (MSB) som återfinns i en utbildning för informationssäkerhet framtagen av myndigheten – DISA (Datorstödd informationssäkerhetsutbildning för användare)

Syftet är att man kan genomgå DISA-utbildningen och parallellt se vilka riktlinjer som gäller i Kumla kommun. DISA består av 10 avsnitt om informationssäkerhet, och alla avsnitt utgörs av en film med tillhörande information och frågor. Dessa riktlinjer består dock endast av avsnitt, eftersom information och regler gällande säkerhetskopiering och molntjänster slagits samman till ett avsnitt samt att avsnitten Säkert Beteende och När det blir fel också har slagits samman.

Före områdena utifrån strukturen från DISA inleds riktlinjen med övergripande information om medarbetares ansvar för informationssäkerhet, informationsklasser, personuppgifter samt allmänna handlingar och sekretess.

Medarbetares ansvar för informationssäkerhet

Information är en viktig resurs för Kumla kommun och är av stor betydelse för alla våra verksamheter. I kommunen hanterar vi varje dag mängder av information som handlar om allt vad vi gör, och rör till exempel förskolor, socialtjänst, stadsplanering och fritidsverksamhet. Information kan förekomma i olika former, den kan vara muntlig, skriftlig eller finnas i IT-system. Information är främst i form av text, men även bilder, symboler, filmer och ljud utgör information.

Viss information är känslig och måste skyddas från obehöriga att ta del av. Det handlar ofta om hänsyn till den personliga integriteten och för att undvika att enskilda individer kommer till skada. Det finns en hel del lagar och föreskrifter som ställer krav på hur kommunen hanterar information. Utöver det så har medborgare, företag, föreningar m.fl. förväntningar och behov på att kommunen hanterar information på ett säkert sätt. Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för att motsvara dessa krav.

Information behöver olika slag av skydd. Det kan vara tekniskt såsom en brandvägg i ett IT-nätverk, administrativt i form av regler (som dessa riktlinjer) eller fysiskt hur man skyddar utrymmen med dörrar, lås, skåp med mera. Medarbetares kunskap och medvetenhet är ett nog så viktigt skydd, till exempel att arbeta på rätt sätt med pappersdokument och i IT-system och att vara försiktig med känslig information, exempelvis känsliga personuppgifter. 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 Kumla kommuns informationssäkerhet beror därför på hur den enskilde medarbetaren hanterar informationen.

Kumla kommun ställer krav på att medarbetare följer dessa riktlinjer för informationssäkerhet. Chefer har ett ansvar att delge information och utbildning i informationssäkerhetsfrågor till sina medarbetare.

Om du som medarbetare eller inhyrd konsult har tillgång till känslig information ska du skriva under en tystnads- och sekretessförbindelse. En sådan förbindelse gäller även efter att anställningen eller avtalet upphört. Underlåtenhet att följa dessa riktlinjer kan innebära lagbrott och sådana kommer att polisanmälas.

Informationsklasser
Viss information är känsligare 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.
I Kumla kommun finns tre klasser för hur känslig informationen är och hur den får spridas:

Öppen, Intern eller Konfidentiell. Dessa illustreras nedan.

Kravnivå		Konfidentialitet
2	Höga skyddskrav (Konfidentiell)	Konfidentiell information som, om den sprids till obehöriga, kan medföra allvarliga konsekvenser för Kumla kommun, externa aktörer eller individer.
1	Normala skyddskrav (Intern)	Intern information som, om den sprids till obehöriga, kan medföra måttliga negativ påverkan på Kumla kommun, externa aktörer eller individer
0	Inga skyddskrav (Publik)	Öppen information som kan spridas fritt inom och utom Kumla kommun

Olika regler gäller för dessa tre klasser vad gäller spridning och hantering av information:

- *Publik* information har inga krav på åtkomstbegränsning utan kan spridas fritt. Ibland krävs dock beslut för att öppen information ska publiceras, till exempel på www.kumla.se
- För *Intern* information gäller de normala hanteringsregler som finns nedan i avsnitt A1 – A8. Intern information kan normalt spridas internt inom kommunen. Om intern information sprids till extern aktör ska det finnas ett tydligt syfte med detta.
- Särskilda hanteringsregler gäller för **konfidentiell** information. I detta kapitel är all information och alla riktlinjer som gäller för **konfidentiell** information markerad med fetstil och med dubbla ramar i tabeller med riktlinjer.

Inom Kumla kommun är idag långt ifrån all information klassad enligt de tre klasserna. Att klassa information på det här sättet är ett arbete som nyligen påbörjats. Det viktigaste är att **konfidentiell** information hanteras på rätt sätt. **Konfidentiell** information är bl.a. känsliga personuppgifter och sekretessklassad information. Om du är osäker på hur viss information ska klassas och hanteras så fråga din chef.

Personuppgifter

I de flesta av Kumla kommuns verksamheter hanteras personuppgifter. Dessa måste behandlas enligt gällande författningar som dataskyddsförordningen (GDPR) och patientdatalagen. Personuppgifter kan vara klassade som **konfidentiell**, intern eller öppen information. Det beror på sammanhang, vilka personuppgifter som avses osv. Känsliga personuppgifter bör dock som huvudregel alltid klassas som **konfidentiell** information. Till känsliga personuppgifter räknas enligt dataskyddsförordningen följande uppgifter:

- Ras/etniskt ursprung
- Politiska åsikter
- Religiös/filosofisk övertygelse
- Medlemskap i fackförening
- Genetiska uppgifter
- Biometriska uppgifter
- Uppgifter om hälsa
- Uppgifter om sexualliv/sexuella läggning

Förutom känsliga personuppgifter finns det integritetskänsliga personuppgifter, som också bör vara konfidentiell information som huvudregel. Följande är integritetskänsliga personuppgifter.

- Personnummer
- Uppgifter om lagöverträdelser
- Löneuppgifter
- Värderande uppgifter
- Uppgifter om sociala förhållanden

Skyddade personuppgifter är alltid **konfidentiell** information och ska hanteras utifrån särskilda rutiner och regler.

Allmänna handlingar och sekretess

En handling är allmän om den är förvarad, inkommen till, eller upprättad hos kommunen. Allmänna handlingar kan både vara analog och digital information och ska hanteras, bevaras och gallras i enlighet med dokumenthanteringsplanerna.

Information som är allmän handling kan vara sekretessbelagd enligt offentlighets- och sekretesslagen eller annan lagstiftning. Sådana handlingar bör klassas som **konfidentiell** information.

Mer information och regler kring allmänna handlingar finns i Ärendehandboken.

1. Lösenord

För att logga in till de flesta av Kumla kommuns 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.

Via Kumla kommuns lösenordsportal kan du få ett nytt lösenord om du har glömt ditt lösenord.

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

Ett lösenord ska vara ”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. Krav på lösenord:

Riktlinjer för utformning av lösenord	
1.1	Lösenord ska vara minst 12 tecken långt, gärna längre.
1.2	Lösenord ska inte vara ”vanliga” lösenord så som password1234
1.3	Lösenord ska inte bestå av ett enda ord, exempelvis kommunikation eller epidemiologi
1.4	Lösenord ska inte gå att koppla till dig eller den aktuella tjänsten, exempelvis användar-ID eller namnet på den aktuella tjänsten
1.5	Lösenord ska inte bestå av repetitiva eller följder av tecken, exempelvis aaaaaaaaaaaa eller abcdefghijklm

Tips på bra lösenord som är enkla att minnas är att kombinera flera slumpmässigt valda ord. Exempelvis korrekt, häst, batteri och klammer.
Lösenord: korrekthästbatteriklammer
Ett annat tips är att använda begynnelsebokstaven i varje ord i en mening. T.ex. JagBoddeILondon1978, med det lösenordet kan minnesanteckningen lyda JBIL1978.

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

Riktlinjer för hantering av lösenord	
1.6	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.
1.7	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 minskas riskerna att någon kommer åt information.
1.8	Lösenord får inte delas. Lösenord är personliga och ska inte delas mellan kollegor. Man kan i så fall bli ansvarig för något som någon annan har gjort. I de fall en dator delas av flera, ska ändå personliga inloggningar göras. Detta är viktigt för spårbarheten, för att kunna veta vem som har gjort vad i systemen.
1.9	Automatisk minnesfunktion för lösenordet ska inte användas. Om man loggar in på webbsidor så ska man inte låta webbläsare spara lösenordet, utan alternativet ”Nej” ska väljas om man får en sådan fråga. Detta är särskilt viktigt då en dator delas av flera.

2. Mobila enheter och utanför arbetsplatsen

Den IT-utrustning som tillhandahålls av Kumla kommun kan vara stationär eller bärbar, en s.k. mobil enhet. Mobil enhet avser både bärbar dator (laptop), smart telefon eller surfplatta, men även USB-minne eller annan lagringsenhet.

Applikationsspecifika enheter kan ha specifika riktlinjer utöver de som presenteras här. Kolla med din chef om du är osäker vad som gäller.

Riktlinjer för hantering av mobila enheter	
2.1	Mobila enheter som tillhandahålls av Kumla kommun är personliga arbetsredskap och får inte lånas eller överlåtas om det inte är enheter som delas av flera.
2.2	Uppsatta säkerhetsinställningar i enheter får inte ändras.
2.3	Endast godkända programvaror får installeras på enheten.

2.4	Installerad programvara får inte kopieras eller installeras på annan enhet.
2.5	Mobila enheter ska låsas med lösenord.
2.6	**Konfidentiell** information måste vara krypterad på mobila enheter.
2.7	Viktig information bör inte lagras enbart på en bärbar enhet, i så fall ska den snarast kopieras över till kommunens nätverk så att informationen säkerhetskopieras.
2.8	Endast av kommunen godkänd enhet och programvara får anslutas till kommunens nät.
A2.9	Privat utrustning kan anslutas till kommunens gästnät. Vissa verksamheter har dessutom ett trådlöst nätverk för privata enheter som datorer, smarta telefoner och surfplattor (s k Bring Your Own Device – BYOD). En särskild instruktion finns för detta: Instruktion: Trådlöst nätverk för privata enheter –
2.10	Enheten får enbart anslutas till trådlösa nätverk som är kända och lösenordskyddade.
2.11	Vid distansarbete måste godkänd säker utrustning och VPN-anslutning användas.
2.12	Anslutning med kommunens VPN-anslutning är inte tillåtet med en dator som används privat.

Riktlinjer för fysisk hantering av mobila enheter	
2.13	Försiktighet ska iakttas vid arbete i publika miljöer, exempelvis kan skärmen skyddas med sekretesskydd.
2.14	Arbete med **konfidentiell** information får inte ske i publika miljöer.
2.15	Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme.
2.16	Förlust av enhet ska omedelbart anmälas till IT-avdelningen. I vissa fall finns möjligheter att fjärradera information.
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 eller av en verksamhet.

2.18	Utrustningen ska i övrigt vårdas och hanteras på det sätt som föreskrivs, till exempel skyddas mot värme och fukt.

Särskilda regler för smarta telefoner och surfplattor

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

Regler för smarta telefoner och surfplattor	
2.19	Kumla kommun är som arbetsgivare ägare till de smarta telefoner 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 till exempel sms, foton och kalenderanteckningar. Eftersom offentlighetsprincipen gäller kan det vara möjligt för utomstående att begära ut informationen.
2.20	Det finns ett stort utbud av appar att ladda ner till den smarta telefonen eller surfplattan. Många av dessa appar kan innehålla skadlig kod. I syfte att minska denna risk är det endast tillåtet att ladda ned appar som godkänts av Kumla kommun.
2.21	Information som är **konfidentiell** får inte hanteras i smart telefon eller surfplatta om inte särskild av kommunen godkänd säkerhetslösning används.
2.22	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, t.ex. pinkod till bankomatkort.
2.23	Vårda utrustningen väl och använd förslagsvis skärmskydd och skal.

3. Skadlig kod och Granska avsändaren

Skadlig kod är ett samlingsbegrepp för oönskade datorprogram som virus, trojaner, spionprogram och maskar. Dessa kan installeras på en dator eller ett nätverk utan administratörens samtycke, och 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” och kan vara svår att upptäcka och kan utföra avancerade operationer. Man behöver idag inte vara en tekniskt kunnig hacker för att skapa skadlig kod, utan det mesta kan köpas och beställas på olika marknadsplatser på Internet.

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 så kallad Ransomware där filer eller diskar på dator (eller smart mobil eller surfplatta) krypteras och man sedan krävs på en lösensumma.

Spridning av skadlig kod

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

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. Detta innebär inte fullständig säkerhet då utvecklingen inom detta område är oerhört snabb. Alla medarbetare kan också bidra till ett bra skydd mot skadlig kod genom att följa dessa regler.

Granska avsändaren

Ett viktigt verktyg i att skydda kommunen mot både skadlig kod och försök att komma åt lösenord och bankuppgifter, så kallad Phishing, är att granska avsändaren.

Avsändarnamn för e-post kan enkelt fejkas så det gäller att granska avsändaradressen. Avsändaradressen är den e-postadress som skickat meddelandet.

Angripare försöker även lura oss genom att använda en avsändaradress som är väldigt lik en ”riktig” avsändare. Exempel på det är att byta ut bokstaven l mot siffran 1, exempelvis fornamn.efternamn@kum1a.se. Om man inte är uppmärksam så är det lätt att missa att adressen inte är den vanliga kumla-adressen. Det gäller även adresser till webbplatser, så det gäller att granska webbplatsadresser innan du fyller i exempelvis lösenord.

Riktlinjer för skydd mot skadlig kod och liknande	
3.1	Stäng aldrig av eller på annat sätt inaktivera installerat skydd mot skadlig kod.
3.2	Anslut endast godkänd IT-utrustning till kommunens nätverk.
3.3	Var misstänksam och undvik att klicka på konstiga länkar eller fyll i irrelevanta uppgifter.

3.4	Öppna bifogade filer endast om de kommer från en känd avsändare och en bilaga är förväntad.
3.5	Var observant på om IT-utrustning beter sig långsamt eller konstigt. Vid misstanke om skadlig kod, anmäla detta via Serviceportalen.
3.6	Granska alltid avsändaren vid inkommande e-post och webbplatsadresser vid misstanke

4. Internet och sociala medier

Användning av Internet och sociala medier kan vara till stor nytta och glädje, privat såväl som på arbetet. Förutom de riktlinjer som är kopplade till skadlig kod i avsnitt A3 finns här särskilda regler för användning av Internet och sociala medier.

Riktlinjer för Internetanvändning	
4.1	Internet är i arbetet på Kumla kommun främst ett arbetsverktyg och ska inte störa ordinarie arbetsuppgifter eller innebära merkostnader för kommunen.
4.2	De regler som gäller i samhället i övrigt gäller självklart även inom Kumla kommun. Tryckfrihetsförordningen, brottsbalken, lagen om upphovsrätt samt allmänna dataskyddsförordningen är exempel på lagar som ibland måste beaktas när man använder Internet.
4.3	För material på Internet som ska användas i tjänsten, får nedladdning och installation av upphovsrättsligt material (datorprogram, film, musik m.m.) inte ske utan stöd i lag, avtal eller med skriftligt tillstånd från rättighetsinnehavaren.
4.4	I begränsad omfattning får Internet användas för privata syften. Utrymmeskrävande filtyper inklusive filmer, program och spel får dock inte för privat bruk laddas ned, strömmas, lagras eller spridas i, eller via, Kumla kommuns nätverk.
4.5	Internet är ett öppet nätverk och endast öppen information får publiceras eller delas, alltså inte intern eller **konfidentiell** information.

Uttalanden och andra aktiviteter som görs på Internet kan påverka allmänhetens uppfattning om den enskilde tjänstemannen som utför aktiviteten, och även för Kumla kommun som organisation. Det är därför särskilt viktigt att som representant för Kumla kommun beakta god etik och gott omdöme på Internet. Kumla kommuns etiska regler och värderingar ska följas även vid kommunikation via Internet och sociala medier. Tänk därför på att:

Etiska riktlinjer	
4.6	All kommunikation på Internet från Kumla kommuns datorer ska vara öppen, saklig och etisk.
4.7	Det är inte tillåtet att besöka webbplatser med till exempel brottslig verksamhet, rasism, diskriminering, extrempolitiskt eller pornografiskt innehåll.
4.8	Publicera inte något på Internet som är oärligt, osant, vilseledande eller kränkande. Tänk på att det som publiceras är synligt och offentligt för allmänheten, sprids snabbt samt finns kvar under lång tid. Tänk därför igenom innehållet noga innan du publicerar.

Kumla kommun är aktivt på sociala medier. Den personal som skriver i Kumla kommuns namn har särskilda regler och kunskap om kommunikation. Tänk därför på följande:

Riktlinjer vid användning av sociala medier	
4.9	Använd endast ett av Kumla kommuns konton om du ska använda sociala medier i tjänsten.
4.10	Användningen av sociala medier ska följa gällande styrdokument i kommunen. Det gäller till exempel kommunikationspolicy, grafiska profilen och riktlinjer för service och bemötande.

5. E-post

E-post är för många medarbetare det vanligaste och viktigaste sättet att kommunicera internt inom kommunen och till externa parter. Det är dock viktigt att tänka på att kommunikation med e-post normalt är helt öppen. Att sända e-post som inte är skyddad, t.ex. med kryptering, kan jämföras med att skicka vykort.

Ansvar	
5.1	Den enskilde medarbetaren som är kontoinnehavare för ett personligt e-postkonto är alltid ansvarig för den e-post som skickas från kontot.
5.2	Medarbetare är ansvarig för att löpande öppna och läsa inkommande e-post. Vid frånvaro, t.ex. sjukfrånvaro, semester eller annan ledighet, ska autosvar användas, och om nödvändigt, behörighet ges till kollega eller chef att öppna och läsa inkommande e-post. Vid avslut av anställning tas e-posten bort.
5.3	E-postkonton som delas av flera, t.ex. myndighetsbrevlådor (för nämnder) och funktionsbrevlådor (t.ex. för enheter) ska ha utpekade ansvariga.

Allmänna handlingar	
5.4	E-post som skickas till personliga brevlådor är som huvudregel allmän handling. Vid arbetsrelaterad e-post ska alltid regler för registrering och hantering av allmänna handlingar följas.
5.5	E-post som är allmän handling får gallras, dvs. raderas, först när e-posten diarieförts eller hålls ordnat på annat sätt. Vissa epostmeddelanden som är allmänna handlingar är av uppenbar ringa eller tillfällig betydelse och är undantagna från kravet på registrering. Dessa får gallras direkt.

Privat e-post	
5.6	Håll isär arbetsrelaterad och privat kommunikation när du kommunicerar via e-post. Använd inte ditt epostkonto i Kumla kommun för privata ändamål, utan ha en privat e-postadress som du inte använder för arbetsmaterial.
5.7	Det är inte tillåtet att automatiskt vidarebefordra e-post till externa e-postadresser.

E-post och konfidentiell information	
5.8	Öppen och intern information får skickas med e-post, medan **konfidentiell** information endast får skickas med e-post som använder av Kumla kommun godkänd kryptering.

Övrig hantering av e-post

Förutom ovanstående regler så är det bra att tänka på följande vid användning av e-post.

- Rensa inkorgen och töm papperskorgen regelbundet; minst en gång i veckan
- Använd e-posten för att kommunicera, inte för att lagra information
- Överväg alternativa sätt att kommunicera, så som verksamhetssystem eller Teams, OBS Teams används ej för konfidentiell information.

6. Lagring, säkerhetskopiering och molntjänster

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

Riktlinjer för lagring och säkerhetskopiering	
6.1	Information ska lagras på godkänd plats, för att kunna säkerhetskopieras. Det kan vara personliga (exempelvis Q: eller OneDrive) eller gemensamma filareor (exempelvis Teams/Sharepoint eller S:).
6.2	Om information behöver lagras på lokal hårddisk, se till att regelbundet kopiera över informationen till en yta som säkerhetskopieras.
6.3	Om information har gått förlorad, exempelvis om man av misstag råkat radera ett dokument, ska Kommunsupport kontaktas, förhoppningsvis kan de då återskapa den senaste säkerhetskopian.
6.4	**Konfidentiell** information får endast lagras i därför avsedda och godkända system och lagringsytor som har begränsad åtkomst, både vad gäller användare och administratörer av systemet eller lagringsytan.

6.5	Lokal lagring av **konfidentiell** information, t.ex. på en persondator, får endast ske om lagringsenheten eller filerna är krypterade av Kumla kommun godkänd metod för kryptering.
6.6	Fysiska dokument som innehåller **konfidentiell** information ska förvaras inlåsta.

Molntjänster är datortjänster som tillhandahålls över Internet, exempelvis lagring eller programvaror.

Riktlinjer för lagring i molntjänster	
6.7	Endast godkända molntjänster är tillåtna att användas. Kontrollera vilka molntjänster som är tillåtna inom din verksamhet.
6.8	**Konfidentiell** information får inte lagras i personliga molntjänster.

7. Spårbarhet och loggning

Loggning sker i kommunens datorer och nätverk. Loggarna används för felsökning och för utredning av incidenter eller för att förhindra brott. 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 och följa förloppet för olika händelser på datorn.

All Internettrafik och e-post loggas centralt. Kumla kommun har som arbetsgivare rätt att, utan att meddela användaren, gå igenom dessa loggar för att kontrollera efterlevnad av lagstiftning och riktlinjer. Vid misstanke om brott kan loggfilerna komma att lämnas ut till rättskipande myndighet utan att du som kontoinnehavare meddelas.

8. Säkert beteende och När det blir fel

En stor del av kommunens information hanteras muntligt och på papper. Vi kommunicerar dagligen informellt och formellt på detta sätt och vi måste bete oss särskilt försiktigt då vi hanterar **konfidentiell** information. Tänk på att det alltid finns informell information som inte i förhand är definierad och klassad, utan som skapas i det ögonblick det uttalas eller skrivs. Det kan vara t.ex. omdömen om chefer och medarbetare – skvaller, rykten m.m. – eller

information om en oförutsedd händelse, t.ex. ett brott. Sådan information kan vara känslig och är i så fall **konfidentiell** information.

Skyldighet att rapportera incidenter och brister

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

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

IT- och informationsrelaterade incidenter och brister ska rapporteras via e-tjänsten Anmäla personuppgiftsincident. Meddela även din chef. Medarbetare som har upptäckt incidenter eller svagheter där brott misstänks föreligga, ska dock inte själva försöka bevisa sådana då det kan försvåra framtida utredningar.

Riktlinjer för muntlig information	
8.1	**Konfidentiell** information har 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, t.ex. vid fikabordet. Man ska enbart tala i stängda utrymmen och även försäkra sig om att fysiska samtal eller telefonsamtal inte hörs i intilliggande rum.
8.2	Endast öppen information ska kommuniceras hörbart utanför arbetsplatsen, exempelvis vid fysiska samtal på tåget, eller i telefonsamtal i kassakön. **Konfidentiell** information får överhuvudtaget inte kommuniceras muntligt i publika lokaler.

Riktlinjer för information på skärmar och i pappersform	
8.3	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, även för kortare stunder.
8.4	**Konfidentiell** information på datorskärmen ska vara skyddad från obehöriga. Skärmen ska låsas när man lämnar datorn, även för en kortare stund. Om man har ett s k smart kort till datorn ska detta tas ut då man lämnar arbetsplatsen.

8.5	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.
8.6	Om fysisk posttjänst används ska förslutna brev användas för intern information och rekommenderade försändelser ska användas om brev innehåller **konfidentiell** information.
8.7	Då **konfidentiell** information överförs via fax ska man försäkra sig om att man har rätt nummer (t.ex. använda sig av kortnummer) och att mottagarens fax är övervakad under överföringstillfället. Man ska inte lämna faxen innan överföringen är klar.
8.8	Vid utskrift av **konfidentiell** information ska utskriften övervakas så att man är säker på att ingen obehörig kan läsa informationen.
8.9	Pappersdokument som innehåller **konfidentiell** information måste vid kassering strimlas eller kastas i godkända säkerhetskärl.