TIMRÅ KOMMUN
Kommunledningskontoret

Vägledande råd och bestämmelser för Användare av IT-system inom Timrå kommun (Q4 2018)

Du xxx måste känna till:

- vilket ansvar du har som medarbetare i Timrå kommun och de allmänna säkerhetsbestämmelserna för informationssäkerhet
- vad du ska göra vid olika IT-incidenter och var du kan få stöd och hjälp
- hur du får använda kommunens e-post och Internet

Ansvar

- ansvara för informationens riktighet och att den skyddas mot obehörig insyn vid såväl inmatning, uttag som bearbetning av information
- XXX
- rapportera fel och brister gällande IT till servicedesk
- framföra behov av information och utbildning till berörd systemförvaltare
- föreslå utvecklande förändringar av IT-systemen till IT-enheten
- meddela systemförvaltare behovet av skydd för personuppgifter och känslig information
- förstå IT-systemets struktur och rollfördelningen inom Timrå kommun
- förstå begränsningar i och risker, med användande och synk av e-post och internet

Behörighet

Kommunens IT-system är utrustade med behörighetskontrollsystem för att säkerställa att endast behöriga användare kommer åt information. De behörigheter du blir tilldelad beror på dina arbetsuppgifter och bestäms av din närmsta chef.

Lösenord

Lösenordet är personligt och skall hanteras därefter. Du lämnar spår efter dig när du är inloggad och arbetar i IT-systemen. Tänk därför på att du själv kan bli misstänkt om någon använder ditt lösenord för olämpliga ändamål. Du ska därför;

- inte avslöja ditt lösenord för andra eller låna ut dina behörigheter
- inte skriva ned dem på en lapp som förvaras i närheten
- omedelbart byta lösenord om du misstänker att någon känner till det
- byta lösenordet på uppmaning samt med jämna mellanrum
- lösenordet skall bestå av minst 10 tecken med versal, siffra/specialtecken. Skapa gärna lösenordet i form av en mening, ***”Varje dag är en ny dag”***. Det ska konstrueras så att det inte lätt kan kopplas till dig som person

Postadress: 861 82 Timrå
Besöksadress: Köpmangatan 14
Telefon: 060-16 31 00
Bankgiro: 5672-9387
Organisationsnummer: 212000-2395
Fax: 060-16 31 05
Hemsida: www.timra.se
E-post: info@timra.se

Offentlighet och sekretess

Regler om allmänna handlingars offentlighet samt om sekretess återfinns i tryckfrihetsförordningen (1949:105) och i offentlighets- och sekretesslag (SFS 2009:400). Det är viktigt att du är förtrogen med karaktären på de handlingar och uppgifter som du hanterar.

Dataskyddsförordningen, GDPR

Om du behöver upprätta särskilda register eller sammanställningar innehållande personuppgifter, bör du i ett tidigt stadium i planeringen av registret samråda med kommunens GDPR-samordnare som finns hos varje förvaltning.

Klassning av information

En stor mängd handlingar kan vara sekretesskyddade eller vara känsliga uppgifter enligt dataskyddsförordningen. Det är viktigt att du är förtrogen med offentlighetsprincipen då du hanterar handlingar/uppgifter även digitalt. Klassning görs utifrån sekretess, riktighet och tillgänglighet. Kommunen använder systemet Klassa från SKL. Vill du ha hjälp med att klassa din information vänd dig till kommunens informationssäkerhetssamordnare.

Lagring av information

Allt arbetsmaterial skall lagras på säkert ställe. För IT-stödet kan vi övergripande se det som två olika typer av lagringsmöjligheter:

- Information i våra verksamhets-/stödsystem, till exempel ekonomi- och lönesystem. I dessa system är informationen ofta redan ”klassad” och inbyggda regelverk ger rättigheter eller sätter begränsningar för dig att hantera informationen.
- Egna register, dokument och handlingar, exempelvis i Word- eller Excelformat. Det är viktigt att du tänker över säkerheten och hur du klassar, lagrar och hanterar informationen.

När du skapar egen information är det viktigt att känna till var den ska lagras. Den information du lagrar på nätverket säkerhetskopieras. Lagra ingen information på din lokala hårddisk (C:\) XXX eller annan lokal lagringsmedia XXX. Du riskerar att förlora lokalt lagrad information vid eventuella haverier. Du bör därför alltid säkerställa säkerhetskopiering genom att lagra informationen i nätverket. Exempel på dessa är; H: din personliga enhet där endast du har tillträde
O: din förvaltnings enhet
K: kommungemensam enhet. Här ska inga sekretess eller skyddade uppgifter finnas.

TIMRÅ KOMMUN
Kommunledningskontoret

Distansarbete och mobil datoranvändning

Användare kan, efter godkännande av IT-chef/systemägare, ges möjlighet att koppla upp sig mot kommunens nätverk från bostaden eller annan plats. Ett grundkrav är dock att det görs på en dator från IT-enheten med fullgott skydd.

e-post

E-postsystemet ska inte användas som ett arkivsystem. e-post är ett rationellt hjälpmedel i arbetet men minneskapaciteten är begränsad. Tänk därför på att regelbundet radera i mappen ”Inkorg”, bifogade filer m.m. Det du vill spara, sparar du på samma sätt som du lagrar annan information. Loggar på din e- postlåda sparas centralt i 30 dagar. En ny riktlinje är antagen gällande arkivering av e-post. Den arbetas in i respektives förvaltnings dokumenthanteringsplaner.

Var extra uppmärksam då du använder e-post. e-post med bilagor utgör ett stort hot när det gäller spridning av virus. Klicka inte heller på länkar i mail där du inte kan garantera avsändarens riktighet.
I kommunen finns möjlighet att få sin brevlåda synkad till kommunens enheter, ex mobil. Alla kommunens enheter hanteras också i ett säkerhetssystem för att göra denna synkning så säker som det går.

Kom ihåg att:

- e-postsystemet är ett arbetsverktyg och ska endast undantagsvis användas för privat bruk
- din e-post ska innehålla avsändarsignatur enligt kommunens grafiska profil
- du ska inte skicka mail relaterade till din tjänst i kommunen med andra e-post adresser än den du blivit tilldelad av din arbetsgivare (ex gmail, hotmail osv)
- skicka aldrig personuppgifter eller andra känsliga uppgifter med din e-post
- all e-post bör betraktas som om du sänt vykort och ska därför inte innehålla information som du är angelägen om att obehöriga inte ska läsa
- samma regler gäller för diarieföring av e-post som för vanliga brev
- om du misstänker att det kommit in virus via e-postsystemet ska du omgående anmäla detta till servicedesk XXX
- kommunen har ett så kallat spamfilter installerat i vårt nät. Om du trots detta anser att du får stora mängder skräppost anmäl detta till servicedesk.
- sprid inte din e-postadress till mindre seriösa mottagare (risk för spam)
- om du får hotelsebrev eller liknande, kontakta din närmaste chef, ta inte bort brevet
- synkning av e-post får endast ske till kommunens enheter och ska administreras i kommunens säkerhetssystem
- i kommunens e-post finns även en kalender för bokade möten. Den är som standard helt öppen så att dina medarbetare kan se vad du har bokat. Den går att låsa. Information om detta finns på intranätet.

Internet

Inga program får laddas ner XXX. Utöver säkerhetsrisken kan en felaktig hantering innebära skadeståndskrav vid t.ex. brott mot upphovsrätten.

Det är inte tillåtet att via Internet titta eller lyssna på material av pornografisk eller rasistisk karaktär. Förbudet gäller också material som är diskriminerande (religion, kön, sexuell läggning, etc) eller har anknytning till kriminell verksamhet. När du surfar på Internet representerar du Timrå kommun och varumärket. Surfa med gott omdöme så att ditt agerande på nätet inte skadar kommunen. Vid besök på webbplatser lämnar vi alltid spår efter oss i form av kommunens IP-adress.

Spel via internet

Att använda kommunens nätverk för dataspel eller on-line-spel, t ex poker, är inte tillåtet.

Sociala medier

Sociala medier, till exempel Facebook, bloggar, Twitter, Instagram, kan vara användbara på många sätt men de används också av kriminella och för att inhämta information. Genom att vara medveten om riskerna kan du förhindra att information kommer i orätta händer.

Sociala medier får under arbetstid endast användas i specifika fall och om arbetet kräver det.

Tänk på!

- Var uppmärksam på om någon ställer frågor om ditt arbete eller andra uppgifter som rör kommunens verksamhet.
- Om Du blir det minsta misstänksam, berätta inte vad du arbetar med eller har tillgång till för information inom kommunen.
- Hot förekommer. Var medveten om risken att lägga ut kontaktinformation eller andra uppgifter.
- Publicera inte uppgifter eller detaljer om verksamheten.
- Publicera ALDRIG information som omfattas av sekretess.
- Flera typer av skadlig kod är specialskrivna för sociala medier. Var försiktig med länkar och nedladdningsbara filer.
- Se till att alltid ha de senaste säkerhetsuppdateringarna för att på så sätt minimera attacker från skadlig kod.
- Ändra sekretess- och säkerhetsinställningar i de sociala nätverken för att öka ditt skydd.

Lösenord

- Använd inte samma lösenord för olika nätverk eller e-postkonton.
- Använd inte heller samma lösenord privat som i arbetet.
- Använd så kallade starka lösenord, d v s blanda små och stora bokstäver, siffror och specialtecken. Lösenordet bör vara minst 10 tecken långt. Gärna i forma av en mening.
- Inga lösenord som är lätta att gissa, ex tangentföljden ASDFG eller liknande.
- Inga lösenord ska vara kopplade eller enkla att associera till dig som person.

Var restriktiv med publicering

Ingen information är skyddad på nätet. Information som du lagt ut kommer att finnas kvar länge eller till och med för alltid. Du får inte publicera uppgifter om eller bilder på dina kollegor, medarbetare, brukare.

Loggning och övervakning

All kommunikation på kommunens nät loggas och övervakas. Stickprov på exempelvis internettrafik och besökta sidor görs regelbundet. Likaså kan din e-post kontrolleras.

Hårdvara

Tänk på att datorer och program är dina arbetsverktyg och ägs av kommunen, det är inte din privata egendom. Du får inte göra ingrepp på hårdvaran eller installera program. Allt detta ska skötas av IT-enheten. Den ska också lämnas tillbaka vid avslutad anställning eller längre frånvaro.

USB-minnen med mera

USB-minnen, externa hårddiskar, digitalkameror, mobiltelefoner, GPS-mottagare, surfplattor med mera, är mycket vanliga. Stora mängder information kan på ett enkelt och snabbt sätt flyttas mellan olika plattformar.

Risker med dessa enheter

- Förvaras ofta i väskan, fickan och är lätta att tappa bort och enkla att stjäla.
- Stora mängder information kan snabbt och enkelt lagras och om minnet stjäls eller tappas bort kan mängden förlorad information bli betydande.
- Förlust av lagringsmedium kan innebära att obehöriga får tillgång till informationen.

- USB-minnen kan användas för att sprida skadliga program, virus, maskar och trojaner. De kan infektera IT-system både anslutna till nätverket och Internet.
- Att endast radera filerna på till exempel ett USB-minne ger inget skydd eftersom informationen kan återskapas.
- Använd bara lagringsmedium du fått från Timrå kommun i kommunens IT-system, eller från tillförlitliga utgivare. Använd aldrig upphittat eller på annat sätt okänt lagringsmedium i kommunens IT-system.

Enheter som inte längre ska användas ska på ett säkert sätt förstöras. Lämna det till IT-enheten. Radera alltid information som du inte längre behöver. Men kom ihåg att det går att återskapa. Rapportera förlorad enhet till din närmsta chef.

Installation av program

Alla program ska installeras av IT-enheten eller servicedesk.

Skrivare/kopiatorer inom Timrå kommun, administrativa nätet

IT-enheten ansvarar för inköp/hyra av hårdvaran utifrån verksamhetens behov. Ingen annan hårdvara än den av IT-enheten godkända får kopplas in på kommunens nät. Skrivare ska anslutas mot nätverket för att säkra funktionalitet, möjliggöra support på distans och automatisk övervakning. IT-enheten ansvarar för att drivrutiner testas, uppdateras och installeras samt att den mjukvara som finns på skrivarna konfigureras. Flytt av skrivaren ska, för att garantera säker funktion utföras av IT-enheten.

Miljö- och kostnadsbesparande inställningar

Som standard är följande inställt:

- Dubbelsidig utskrift på A4-papper.
- Svart/vit utskrift
- Energisparläge, tidsstyrning för start och avstängning/standby.

Säkerhet

På alla våra kopiatorer krävs kort/kod för utskrifter. Detta innebär att även sekretess- handlingar kan skrivas ut på lämplig skrivare och ”kvitteras ut” med kort/kod. Genom detta behövs inte en lokal skrivare på varje rum. Personliga skrivare är både dyrt och tidskrävande i support. Funktionen med kort/kod förhindrar också att ”obehöriga” får tillgång till kommunens resurser.

Rekommendationer

Tillgång till utskrift bör finnas inom rimligt gångavstånd från datorarbetsplatsen. Om tillgång till ”avancerad kopiering” krävs och större mängder utskrifter, hänvisas till Kontorsservice och deras tryckeri.

När du slutar

När du slutar din anställning eller byter arbetsplats inom kommunen ansvarar du för att:

- Rådgöra med din chef om vad av ditt arbetsmaterial som skall sparas. Notera att allt arbetsmaterial du framställt anses vara kommunens egendom och inte får tas med utan godkännande från ansvarig chef
- Överlämna information som ska vara kvar till dina kollegor. Privat material rensas och tas bort.