Malin Ekblad
Säkerhetschef
malin.ekblad@trelleborg.se

Kommunstyrelsen

Bilaga 5 – Informationssäkerhet och GDPR vid hemarbete

När fler än vanligt arbetar hemifrån leder det till att information hanteras på ett sätt som varken vi eller våra IT-system är vana vid. Det i sin tur kan resultera i negativa konsekvenser för verksamheten.

Det är viktigt att informationen hanteras säkert så att vi undviker att det hamnar i orätta händer, att den förstörs eller blir felaktig. Vi behöver minska riskerna inom kommunen.

Dataskyddförordningen

GDPR är lika viktig om du jobbar hemma som om du sitter på kontoret.

Oavsett om hemarbetet sker vid enstaka tillfällen eller har en mer långvarig karaktär är det samma rutiner som gäller.

Det ytterst viktigt att alla medarbetare är medvetna och följer de riktlinjer och rutiner som arbetsgivaren har tagit fram. Behandlar man känsliga personuppgifter ska arbetet alltid ske mot säkra nätverk – de flesta hemnätverk är säkra – med tvåfaktorsautentisering för inloggning,

Digitalt arbete

För att minska riskerna vid digitalt arbete behövs tydliga och enkla rutiner som är anpassade till just din verksamhet. Du och dina medarbetare behöver veta vad som är viktigt att tänka på vid distansarbete.

Nedan har vi delat upp viktiga saker att tänka på när du eller dina medarbetare arbetar hemifrån.

Säkerhetsaspekter vid hemarbete

Arbetsutrustning såsom dator, surfplatta eller mobiltelefon är personlig och ska inte användas för privat bruk eller av andra. Informationen där ska skyddas. Det innebär att du alltid ska logga ut och låsa datorn när du lämnar

den, även hemma. Ingen annan ska ha tillgång till utrustningen eller kunna ta del av informationen.

Säkerhetsuppdatera din utrustning så fort du blir uppmanad (datorer, surfplattor och mobiltelefoner. Säkerställ att du har starka lösenord (12 tecken) . Använd gärna tvåfaktorsinloggning där det är möjligt.

Känslig information ska inte bli tillgänglig för obehöriga. Var därför extra medveten om vilken information som du hanterar digitalt, i pappersform eller i samtal på telefon och distansmöten.

Har du utskrivna papper som innehåller personuppgifter så ska du inte slänga dem i pappersåtervinningen utan spara handlingarna tills du kommer tillbaka till jobbet och kan slänga dem i sekretess kärl där. Slarva inte med integriteten!, tänk på att du har lånat någon annans personuppgifter tillfälligt till att utföra arbetsuppgiften!

Känslig information

Känsliga och extra skyddsvärda personuppgifter samt information som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) behöver hanteras på ett säkert sätt. För att minska risken för att obehöriga får åtkomst till personuppgifter som behandlas av kommunen kan du tänka på följande:

- Anslut alltid till Trelleborg kommuns VPN på datorn, detta är extra viktigt om du kopplar upp dig på ett öppet nätverk.
- Anslut inte till öppna nätverk om du inte behöver. Säkerheten kan inte garanteras och det finns en risk att din aktivitet på nätverket övervakas. Använd istället din mobil för att dela din internetanslutning med datorn.
- Utbyt aldrig känslig eller sekretessbelagd information via offentliga, trådlösa nätverk.
- Spara aldrig verksamhetsrelaterad information på privat dator, surfplatta eller telefon eller liknande. Tänk också på att inte använda din privata e-postadress när du kommunicerar med kollegor inom ramen för ditt arbete.
- Tänk på risken för överhörning av samtal och risken att andra kan läsa vad som står på din bildskärm.
- Använd inte Office 2010 e-post, eller Zoom och Skype *(Office 365 e-post, Onedrive, Sharepoint, Teams)* till att hantera känslig information. Din tjänstetelefons appar ska inte heller användas till känslig information om de inte tagits fram för detta ändamål.
- USB-minnen ska inte användas mellan privat utrustning och din arbetsdator eftersom virus kan spridas mellan enheter. Eller ännu värre upphittade USB minnen kan ha avsiktliga virus och ska heller inte användas.
- Skydda viktig information som finns på papper och i anteckningar. Förvara informationen säkert och tänk på låsa utrymmen där känslig information finns.

- Oavsett vilket verktyg som används vid digitala arbetsmöten, bedöm risken att andra kan höra eller se informationen som förmedlas.
- Minska risken för bedrägerier genom att låta bli att klicka på länkar eller bilagor från okända avsändare. Ladda heller inte ned program som kommer via e-post, sms eller olika webbsidor, särskilt när avsändaren är okänd. Fråga kommunens IT-avdelning innan nerladdning sker av program.
- Vid digitala möten ska det i första hand användas Trelleborg kommuns Skype för företag till att bjuda in till webmöten. Med Skype för företag kan vi säkerställa informationssäkerhetskraven då kommunikationen är krypterad. Vid inbjudan att använda andra program för digitala möten, tänk på vad som förmedlas under mötet samt vilken information som skickas över och lagras via verktyget. Vid osäkerhet skall ni kontakta informationssäkerhetssamordnaren eller IT-avdelningen för att säkerställa att de uppfyller informationssäkerhetskraven.

Skydda din dator

Virus eller annan skadlig kod som drabbar din dator kan orsaka många olika typer av problem. Vissa förstör information och andra kan ge obehöriga möjligheter att fjärrstyra din dator. Det finns exempel på skadlig programvara som laddas ner till datorn efter ett klick på en länk i webbläsaren och registrerar det du skriver på din dator. Den skadliga programvaran märks inte för dig som användare. På så vis kan förövaren komma över exempelvis lösenord och kortuppgifter.

För att din dator ska vara säker behöver den kontinuerligt uppdateras. Detta sköts centralt från IT-avdelningen även när ni arbetar hemifrån, för operativsystem och verksamhetssystem. Om ni av någon annan än IT-avdelningen ombeds stänga av säkerhetsfunktioner för att exempel kunna leverera en tjänst eller installera program, skall du inte följa den uppmaningen.

Klicka bara på kända länkar

Tänk på att vara försiktig med att klicka på länkar, bilagor eller ladda ned program som kommer via e-post, sms eller olika webbsidor särskilt när du inte känner till avsändaren. Om du är osäker på om en fil du ombeds ladda ner från nätet kan innehålla virus eller annan skadlig kod bör du avstå. Har du redan laddat ner en sådan fil, undvik att öppna den och kontakta IT-avdelningen.

Genom att klicka på okända länkar kan bedragare komma över dina lösenord och på så vis kan de använda din identitet på nätet. Eller så kan någon få tag i dina kortuppgifter och tömma ditt konto efter att du klickat på en för dig okänd länk. Det kan även hända att internetanslutningen slutar att fungera, att datorn drabbas av virus eller att den till och med går sönder.

Ta för vana att logga ut från webbsidor när du är klar.

Undvik att använda andras trådlösa nätverk (publika nätverk på till exempel caféer och hotell). Den som tagit kontroll över nätverket och trådlösa routern har möjlighet att följa vad du gör. Är trafiken inte krypterad kan den komma åt känslig information till exempel mejl eller lösenord. Välj istället att koppla upp dig via din arbetstelefons mobila uppkoppling.

Tänk på det här och var en upplyst medarbetare!

Säkerställ att du som medarbetare känner till och förstår innebörden av rutinerna för att arbeta hemma.

Som medarbetare se till att du kan komma åt de resurser som behövs för att utföra ditt arbete på ett säkert sätt.

Behöver du få hjälp och svar på eventuella frågor ta inga genvägar och utgör en säkerhetsrisk utan kontakta kommunens källor eller närmsta chef för hjälp.

Som medarbetare i kommunen hanterar man regelbundet en stor mängd personuppgifter och/eller känsliga och extra skyddsvärda personuppgifter. Utan att man kanske tänker på det särskilt.

Arbetsgivaren har en del av ansvaret för att informationen hanteras på rätt sätt, genom att säkerställa att medarbetaren känner till vilka typer av uppgifter som hen hanterar i sin roll som det gäller att vara extra försiktig med. Det kan vara allt från personuppgifter om lön, barn och hälsouppgifter till lagöverträdelser och sekretessbelagda uppgifter. Vid osäkerhet fråga din närmsta chef samt viss information hittar ni också på Slättnet.

En annan del av ansvaret faller på medarbetaren. Är du osäker på vad som gäller så måste du fråga arbetsgivaren.

Följer inte du som medarbetare de rutiner som finns på arbetsplatsen, och detta leder till att uppgifter kommer i orätta händer och skapar ekonomisk skada kan numera kommunen drabbas av sanktionsavgifter om personuppgifter inte hanteras på korrekt sätt utifrån dataskyddsförordningen.