SÅ HÄR GÖR VI I NACKA
IT-SÄKERHET: EN VÄGLEDNING FÖR MEDARBETARE

Diarienummer	Fastställd/senast uppdaterad	Beslutsinstans	Ansvarigt politiskt organ	Ansvarig processägare
KFKS-2023-00764	2023-08-15	Stadsdirektör	Kommunstyrelsen	Digitaliseringsdirektör
Så här gör vi i Nacka	IT-säkerhet: En vägledning för medarbetare			

IT-säkerhet: En vägledning för medarbetare

Dokumentets syfte
Handledningens primära syfte är att förhindra störningar i vår gemensamma IT-miljö som kan medföra negativa konsekvenser för kommunorganisationen och/eller Nackaborna.

Dokumentet gäller för
Samtliga medarbetare i Nacka kommun.

Så arbetar vi med IT-säkerhet i Nacka kommun – en vägledning för dig som medarbetare

Inledning

Tekniska framsteg
Näringsliv och offentlig förvaltning i Sverige har under de senaste decennierna tagit stora språng i arbetet att digitalisera processer och information, där modern teknik bidragit till besparingar i såväl tid som pengar. Denna utveckling har ökat vårt beroende av tekniska system och datakommunikation, men säkerhetsarbetet har inte hunnit hålla jämna steg med digitaliseringens utvecklingstakt och riskmedvetenheten har generellt varit låg.

Förändrat världsläge
Mot bakgrund av det förändrade världsläget där IT-angrepp från statliga- och statsfinansierade aktörer och cyberkriminella förekommer i allt större utsträckning, kombinerat med nya nationella- och internationella rättsliga regelverk som styr samhällets informationssäkerhet, har Nacka kommun tagit fram en vägledning för hur våra verksamheter ska jobba med IT-säkerhet för att skydda våra IT-system, enheter, programvaror och information.

Olika typer av hot och skydd
Denna vägledning fokuserar på hot och skydd som är förenade med användning av kommunens gemensamma IT-resurser och ska fungera som ett stöd för varje medarbetare i syfte att stärka skyddet för vår gemensamma IT-miljö mot

avsiktliga intrång, otillåten användning, förvanskning eller stöld av information. Även oavsiktliga handlingar som exempelvis brister i arbetsprocessernas säkerhet samt mänskliga misstag tas upp i vägledningen.

Handledningens syfte

Övergripande mål

Handledningens primära syfte är att förhindra störningar i vår gemensamma IT-miljö som kan medföra negativa konsekvenser för kommunorganisationen och/eller Nackaborna. En grundläggande förutsättning i vår befintliga och fortsatta IT-förvaltning och -utveckling är att vi följer kommunens vision om öppenhet och mångfald utifrån Nacka kommuns övergripande mål:

1. **Maximalt värde för skattepengarna:** En gemensam handledning för IT-säkerhet ska bidra till att minska risken för IT-incidenter, som i sin tur kan leda till kostsamma avbrott och kostnader för reparation och återställning. Tack vare IT-handledning kan vi också undvika onödiga utgifter för licenser och andra verktyg som inte är nödvändiga eller som kan utgöra en säkerhetsrisk.
2. **Attraktiva livsmiljöer i hela Nacka kommun:** IT-säkerhet är en viktig faktor för att skapa en trygg och säker livsmiljö för invånare i hela Nacka kommun, oavsett var vi väljer att bo och arbeta och i vilken fas i livet som vi befinner oss i. Genom att varje medarbetare har kunskap om hur var och en kan ta ansvar för den egna IT-säkerheten kan vi minimera risken för att Nackas invånare blir utsatta för cyberattacker, dataintrång och annan cyberkriminalitet. Detta är särskilt viktigt när det ska vara möjligt, för den som vill, att arbeta på distans eller enligt en hybridmodell från sitt hem i varje del av Nacka kommun.
3. **Stark och balanserad tillväxt:** En stark IT-säkerhetskultur är avgörande för att upprätthålla en stark och balanserad tillväxt både för Nacka kommun, medborgare och företag i kommunen. Genom vår gemensamma handledning om IT-säkerhet kan vi minimera risken för datastölder och andra IT-incidenter i våra system, som kan hota kommunala verksamheter och därmed, direkt eller indirekt, Nackaborna.
4. **Bästa utveckling för alla:** Vår handledning om IT-säkerhet ska bidra till en gemensam IT-säkerhetskultur och öka medvetenheten om IT-säkerhetsfrågor bland kommunens alla medarbetare. Detta resulterar i en förbättrad IT-säkerhet för alla i kommunen och bidrar till en mer hållbar och säker utveckling för alla.

Innehåll

Handledning för användare av Nacka kommuns IT-miljö

Så hanterar du system, utrustning och information.

E-post, Teams och internet

Användande av elektroniska kommunikationstjänster och tjänster på internet.

- E-postkonton som delas av flera, t.ex. myndighetsbrevlådor (för nämnder) och funktionsbrevlådor (t.ex. för enheter) ska ha utpekade ansvariga personer.
- Klicka inte på bifogade filer och länkar om du är osäker på vad de innehåller.
- Användande av sajter och tjänster avsedda för olaglig fildelning är inte tillåten från kommunens enheter och nätverk.

- När du registrerar konton som ska användas i tjänsten ska du använda en e-postadress tillhörande Nacka kommuns domän. Exempelvis ska Apple-ID i tjänst vara knutet till en @nacka.se-adress.
- Använd inte en privat e-postadress när du registrerar konton för användning i tjänsten.
- Använd Nackas tjänst Säkra meddelanden vid behov att skicka meddelanden med känsligt- eller sekretesskyddat innehåll.
- Funktion för att spara lösenord i webbläsaren ska inte användas för inloggningsuppgifter till kritiska system eller system innehållande känsliga- eller sekretessklassade uppgifter. Det är särskilt viktigt då en dator delas av flera.
- Vid skanning av dokument som innehåller känslig- eller sekretesskyddad information ska du inte använda funktionen att skanna till e-post. Skanna i stället till en lagringsyta så som H:.
  Glöm inte bort att radera dokumentet när det behandlats.
- Var uppmärksam på bedrägliga e-postmeddelanden s.k. nätfiske eller ”phishing”, telefonsamtal, SMS och meddelanden via Teams. Är bedrägeriförsöket särskilt sinnrikt ska du kontakta Servicecenter. Det kan vara motiverat att gå ut med en varning och vidta tekniska åtgärder.

Tips för e-post och chatt

- Granska meddelandens avsändaradress, bifogade filer och länkar: Vem är avsändaren? Brukar avsändaren uttrycka sig på detta sätt? Förväntade du dig att få detta meddelande?
- Var misstänksam om avsändaren uttrycker sig brådskande och/eller uppmanar att lämna ifrån dig exempelvis lösenord, kortnummer eller ladda ned en viss fil eller programvara.
- Om du är osäker: Agera inte på mejlet, utan kontakta Servicecenter, telefon
  08-718 92 50 eller e-post service@nacka.se
- Teams är inte ett verktyg enbart för intern chatt. Även externa parter utanför Nacka kan inleda Teams-chatt med dig. Säkerställ att personen du chattar med är den som personen utger sig för att vara.
- Läs mer om hur du kan hantera e-post på ett säkert sätt på www.nacka.se/medarbetare/digitalisering/informationssakerhet/guider-och-mallar-for-informationssakerhet/

Åtkomst och behörighet

Hantering av inloggningsuppgifter.

- Dina inloggningsuppgifter får användas endast av dig personligen och uppgifterna ska skyddas mot obehörig användning. Lösenord och koder

ska hanteras som en värdehandling och inte ligga framme nedskrivet på en lapp eller på annat sätt vara tillgänglig för någon annan.

- För personal anställd av Nacka kommun, förtroendevalda och elever krävs en av Nacka utfärdad digital identitet för att få åtkomst till Nacka kommuns IT-system och information.
  Ett användarkonto ska finnas i Nackas katalogtjänst Active Directory.
- Återanvänd inte lösenord mellan jobbrelaterade system, och använd heller ej samma lösenord till privata tjänster.
- Vid inloggning till system och tjänster ska inloggning ske med flerfaktorsautentisering om möjligheten finns eller då det finns rättsliga krav.
- Lösenord ska vara starka och bestå av minst 14 tecken, innehålla gemener och versaler samt ett specialtecken. Fler tecken är viktigare än att använda många specialtecken.
  Lösenord ska bytas minst årligen.
  Tips för hur du skapar bra lösenord:
  www.nacka.se/medarbetare/system/it-sakerhetstjanster/
- Om du misstänker att ditt lösenord blivit röjt så ska du byta det omgående och därefter informera Servicecenter.
- I system som inte stödjer tvingande lösenordsbyten är det medarbetarens ansvar att byta lösenord minst årligen.
- Det är inte tillåtet att kringgå säkerhetsfunktioner eller att otillåtet höja egna- eller andras behörigheter.
- Läs mer om hur du kan arbeta med behörigheter på ett säkert sätt:
  www.nacka.se/medarbetare/digitalisering/informationssakerhet/guider-och-mallar-for-informationssakerhet/

Enheter och nätverk

Så använder vi och skyddar våra enheter och nätverk.

- Enheter som tillhandahålls av Nacka kommun är personliga arbetsredskap såvida de inte är uttalat delade enheter.
  Enheterna får inte lånas eller överlåtas utan att först ha tömts på information. Kontakta Servicecenter om du vill ha hjälp.
- Om medarbetare byter enhet ska dator registreras på den nya enheten. Kontakta servicecenter som för hjälp.
- Åtkomst till kommunens system och information ska i regel ske från av kommunen tillhandahållna enheter.
- Kommunens enheter så som datorer, mobiltelefoner och surfplattor eller andra smarta enheter, ska anslutas till för ändamålet avsett nätverk.
- Enheter tillhörande besökare och leverantörer får endast anslutas till Nackas gästnätverk.

Privata enheter får endast anslutas till för ändamålet avsett nätverk **Nacka BYOD**.

- Främmande IT-utrustning får inte anslutas till Nackas nätverk utan godkännande från digitaliseringsenheten.
- Mobiltelefoner och surfplattor ska ha ett skärmlås med säkerhetskod bestående av minst sex tecken. Skärmlåset ska aktiveras automatiskt inom som längst två minuter.
  I stället för säkerhetskod kan även biometrisk upplåsning så som fingeravtryck eller ansiktsavläsning användas om du föredrar detta.
- Mobila enheter får inte lämnas utan uppsikt och ska förvaras i säkert och skyddat utrymme.
- Lås din dator när du inte är vid ditt skrivbord. På Windows-datorer görs detta enklast genom att trycka på Windows-tangenten och L samtidigt.
- En stulen eller borttappad enhet ska anmälas till Servicecenter så snart som möjligt då enheten kan spärras och i vissa fall fjärraderas. Därefter ska en polisanmälan upprättas.
- Kommunens enheter ska hanteras enligt en livscykelhanteringsplan som syftar till att bibehålla funktion och säkerhet samt minska risk för avbrott och informationsförlust.
  Planen gör det också möjligt att planera inköp av utrustning vilket ger bättre överblick och jämnare fördelning av kostnader samt en tillförlitlig försörjning av enheter.
- IT-utrustning som inte längre är i bruk ska lämnas in till Servicecenter där utrustningen återvinns eller avfallshanteras på ett IT-säkerhetsmässigt korrekt sätt.
  Servicecenter kan hjälpa till med att destruera inlämnat lagringsmedia.
- Vid distansarbete ansvarar du själv för säkerheten i det nätverk du ansluter till.
- Undvik att ansluta till publika trådlösa nätverk då det finns en risk att nätverkstrafiken avlyssnas eller att enheten utsätts för IT-angrepp.
  Parkoppla hellre dator med din mobiltelefon för åtkomst till internet.
- Aktiviteter som påverkar säkerheten och integriteten för kommunens IT-miljö är förbjudna.
- Uppsatta säkerhetsinställningar i enheter får inte ändras.
- Använd aldrig en publik eller okänd dator för att ansluta till något av kommunens system.

Lagring

Var vi lagrar information och hur vi hanterar den.

- Information som behandlas av kommunen ska skyddas på rätt sätt. I första hand ska information behandlas i avsett verksamhetssystem där

skyddet är rätt dimensionerat.
Se guide för att välja lagringsplats om verksamhetssystem saknas: https://www.nacka.se/medarbetare/digitalisering/informationssakerhet

- Information som lagras på nätverksdiskar eller i kommunens molnlagring säkerhetskopieras. Det kan vara personliga (H:) eller gemensamma lagringsytor (Q:), eller i Nackas Microsoft 365- miljö, t.ex. Onedrive, Sharepoint eller Teams.
  Viktig information bör inte lagras enbart på en bärbar enhet så som en USB-disk eller bärbar dator.
- Använd endast av informationsägaren godkända molntjänster för behandling av information.
- Vid informationsdelning med leverantör eller annan extern part ska kommunens samarbetsverktyg och lagringsplatser användas i första hand. Se guide för val av lagringsplats på: https://www.nacka.se/medarbetare/digitalisering/informationssakerhet/guider-och-mallar-for-informationssakerhet/
- Filer för privat bruk så som filmer, program och spel får inte laddas ned, strömmas, lagras eller spridas i eller via Nacka kommuns nätverk.
- Flyttbar lagringsmedia ska om möjligt undvikas då det lätt tappas bort. Behöver arbetsmaterial lagras på flyttbar lagringsmedia bör informationen krypteras.
- Anslut inte okända eller upphittade flyttbara lagringsmedia till din dator då de kan innehålla skadlig kod så som virus.

Placering av IT-utrustning

Var du placerar din utrustning.

- Enheter som datorer och skrivare ska placeras där allmänheten inte har tillträde eller lättåtkomlig för obehörig.
- Om dator eller skrivare är avsedd för användning av besökare ska den placeras där personal har uppsikt över den.

System och programvaror

Hur vi använder system och programvaror.

- Använd bara system och programvaror som är godkända ur såväl informationssäkerhets- som personuppgiftshänseende.
  Av Nacka upphandlade och tillhandahållna tjänster uppfyller ställda krav.
- Endast programvaror som godkänts av Digitaliseringsenheten får användas.

Godkända program finns att hämta från Nackas programbibliotek eller beställa hos Servicecenter.

- Installerad programvara får inte kopieras till annan enhet.
- Vid installation av appar på mobila enheter så får de får endast hämtas från Apple App Store, Google Play eller distribueras av Digitaliseringsenheten.
- Det är viktigt att välja appar med omsorg. Användande av vissa appar kan medföra otillbörligt röjande av information t.ex. personuppgifter och dokument. De kan också utsätta Nacka kommuns IT-miljö för risk till exempel skadlig kod.
  Vänd dig till din chef för lämplighetsbedömning av appar.
- Vissa appar kan vara otillåtna att använda på kommunens enheter. Dessa kommuniceras via Nacka.se. Tekniska begräsningar för att förhindra användning av otillåtna appar kan införas av Digitaliseringsenheten.
- De kontorsprogramvaror (tidigare kallat Office 365) som medföljer Microsoft 365-licensen får endast installeras på enheter som tillhör Nacka kommun.

Avvikelser och incidenter

Rapportering av avvikelser och incidenter.

- IT-och informationssäkerhetsincidenter ska rapporteras och dokumenteras för att minska sannolikheten för liknande framtida händelser.
  Incidenter rapporteras till Servicecenter.
- Om du misstänker att din dator är infekterad av virus ska du koppla bort den från nätverket och ta kontakt med servicecenter
- Var observant på om IT-utrustningen beter sig långsamt eller konstigt. Vid misstanke om angrepp av skadlig kod så som virus, eller andra avvikelser på utrustning kontakta Servicecenter.

Handledning för verksamheter – åtkomst och behörighet

Så arbetar verksamheter med åtkomst- och behörighetshantering i sina verksamhetssystem.

- Om en verksamhet hanterar många lösenord ska en lösenordshanterare användas.
  En lösenordshanterare är ett program som sparar dina inloggningsuppgifter i ett krypterat valv. Valvet är krypterat med ditt huvudlösenord, vilket du väljer själv och ingen annan känner till. Lösenordshanteraren fungerar på så vis som en låst anteckningsbok med alla dina lösenord. När du vill logga in någonstans låser du bara upp lösenordshanteraren och kopierar det rätta lösenordet.

- För varje system ska det finnas tydliga rutiner för tilldelning, granskning och avslut av behörigheter.
- Användaridentiteter ska vara personliga och unika över tid.
- Externa användares (t.ex. konsulter) åtkomster bör vara tidsbegränsade samt föregås av sekretessavtal.
- När behörigheter tilldelas eller ändras ska en bedömning göras avseende användarens tilltänkta roll i systemet och med utgångspunkt i "minsta möjliga behörighet".
- Behörigheter till systemet ska inaktiveras, justeras eller raderas vid avslutande eller ändring av roll, avslut av avtal eller i överenskommelse med externa parter.
- För privilegierade behörigheter (ex. systemadministratörer) i systemet ska separata och personliga användaridentiteter tilldelas som ska godkännas av systemägare.
  Behörigheter ska vara tidsbegränsade och förnyelse ske efter bedömning om behörigheter fortfarande krävs.
- Behörigheter ska granskas minst halvårsvis genom stickprov. Användare med priviligierade behörigheter granskas särskilt.

Så jobbar Digitaliseringsenheten med säkerhet i Nacka kommuns IT-miljö

Så samarbetar Digitaliseringsenheten, Servicecenter och driftleverantör kring IT-säkerhet.

E-post och internet

Centrala skydd vid användning av e-post och internet

- E-post genomgår skräppostfiltrering och genomsöks efter skadlig kod.

- Vissa filtyper blockeras av vårt e-postsystem eftersom dessa är vanligt förkommande i spridande av skadlig kod. Förteckning över blockerade filtyper hittar du på www.nacka.se/medarbetare/system/it-sakerhetstjanster/

- Åtkomst till webbsidor och servrar på internet som kan misstänkas innehålla skadlig kod begränsas.

Åtkomst och behörighet

Så arbetar vi med åtkomst och behörighet.

- Nacka kommun har som lösenordspolicy att ett lösenord ska bestå av minst 14 tecken, innehålla gemener och versaler samt ett specialtecken.
- Lösenordet ska bytas minst en gång per år.
- Flerfaktorsautentisering används vid åtkomst till system- och information som är av särskild vikt eller innehåller känsliga eller sekretessklassade uppgifter samt vid åtkomst till tjänster i Microsoft 365. Rekommendation från IT-säkerhetssamordnare, informationssäkerhetssamordnare och dataskyddsombud beaktas och är vägledande.

Enheter och nätverk

Samlad hantering av enheter och nätverk.

- Enheter som tillhandahålls av kommunen, t.ex. datorer, mobiltelefoner, surfplattor och liknande hanteras centralt och har ett skydd mot skadlig kod och förses med av leverantören rekommenderade säkerhetsuppdateringar.
- Enheter som inte hanteras centralt eller inte uppfyller av Digitaliseringsenheten ställda säkerhetskrav får inte anslutas till kommunens IT-miljö.
- Delade enheter och enheter med specificerad funktion har mer ingående central styrning.
- Kommunen har olika nätverk beroende på användningsområde. Det för att segmentera trafiken mellan för olika system och enheter och för att begränsa skadeverkningar vid IT-angrepp.
- Information på datorns lokala hårddisk skyddas med fulldisk-kryptering.
- Digitaliseringsenheten loggar all trafik som sker till, från, och inom kommunens nätverk. Syftet är att kunna analysera trafiken för att upptäcka olika former av hot mot kommunens nätverk.
- IT-infrastruktursystem och nätverk övervakas för säkerhetshändelser.

Lagring

Så hanteras kommunens lagringsytor.

- Digitaliseringsenheten ansvarar för att säkerhetskopiera information som lagras på nätverksdiskarna, så som H, I, P, Q samt det som lagras i Microsoft 365, så som Onedrive, Sharepoint och Teams.
- Digitaliseringsenheten ansvarar för att kunna katastrof-återställa system där drift sker hos kommunens upphandlade driftleverantör.

Teknikutrymmen

Så hanteras utrymmen för IT-utrustning.

- Utrymmen för IT-utrustning tillträdesbegränsas.

System och programvaror

Skydd för enheter och system samt säkerhetsövervakning.

- System och applikationer hanteras enligt en livcykelhanteringsplan som syftar till att få kontroll över hur mjukvara tas i drift, underhålls och avvecklas.
- Skydd mot skadlig kod finns för kommunens datorer samt systemet som driftas hos kommunens upphandlade driftleverantör.
- Vartefter leverantör tillgängliggör säkerhetsuppdateringar till system och programvaror installeras dessa skyndsamt.
- Digitaliseringsenheten går igenom tekniska säkerhetsåtgärder regelbundet och vid större förändringar.
- Loggar inhämtas från IT-infrastruktur och system i syfte att identifiera och hantera tekniska avvikelser, uppfylla lagkrav och som en del av säkerhetsövervakningen.
- System för att övervaka säkerhetshändelser i kommunens IT-miljö används för att skydda system och information mot olika former av IT-säkerhetshot.