IT-säkerhet för användare i Danderyds kommuns IT-miljö

Målgrupp
Samtliga användare av Danderyds kommuns digitala utrustning, system och nätverk.

DANDERYDS KOMMUN

Inledning

Dokumentet beskriver vad du som användare har för skyldigheter och rättigheter när du använder Danderyds kommuns digitala utrustning, system och nätverk. Du som användare har ansvar för att den information vi har att tillgå och som registreras i vår IT-miljö skyddas. Därför är det av stor vikt att du förstår innehållet i dokumentet. Det är viktigt att få goda kunskaper i de system du ska använda för att minska risken för felhantering. Som medarbetare ska du ha en hög säkerhetsmedvetenhet för att förebygga eventuella hot och skador i vår IT-miljö. En grundläggande regel är att kommunens utrustning och system är dina arbetsredskap.

Äganderätt

Tilldelad IT-utrustning ägs av kommunen och är dina arbetsredskap under din anställning. Du ska som anställd vårda, hantera och förvara utrustningen på ett sätt så att skada och stöld förebyggs. Ersättningsskyldighet kan uppkomma vid vårdslöst handhavande. Stöld ska anmälas snarast genom en polisanmälan, till IT och närmaste chef. Närmaste chef har vidare ansvaret att vid behov anmäla till dataskyddsombud. Vid skada anmäler du det till IT.

Kontaktuppgifter:
it-support@danderyd.se
dataskydd@danderyd.se

Användaridentitet och lösenord

Vid nyanställning får din chef ditt användarnamn och lösenord av IT. Detta blir ditt kommunkonto som är personligt och får aldrig lånas ut till andra. Ditt kommunkonto är din e-postadress eller en kortare kombination av bokstäver från för- och efternamn. Kontot ger dig tillgång till några av organisationens system. Första gången du loggar in ska lösenordet bytas.
För ditt kommunkonto gäller lösenordskraven nedan.

- Lösenordet ska innehålla minst åtta alfanumeriska tecken. Ett starkt lösenord är att exempelvis ta första bokstaven i varje ord i en mening, samt variera med specialtecken. ***J**ag **l**ängtar **t**ill **s**ommaren **2021!*** = Jlts2021!
- Använd inte bokstäverna å,ä,ö eller specialtecknet € i lösenordet.
- Ditt lösenord får inte innehålla ditt personnummer, namn eller användarnamn.
- Du får inte avslöja ditt lösenord till andra. Endast IT kan behöva ta del av lösenordet, då ansvarar du för att byta lösenordet efter.
- Du får inte förvara ditt lösenord i klartext tillgängligt för andra.
- Använd inte samma lösenord i arbetet som privat.
- Om du har misstankar att någon känner till ditt lösenord ska du omedelbart byta.
- Tidigare lösenord kan ej återanvändas.
- Efter 120 dagar behöver du byta ditt lösenord.

Privata konton (exempelvis Apple-ID, Google- eller Facebook-konton) får inte användas eller kopplas ihop med kommunkontot för att komma åt tjänster som används i arbetet.

Informationssäkerhet

En del av informationen är värdefull och vi behöver skydda den särskilt väl, så att den inte kommer i orätta händer. Informationen ska också vara korrekt och tillgänglig när man behöver den. Majoriteten av informationen finns i våra digitala system och du som användare har ansvar att hantera informationstillgångarna på ett korrekt sätt. Läs mer om informationshantering i kommunens interna styrdokument för informationssäkerhet. Information om behandling av personuppgifter hittar du på intranätet. Se även rutin för informationsklassning om exempel på skyddsvärd information och hur du klassar den samt vilka säkerhetsåtgärder du behöver vidta.

I början av din anställning kan det bli aktuellt att skriva på en sekretessförbindelse som beskriver att det är förbjudet att muntligen, skriftligen eller på annat sätt föra vidare, röja eller utnyttja uppgifter som omfattas av sekretess.

Arbetsplatsen

En inloggad dator som lämnas obevakad kan innebära olika säkerhetsrisker, som att obehöriga kan få tillgång till KÄNSLIG information. Därför är det viktigt att du som användare minskar riskerna som det kan medföra vid din arbetsplats.

- Lämnar du din dator obevakad ska du låsa skärmen eller logga ut.
- Du ansvarar för allt som görs på din dator. Behöver någon använda datorn får personen logga in på sitt kommunkonto.
- Låt inte KÄNSLIG information bli liggande i en skrivare. Använd säkerutskrift.
- Tänk på vem som kan se din skärm. Sekretessfilm/skärmfilter finns att beställa via Beställningsportal dator.

Internet och AI tjänster

Du uppträder alltid i tjänsten när du är uppkopplad till Internet via kommunens nätverk eller utrustning. Olämplig användning av Internet och AI tjänster får inte förekomma som exempelvis är olaglig eller strider mot allmänt vedertagen moral, som har stötande innehåll till exempel kränkningar på grund av kön, etnisk eller religiös tillhörighet, brott mot mänskliga rättigheter, pornografi eller kriminell verksamhet. Detta gäller inte om du behöver ha tillgång till sådana sidor i tjänsten. Agera i enlighet med ovanstående värderingar så att det du förmedlar på Internet och AI tjänster inte skadar kommunen. Alla dina aktiviteter på Internet och AI tjänster lämnar spår efter dig i form av till exempel organisationens IP-adress. Vid misstanke om olämplig användning av Internet och AI tjänster kan kommunen granska den enskildes aktiviteter.

Virus och skadlig kod

För att minska risken att bli utsatt för virus och liknande angrepp behöver man som användare följa nedan.

- Du får inte installera program på kommunens datorer utan godkännande av IT. På kommunens datorer ska all installation av programvaror ske automatiskt eller med hjälp av IT-support.
- Privata konton (exempelvis Apple-ID, Google- eller Facebook-konton) får inte användas inom kommunens verksamhet. Dessa funktioner används i stället via webgränssnitt via utrustningens webbläsare.
- Privata konton får dock användas för att installera programvaror (appar) för användning i tjänsten och för viss privat användning på mobil användarutrustning. Sådan installation ska alltid ske från officiella online-butiker, dvs Google Play och Apple AppStore, eftersom det där upprätthålls en grundläggande säkerhetsnivå. Apparna ska hållas uppdaterade av användaren.
- Du får inte koppla in utrustning i kommunens nätverk utan godkännande av IT.
- Gör alltid en viruskontroll av extern lagringsutrustning (USB, minneskort och bärbara hårddiskar) innan användning.
- Var vaksam på virussmittad e-post genom att kontrollera att e-post-adressen är korrekt och genom att aldrig trycka på länkar som ser misstänkta ut.
- Om du misstänker att du drabbats av virus eller skadlig kod kontakta omedelbart IT via mail it-support@danderyd.se eller telefon 08-568 910 69.

E-post

E-postsystemet är ett arbetsverktyg och ska inte användas för privat bruk. Det är viktigt att veta att även elektroniska brev omfattas av offentlighetsprincipen. Viss e-post kan vara en allmän handling som är offentlig och kan då begäras ut. De flesta användare i kommunens IT-miljö har en personlig e-postadress.

Du är ansvarig för daglig kontroll av din elektroniska brevlåda, vid frånvaro ska autosvar läggas in där din frånvaro framgår. Om du behöver skicka information som är klassad KÄNSLIG till externa parter får det endast skickas med godkänd krypteringstjänst. Läs mer i säkerhetsanvisningarna hur du hanterar e-post.

Spam

E-postadresser är idag en handelsvara. Listor över e-postadresser säljs för att användas i massutskick av e-post, s.k. spam. Spam är skräppost som mottagaren inte önskar och innehåller oftast reklam och länkar till olika sidor med alltifrån bantningsmedel till pornografi men även virussmittad e-post förekommer. Det görs en övergripande kontroll av e-post hos IT men all spam kan inte stoppas. Kontakta it-support@danderyd.se om du får misstänkt e-post eller saknar e-post.

Lagring/säkerhetskopiering

Kommunens dokument och handlingar ska lagras i verksamhetssystem, på kommunens filservrar – ”Sharepoint” eller i molntjänsten Microsoft (Office) 365. Säkerhetskopiering görs regelbundet på dessa lagringsytor för att möjliggöra återläsning av dina dokument.

- Endast handlingar upp till informationsklassningen KÄNSLIG får lagras enligt ovan.
- Du får inte lagra eller säkerhetskopiera information lokalt på dina privata enheter.
- Undvik att lagra information lokalt på din enhet som ägs av kommunen. Om du skulle behöva göra det ansvarar du själv för att säkerhetskopiera.
- Du får inte lagra eller säkerhetskopiera på icke godkända molntjänster.
- Dokument och handlingar ska sparas och rensas när de är inaktuella i enlighet med förvaltningens dokumenthanteringsplan.
- Undvik att skapa kopior. Det finns en risk att de hamnar i orätta händer, blir inaktuella och försvårar rensningen.

De behörigheter du blir tilldelad beror på dina arbetsuppgifter avgörs och beställs av närmaste chef. Att försöka komma åt information utanför din behörighet är inte tillåtet.

Distansarbete

Vid distansarbete måste du få ett medgivande från närmaste chef. Du ansvarar för att du använder en säker uppkoppling mot kommunens system och att ingen kommer åt kommunens uppgifter. Övriga IT-säkerhetsregler som tas upp i dokumentet gäller även vid distansarbete.

Privat nyttjande

Privat användning får inte inkräkta på arbetet.
Tänk på att:

- Ingen privat användning av verksamhetssystemen får förekomma.
- Ingen olämplig användning av Internet och AI tjänster (se avsnitt *Internet och AI tjänster* för mer information)
- Det är inte tillåtet att installera egna program/tjänster på din dator.
- Ingen lagring av privata bilder/data i kommunens nätverk
- Ingen registrering av kommunens e-postadresser på kommersiella webbplatser för privat bruk.

Loggning

Ur verksamhets- och säkerhetssynpunkt är det viktigt med spårbarhet. Därför görs loggning på anställdas användning av verksamhetssystem och Internet. Du ansvarar för de aktiviteter som görs på ditt konto, så därför är det viktigt att du aldrig lånar ut det. IT-enheten samt kommunens säkerhetschef kan komma att ta del av de uppgifterna om så är nödvändigt.

Vid avslutad anställning kommer din närmaste chef få tillgång till din OneDrive i en månad, i syfte att säkerställa att information inte går förlorad.

Incidentrapportering

Vid en incident ska man snarast möjligt rapportera detta till IT via it-support@danderyd.se eller 08-568 910 69. En incident som även omfattar personuppgifter ska anmälas till närmaste chef som ansvarar för att anmäla till dataskydd@danderyd.se. Om så är nödvändigt ska man dokumentera händelsen med tidpunkt och händelseförlopp.
Exempel på incidenter:

- Skada på hårdvara
- Stöld
- Informationsläckage
- Drabbad av virus eller skadlig kod
- Ingen åtkomst till system

Uppföljning

Uppföljning av att kommunens IT-säkerhetsregler följs genomförs genom stickprov och loggning av användandet.

Påföljder

Du som användare i Danderyds kommuns IT-miljö är skyldig att ta del av kommunens gemensamma regler och anvisningar för IT-användandet samt följa dem. Underlåtenhet att följa reglerna kan bedömas som avtalsbrott mot anställningsavtalet och ytterst leda till uppsägning från arbetsgivarens sida.