Återremissyrkande Demokraterna, Moderaterna, Liberalerna, Kristdemokraterna

Datum 2025-08-22 Ärendenummer SLK-2024-00392

Yrkande angående – Revidering av Göteborgs Stads regel för IT-användare

Förslag till beslut

I kommunstyrelsen och kommunfullmäktige:

1. Ärendet återremitteras till kommunstyrelsen för hörande av samtliga nämnder och bolag med inhämtning av synpunkter utifrån en fördjupad analys av de ekonomiska och arbetsmiljömässiga konsekvenserna av det föreslagna regelverket.
2. Ärendet återremitteras till kommunstyrelsen för att inhämta ytterligare underlag och analysera hur Sveriges Kommuner och Regioner (SKR), Stockholms stad, Malmö stad samt andra relevanta aktörer arbetar i frågan.

Yrkande

Det finns ett tydligt behov av att uppdatera stadens regler för IT-användning. En modern styrning är avgörande för att möta de krav som följer av utvecklingen inom informationssäkerhet, effektivitet och lagstiftning.

Vi har tagit del av det reviderade förslaget till regelverk och tillhörande tjänsteutlåtande. Intentionerna bakom förändringarna är begripliga, särskilt avseende förstärkt säkerhet och anpassning till gällande rätt. Vår oro gäller dock att konsekvenserna ur ett praktiskt verksamhetsperspektiv inte är tillräckligt belysta eller förankrande bland de som berörs. Flera av skrivningarna riskerar att skapa betydande problem och i vissa fall ohanterliga situationer för både medarbetare och verksamheter.

Ett exempel är förslaget om att inskränka eller förbjuda privat användning av tjänstemobiler. Förslaget saknar en fullständig konsekvensanalys av hur detta påverkar både organisationen och de anställda. Det finns dessutom en påtaglig risk att en alltför restriktiv hållning, där gränsen mellan arbete och privatliv skärps, i praktiken leder till att fler medarbetare använder sina privata telefoner för arbetsuppgifter. Detta skulle i stället öka säkerhetsriskerna och ge upphov till svårhanterliga ansvarsfrågor, vilket motverkar syftet med de nya reglerna.

För att säkerställa att ett framtida regelverk får avsedd effekt utan att i onödan försvåra verksamheternas uppdrag, och för att kunna tillhandahålla de verktyg och den utbildning som krävs, anser vi att ärendet bör återremitteras.

Yrkande

SLK-2024-00392

2025-05-02

Yrkande angående Revidering av Göteborgs Stads regel för IT-användare

Förslag till beslut:

I kommunstyrelsen och kommunfullmäktige:

1. Göteborgs Stads regel för IT-användare revideras i enlighet med bilaga 2 till stadsledningskontorets tjänsteutlåtande och börjar gälla från och med 2027-01-01.
2. Göteborgs Stads regel för användande av e-post, beslutad i kommunfullmäktige 2011-06-09 § 13, upphör att gälla från och med 2027-01-01.
3. Göteborgs Stads regel för IT-användare, beslutad i kommunfullmäktige 2009-09-10 § 17, upphör att gälla från och med 2027-01-01.
4. Inköp- och upphandlingsnämnden får i uppdrag att säkerställa att vid framtida upphandling och användning av IT-system, IT-utrustning och IT-tjänster inom Göteborgs Stad ska särskild vikt fästas vid leverantörers och produkters förmåga att uppfylla krav på informationssäkerhet, datasuveränitet och oberoende från utländska jurisdiktioner som kan innebära säkerhetsrisker.

Yrkandet

Med hänsyn till att den nuvarande mandatperioden avslutas den 31 december 2026 och att ett nytt politiskt styre tillträder 2027, är det lämpligt att den reviderade regeln för IT-användare träder i kraft från och med 1 januari 2027.

Det säkerställer stabilitet, underlättar införandet av nya rutiner i början av mandatperioden och ger samtliga förvaltningar möjlighet till god planering och genomförande.

Vi ser också positivt på en ökad cybersäkerhetsinriktning i Göteborgs Stad. Sverigedemokraterna har tidigare motionerat om att förbjuda TikTok på stadens utrustning av säkerhetsskäl, vilket tydliggjorde behovet av att noggrant hantera risker kopplade till utländska applikationer och leverantörer.

För att ytterligare stärka stadens motståndskraft mot cyberhot föreslås därför också att särskild vikt ska fästas vid informationssäkerhet och datasuveränitet vid framtida IT-upphandlingar. Utan att rikta in oss på specifika länder, vill vi säkerställa att Göteborgs Stad inte blir beroende av leverantörer eller lösningar som kan stå under inflytande från stater som utgör en potentiell säkerhetsrisk, såsom aktörer som inte respekterar svensk eller europeisk säkerhetsstandard.

Tjänsteutlåtande
Utfärdat 2024-04-11
Reviderat 2025-04-14
Ärendenummer SLK-2024-00392

Handläggare
Linda Larsson, Helena Österlind och Sara Linderup
Telefon: 031-386 03 09
E-post: linda.larsson@stadshuset.goteborg.se

Revidering av Göteborgs Stads regel för IT-användare

Förslag till beslut

I kommunstyrelsen och kommunfullmäktige:

1. Göteborgs Stads regel för IT-användare revideras i enlighet med bilaga 2 till stadsledningskontorets tjänsteutlåtande och börjar gälla från och med 2026-01-01.
2. Göteborgs Stads regel för användande av e-post, beslutad i kommunfullmäktige 2011-06-09 § 13, upphör att gälla från och med 2026-01-01.
3. Göteborgs Stads regel för IT-användare, beslutad i kommunfullmäktige 2009-09-10 § 17, upphör att gälla från och med 2026-01-01.

Sammanfattning

Stadsledningskontoret har reviderat Göteborgs Stads regel för IT-användare utifrån behov av tydligare styrning och vägledning, ökad användbarhet samt ändrad och tillkommen lagstiftning inom informations- och cybersäkerhetsområdet. De ändringar som gjorts i regeln innefattar i huvudsak ett förtydligande gällande privat användning, nedladdning av appar (applikationer) samt arbetsgivarens rätt till tillgång och kontroll över IT-resurser. I revideringen av regel för IT-användare har innehåll från Göteborgs Stads regel för e-post omhändertagits. Göteborgs Stads regel för e-post bedöms därmed kunna upphöra.

Stadsledningskontoret bedömer att de ändringar som gjorts i regeln samt sammanslagningen av två styrande dokument bidrar till en mer ändamålsenlig styrning. De omarbetade reglerna bedöms vara en förutsättning för att efterleva lagkrav, minska stadens säkerhetsrisker och samtidigt möta de utmaningar som kommer med digitaliseringen kring bland annat tillgänglighet, informations- och cybersäkerhet. En tydligare reglering bedöms underlätta för IT-användare att göra rätt och minska risken för informations- och cybersäkerhetsincidenter som kan skada stadens verksamheter, medarbetare, brukare och invånare.

Inom ramen för revideringen har det framförts utmaningar som försvårar för IT-användare att följa regeln. Stadsledningskontoret bedömer att nämnder och styrelser bör ges tid för att säkerställa förutsättningar för efterlevnad, såsom kommunikationsinsatser och lokala rutiner, innan den nya regeln börjar gälla.

Stadsledningskontoret har utifrån beslut om återremiss av kommunstyrelsen 2024-06-12 § 568 kompletterat utredningen med konsekvenser av privat användning av Göteborgs Stads digitala arbetsverktyg med hänsyn till säkerhet, ekonomi och juridik.

Utredningen visar att det finns tekniska åtgärder som kan genomföras för att möjliggöra privat användning av Göteborgs Stads digitala arbetsverktyg. Stadsledningskontoret bedömer dock att de tekniska åtgärderna inte är tillräckliga utifrån ett informationssäkerhetsperspektiv. Även ur ett juridiskt och ekonomiskt perspektiv bedömer stadsledningskontoret att stadens IT-resurser endast i ytterst begränsad omfattning bör användas för privat bruk.

Bedömning ur ekonomisk dimension

Revideringen av regler för IT-användning, inklusive inarbetning av regler för e-post, förväntas bidra till tydligare styrning och ett ökat säkerhetsfokus. Det tydliga säkerhetsperspektivet i de omarbetade reglerna minskar risken för uppkomsten av kostsamma säkerhetsrisker som exempelvis cyberattacker, IT-avbrott och informationssäkerhetsincidenter. Den primära anledningen till att reglera användandet är ur ett säkerhetsperspektiv där kostnaderna kopplas till risken för sanktionsavgifter och informationssäkerhetsincidenter, snarare än att staden har löpande utgifter för det privata användandet. I händelse av ett IT-avbrott eller en cyberattack när informationen blir otillgänglig kan arbetsuppgifter och uppdrag inte utföras som planerat vilket både blir tidskrävande och kostsamt.

För att säkerställa efterlevnad av regeln krävs att nämnder och styrelser tar fram erforderliga rutiner samt justerar behörigheter och beställningar för IT-resurser. Detta kan på kort sikt öka mängden administration. På längre sikt bedöms emellertid administrationen minska eftersom tydlighet i hur stadens medarbetare får använda sina IT-resurser och hur staden hanterar dessa bedöms bidra till effektivare processer och färre avvikelser, vilket i sig kan ge positiva ekonomiska effekter. Tydligare och mer central hantering av behörigheter förväntas även bidra till att staden får bättre överblick över vilka program och appar som är nödvändiga för stadens IT-användare utifrån roll och arbetsuppgifter. Detta innebär att staden inte behöver finansiera tjänster som inte är nödvändiga.

På sikt bedöms en ytterst begränsad privat användning av IT-resurser bidra till minskat slitage av stadens egendom, vilket medför att den inte behöver bytas ut i samma utsträckning med minskade kostnader till följd.

För att minska risken att IT-användare laddar ner skadliga appar på sina mobila enheter bör tekniska åtgärder genomföras. Inom ramen för Intraservice uppdrag med att tillhandahålla en säker digital infrastruktur arbetar de med tjänster som avser centraliserad styrning av vilka appar som ska tillåtas. Tjänsten bedöms ingå i det underlag som nämnden lämnat i Årlig analys 2025, vilken i sin tur ingår i de budgetförutsättningar som stadsledningskontoret lämnat till kommunstyrelsen. Stadsledningskontoret kan inte bedöma motsvarande kostnader för de nämnder och styrelser som valt systemlösningar utanför Intraservice tjänstekatalog, utan dessa får hanteras i enlighet med ordinarie budgetprocess.

För den enskilde medarbetaren kan en begränsad möjlighet att använda IT-resurser utanför tjänsten innebära tillkommande kostnader för inköp av privata resurser, såsom telefon och dator. De tekniska åtgärder som föreslås i utredningen skulle dessutom innebära en begränsning av funktionaliteten privat, varför stadsledningskontoret antar att privata inköp av IT-resurser ändå kan bli nödvändiga. Kostnaderna för detta är beroende av personliga val och kan inte uppskattas generellt. I det fall staden skulle tillåta privat

användning av IT-resurser kan det för vissa medarbetare utgöra en skattepliktig förmån som måste redovisas.

Stadsledningskontorets bedömning är att det i sak inte tillkommer några ytterligare kostnader utifrån den föreslagna regeln då den primärt syftar till att styra hur stadens IT-användare agerar. För att underlätta en efterlevnad av regeln bedömer dock stadsledningskontoret att staden behöver tillhandahålla utbildningsinsatser och kommunikationsmaterial. Ansvaret för informationssäkerhet ligger på respektive nämnd och styrelse men stadsledningskontoret bedömer det vara ekonomiskt fördelaktigt att ett övergripande stadengemensamt material tas fram av stadsledningskontoret. Utifrån detta kan nämnder och styrelser ta fram egna insatser som utgår från verksamhetens uppdrag samt nuvarande tekniska och organisatoriska förutsättningar. Bedömningen är att framtagande av övergripande kommunikationsmaterial ryms inom kommunstyrelsens budget för 2025.

För att möjliggöra privat användning av de mobila enheterna, såsom telefon och surfplatta, visar utredningen från Intraservice grova uppskattningar om kostnader för detta. Enligt utredningen skulle nämndens kostnader uppgå till cirka 4,4 miljoner kronor för ett fortsatt utredande av vissa möjliga åtgärder samt ett faktiskt införande av vissa åtgärder. Kostnaderna för förvaltning av de åtgärder som bedöms kunna införas utan vidare utredning uppskattas uppgå till cirka 12 miljoner kronor årligen för Intraservice. Utredningen är dock tydlig med att uppskattningen av kostnader kan påverkas av kommande utredningar och inte heller garanterar absolut säkerhet. Utvecklingen inom området går snabbt och åtgärder som bedöms tillräckliga 2025 kan behöva justeras och ändras i takt med att hoten ändrar karaktär eller styrka.

Intraservice utredning nämner att införandet av åtgärder även kommer innebära kostnader för andra nämnder och styrelser. En förutsättning för att Intraservice ska kunna stärka skyddet för stadens enheter är att samtliga förvaltningar och bolag nyttjar tjänsten staden-mobil. Ytterligare kostnader som ankommer på nämnder och styrelser är utbildning av IT-användare och framtagande av rutiner samt administrativa kostnader för att upprätthålla nödvändiga regelverk.

Bedömning ur ekologisk dimension

I Göteborgs Stads Miljö- och klimatprogram finns målet att Göteborgs Stads klimatavtryck är nära noll, vilket bland annat ska ske genom att staden minskar klimatpåverkan från inköp. Ett minskat slitage av stadens IT-resurser bedöms medföra färre inköp för stadens del. Samtidigt innebär en skärpning av möjligheten att använda stadens IT-resurser för privat bruk att vissa medarbetare kommer behöva införskaffa en privat telefon/dator, vilket bedöms inverka negativt på den ekologiska dimensionen.

När förvaltningen för kretslopp och vatten införde en ny riktlinje för mobiltelefonanvändning i december 2023 gjordes det utifrån ett säkerhetsperspektiv. Riktlinjen innebär ett förbud mot nedladdning av appar för privat bruk i syfte att skydda förvaltningens information och data. I samband med den nya riktlinjen bytte förvaltningen även ut äldre mobiltelefoner. De gamla mobilerna lades sedan ut på Återbruket vilket möjliggjorde för medarbetare att köpa tillbaka dem för privat bruk till en rimlig kostnad, vilket bidrog till minskad klimatpåverkan.

Bedömning ur social dimension

Bristande informationssäkerhetsarbete kan slå hårt mot en offentlig verksamhet ur ett säkerhetsperspektiv. Otillgänglig information eller röjande av information kan skada både organisationer och individer och bidra till minskad tillit till samhället. Bristande förtroende till att staden hanterar sin information och sina resurser på ett säkert och ändamålsenligt sätt riskerar att leda till att tilliten till stadens verksamheter sjunker. På sikt kan detta leda till att de som har behov av och rätt till kommunens insatser väljer att inte ta del av dem av rädsla för hur informationen hanteras. Bristande IT-säkerhet riskerar även att skada stadens brukare. Exempelvis inom socialtjänsten bedöms det vara av största vikt att i möjligaste mån försvåra exempelvis spårning av mobiltelefoner för att spåra personal eller utsatta brukare via personal.

För att stadens verksamheter även vid kriser och IT-avbrott ska kunna upprätthållas på en acceptabel nivå krävs ett systematiskt och långsiktigt arbete med informations-och cybersäkerhet. Ett systematiskt informations- och cybersäkerhetsarbete bygger på ett samspel mellan teknik, människa, juridik och administration såsom rutiner, utbildning och att säkerheten arbetas in i verksamheten. I grunden handlar det om att bidra till att stadens användare kan arbeta digitalt i en ny och mer riskfylld omvärldskontext än tidigare och därmed skydda vår demokrati.

Den reviderade regeln medger att privat användning av stadens IT-resurser får ske i ytterst begränsad omfattning. En av anledningarna till att en begränsad omfattning tillåts är att exempelvis barn ska kunna känna sig trygga med att de kan nå sina vårdnadshavare även när dessa är i tjänst samt att medarbetare ska kunna sköta privata akuta frågor på ett sätt som inte stör arbetet mer än nödvändigt.

Stadsledningskontorets bedömning är att ett tillåtande av privat användning av stadens IT-resurser i mer än ytterst begränsad omfattning skulle inverka negativt på den personliga integriteten. Den utredning som gjorts om möjligheter att tillåta privat användning visar att åtgärderna innebär en mer omfattande övervakning av enheterna, vilket skulle innefatta även den privata aktivitet som sker. Privat användning kan även leda till att känsliga data oavsiktligt exponeras, exempelvis genom appar som samlar in information om personuppgifter som är av privat karaktär.

Samverkan

Ärendet har samverkats i Central samverkansgrupp 2024-04-18 och 2025-04-10. Dialog har skett med Koncernfackliga rådet 2024-04-24 samt 2025-03-19.

Bilagor

1. Kommunstyrelsens protokollsutdrag 2024-06-12 § 568
2. Förslag till Göteborgs Stads regel för IT-användare
3. Göteborgs Stads regel för IT-användare, beslutad 2009-09-10 § 17
4. Göteborgs Stads regler för användande av e-post, beslutade 2011-06-09 § 13
5. PM - Rättslig reglering
6. Protokollsutdrag Central samverkansgrupp, CSG, 2024-04-18 § 5b
7. Protokollsutdrag, Koncernfackliga rådet, KFR, 2024-04-24 § 9
8. Protokollsutdrag Central Samverkansgrupp, CSG, 2025-04-10 § 5a
9. Protokollsutdrag, Koncernfackliga rådet, KFR, 2025-03-19 § 8

Ärendet

Stadsledningskontoret har reviderat Göteborgs Stads regel för IT-användare utifrån ett förändrat omvärldsläge, ny EU-lagstiftning och den snabba digitala utvecklingen. Den reviderade regeln avser att ersätta nuvarande regel vilken beslutades av kommunfullmäktige 2009-09-10 § 17. Göteborgs Stads regel för användande av e-post har inarbetats i den reviderade regeln för IT-användare och bedöms därmed kunna upphöra.

Stadsledningskontoret har utifrån beslut om återremiss i kommunstyrelsen 2024-06-12 § 568, kompletterat utredningen med konsekvenser av privat användning av Göteborgs Stads digitala arbetsverktyg med hänsyn till säkerhet, ekonomi och juridik.

Beskrivning av ärendet

Göteborgs Stads uppdrag innebär ett ansvar att upprätthålla flera viktiga samhällsfunktioner. Detta ställer höga krav på informations- och cybersäkerhet. I Göteborgs Stads plan för digitalisering 2023-2026 finns en insats om att genomföra en översyn av riktlinjen för informationssäkerhet och de styrande dokument som angränsar till denna för att säkerställa ändamålsenlig styrning och tillämpning. Kommunfullmäktige beslutade 2023-05-25 § 7, om reviderad riktlinje för informationssäkerhet samt upphörande av två regler. Stadsledningskontoret redovisar i detta ärende översynen av resterande närliggande styrande dokument, vilka är Göteborg Stads regel för IT-användare och Göteborgs Stads regler för användande av e-post.

Göteborgs Stads nuvarande regel för IT-användare antogs av kommunfullmäktige 2009 och de revideringar som gjorts sedan dess har i huvudsak varit av redaktionell karaktär. Detsamma gäller för Göteborgs Stads regler för användande av e-post som antogs 2011. Översynen har visat att det har utvecklats en praxis av tillämpningen som inte överensstämmer med nuvarande behov av reglering. När regeln för IT-användare togs fram var det främst fokus på kostnader, prestanda och arbetstagarens tid. Idag är ekonomin inte en begränsande faktor eftersom det för staden inte innebär några större kostnader att låta IT-användare nyttja stadens resurser för privat bruk. Detta har resulterat i ett tillåtet privat användande av stadens IT-resurser, framför allt gällande mobiltelefoner.

Stadens medarbetare, konsulter, leverantörer med flera kommunicerar och använder IT-resurser på ett helt annat sätt idag än vad som var brukligt 2009. Digitaliseringen har skapat nya arbetssätt samtidigt som säkerheten och tillämpningen av regeln för IT-användare inte har reviderats i takt med utvecklingen. Den snabba utvecklingen av digitala arbetssätt, teknik och artificiell intelligens (AI) har medfört ett ökat beroende av digital information och IT-resurser. Samtidigt som digitalisering och teknikutveckling innebär möjligheter medför det också ökad risk för sårbarheter, mänskliga misstag, cyberattacker och intrång i stadens system.

Det är dessutom ett annat omvärldsläge år 2025 än 2009. IT-hoten och risken för mänskliga misstag ställer högre krav på säkerhet och tydligare styrning kring hantering av stadens IT-resurser. Totalförsvarets forskningsinstitut (FOI) skriver i sin rapport ”Delat ansvar är ingens ansvar” att det är i det nutida digitaliserade samhällets natur att vara uppkopplat och sammankopplat, såväl mellan svenska offentliga parter och privata

företag som mot utlandet. Det digitala samhället för med sig effektivitet, bekvämlighet, välstånd och innovation men även nya sårbarheter, utmaningar och hot.

Nationellt cybersäkerhetscenter (NCSC) skriver i sin rapport "Cybersäkerhet i Sverige 2022, Del 1: Hot, metoder, brister och beroenden" att Sverige varje dag utsätts för säkerhetshotande aktioner i form av cyberangrepp som kan kopplas till olika hotaktörer, i huvudsak statliga aktörer och kriminella och i viss omfattning även av ideologiskt motiverade aktörer, såsom hacktivister. Hotet från främmande makt är högt, vilket återkommer bland annat i Säkerhetspolisens årsrapport från 2022/2023 där de ser en förändrad hotbild där Sverige är en arena för en större konflikt med olika former av cyberattacker och hot mot informationssäkerheten i det digitaliserade samhället. NCSC skriver att mobiltelefoner, surfplattor och andra bärbara enheter är plattformar som genom cyberangrepp kan omvandlas till verktyg för inhämtning. Om de infekteras går mobiltelefoner att använda för att inhämta mycket individ om individen (e-post, kreditkort, planerade resor, bilder, meddelande, GPS-position med mera) samt använda för att på distans avlyssna omgivningen. Ett vanligt tillvägagångssätt att få in skadlig kod på mobiltelefoner är genom appar som oftast installeras från en tredje part. Utöver att inhämta personlig information eller att användas för avlyssning kan mobiltelefoner sprida infektioner vidare till nätverk som mobiltelefonen kopplas in på.

I årets rapport från Nationellt cybersäkerhetscenter (NCSC) "Cybersäkerhet i Sverige 2024" kvarstår de risker som lyftes förra året. Rapporten påtalar även att hoten fortsätter att öka, vilket understryker vikten av ett systematiskt, dynamiskt och långsiktigt säkerhetsarbete som inkluderar både tekniska lösningar och organisatoriska insatser. Ett bristande säkerhetsarbete kan få allvarliga konsekvenser. Röjande av känslig information kan skada individer, medan manipulation eller skador på system kan hota hela verksamheten.

I Sveriges Nationella strategi för cybersäkerhet 2025-2029 fastslås att Sverige länge dragit stor nytta av digitaliseringens möjligheter, men historiskt sett har cybersäkerhet ofta fått stå tillbaka för andra prioriteringar, vilket inte längre är ett alternativ. Dagligen utsätts myndigheter, företag och enskilda individer för cyberangrepp i varierande omfattning, och mycket talar för att hotet kommer fortsätta öka.

I Säkerhetspolisens lägesrapport 2024-2025 konstateras att Sveriges säkerhet fortsätter påverkas av en orolig omvärld. Genom att hacka individers mobiltelefoner och datorer kan främmande makt få tillgång till information med bäring på Sveriges säkerhet, politiskt beslutsfattande eller annan information som kan användas i kartläggnings- eller påverkans syfte.

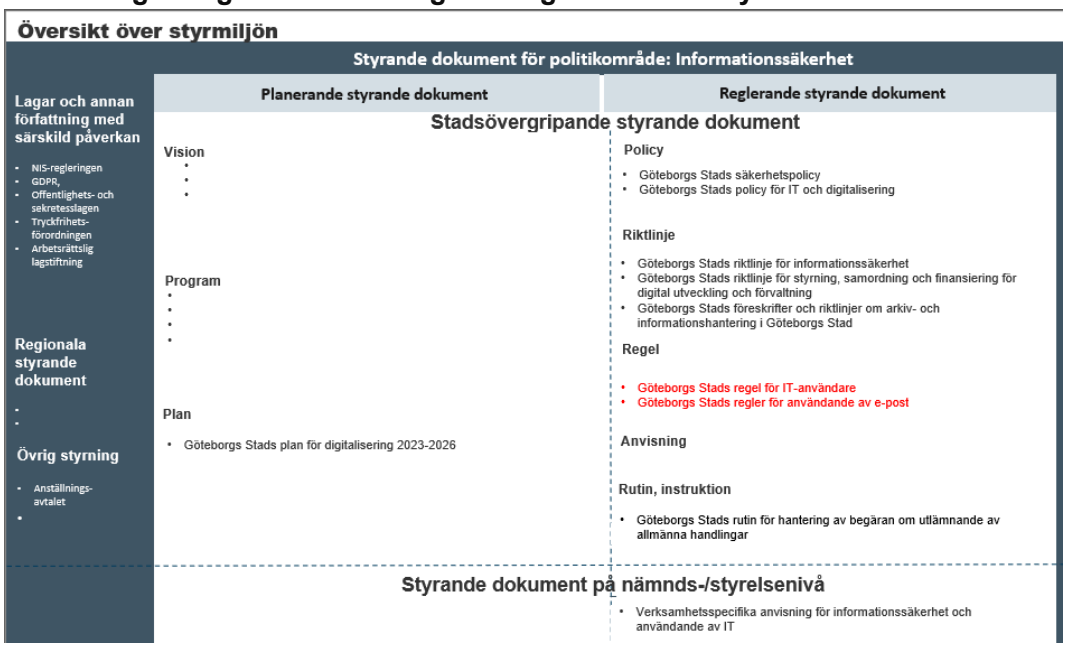
Revideringen har skett i dialog med förvaltningar, bolag och fackliga organisationer

Inom ramen för översynen har stadsledningskontoret fört dialoger med medarbetare som arbetar med informationssäkerhet på förvaltningar och bolag. Förvaltningar och bolag har efter dialog haft möjlighet att skicka in synpunkter på de föreslagna ändringarna. Det har även förts löpande dialoger med avdelningen för informationssäkerhet på förvaltningen för Intraservice samt andra berörda delar exempelvis digital infrastruktur. Utöver dessa dialoger har avstämningar skett med nätverk inom staden, såsom HR-chefsnätverk, nätverket för informationssäkerhet, och stadens dataskyddsombud. Ärendet har samverkats med den centrala samverkansgruppen (CSG) med fördjupad dialog med

facklig referensgrupp. Även koncernfackliga rådet har informerats och lämnat synpunkter.

Då översynen omgående visade på behov av revidering och ett tydliggörande av IT-användares ansvar har fokus för dialogerna framför allt handlat om hur staden kan möjliggöra den förändring som behöver ske. Dialogerna har visat på ett antal utmaningar med regeln som behöver hanteras för implementering och efterlevnad. Samtliga dialoger utgör underlag för stadsledningskontorets förslag och har på olika sätt arbetats in i ärendet. På sidan 14 framgår de delar som bemöts särskilt.

Revideringen utgår från såväl lagstiftning som andra styrande dokument



Göteborgs säkerhetspolicy syftar till att skapa en stadengemensam inriktning och samsyn på säkerhetsarbetet samt att tydliggöra ansvar och övergripande krav. Informationssäkerhet är ett område som inkluderas i Göteborgs Stads säkerhetsarbete.

Enligt **Göteborgs Stads policy för digitalisering och IT** ska Göteborgs Stad ha en digital miljö såsom infrastruktur, tjänster och funktioner med ändamålsenlig tillgänglighet, kapacitet, stabilitet och säkerhet.

I **Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning** ges nämnden för Intraservice ansvarar för förvaltning och utveckling av kommunkoncernens gemensamma digitala infrastruktur, samt att det finns ramverk/regler för stadens arkitektur och infrastruktur för nämnder och bolagsstyrelse att tillämpa. I det uppdraget ligger det att tillhandahålla en säker digital infrastruktur i linje med Göteborgs Stads riktlinje för informationssäkerhet.

Göteborgs Stads riktlinje för informationssäkerhet anger hur Göteborgs Stad ska arbeta med informationssäkerhet. Inom Göteborg Stad ska ett systematiskt och långsiktigt informationssäkerhetsarbete bedrivas. Göteborgs Stads metod för säker informationshantering bygger på ett antal steg där informationsägaren inleder med att klassificera information, genomför en riskanalys för att därefter vidta lämpliga organisatoriska, personrelaterade, fysiska och tekniska säkerhetsåtgärder.

I enlighet med vad som gäller för övrig verksamhet, är ansvaret för informationssäkerheten kopplat till ordinarie verksamhetsansvar. Det innebär att ansvarig nämnd/styrelse för en verksamhet också är ansvarig för att informationssäkerheten upprätthålls och efterföljs i denna verksamhet. Varje nämnd och styrelse ska säkerställa att det finns en förteckning över verksamhetens informationstillgångar (exempelvis appar), följa upp informationssäkerheten och vidta de åtgärder som krävs för att säkerställa att styrande dokument, lagar och andra regelverk inom informationssäkerhet efterlevs inom den egna verksamheten.

Göteborgs Stads riktlinje för personalförmåner syftar till att fastställa Göteborgs Stads personalförmåner i enlighet med kommunfullmäktiges beslut, 2022-01-27 §15, där det anges att det ekonomiska värdet på personalförmåner ska vara likvärdigt för alla medarbetare. Värdet fastställs årligen i kommunfullmäktiges budget. Förutom det förvaltningsgemensamma utbudet som består av friskvårdsbidrag, cykelförmån och personalstöd kan stadens medarbetare även erhålla rabatterat kollektivtrafikkort och gruppförsäkring.

Juridiska utgångspunkter

Som beskrivits är grunden för framtagandet av en ny regel att det finns ett behov av tydligare styrning i syfte att öka informationssäkerheten, både utifrån en förändrad omvärld och utifrån att det skett förändringar i lagstiftningen sedan nu gällande regler togs fram.

NIS-direktivet införlivades 2018 i svensk rätt genom införandet av lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagstiftningen har kompletterats av föreskrifter från bland annat Myndigheten för samhällsskydd och beredskap. NIS-regleringen omfattar i dagsläget leverantörer av samhällsviktiga tjänster inom sju sektorer, bland annat hälso- och sjukvårdssektorn.

I december 2022 antog Europaparlamentet och rådet NIS2-direktivet. NIS2-direktivet ersätter det tidigare NIS-direktivet och skärper kraven på systematiskt informationssäkerhetsarbete i syfte är att uppnå en högre cybersäkerhet. Utredningen som haft i uppdrag att se över vilka anpassningar av svensk lagstiftning som är nödvändiga för att genomföra NIS2-direktivet har presenterat sina slutsatser och förslag i delbetänkandet SOU 2024:18, Nya regler om cybersäkerhet. Enligt förslaget ska nuvarande lagstiftning ersättas av en ny lag om cybersäkerhet och en förordning om cybersäkerhet. Till skillnad från vad som gäller enligt nu gällande regelverk innebär förslaget till ny lagstiftning att kommunens verksamhet omfattas i sin helhet.

Ett annat område som är viktigt för utformningen av regeln är de förutsättningar som regleras inom arbetsrätten. Medarbetare i staden får IT-resurser som till exempel dator och mobiltelefon till låns för att utföra sitt arbete. Arbetsgivaren har normalt inget behov av att bereda sig tillgång till medarbetares IT-resurser men det finns situationer när detta kan vara nödvändigt. Arbetsgivarens möjlighet att bereda sig tillgång till medarbetares IT-resurser vid till exempel oplanerad frånvaro eller för att genomföra kontroller vid misstanke om och utredning av oegentligheter betraktas primärt som åtgärder grundade i den s.k. arbetsledningsrätten. Arbetsgivarens arbetsledningsrätt är enligt äldre praxis en allmän rättsgrundsats som gäller även utan stöd i kollektivavtal.

Möjligheten att genomföra kontroller härleds alltså inte från lagstiftning utan från den underliggande arbetsledningsrätten, vilken innebär att arbetsgivaren bestämmer över arbetets utförande och även över arbetsplatsen och dess utrustning.

Arbetsgivarens arbetsledningsrätt kan emellertid inte utövas oinskränkt. Av praxis följer att arbetsgivaren inte får utöva sin rätt i strid med lag eller god sed på arbetsmarknaden. En förutsättning för att arbetsgivaren ska få kontrollera medarbetares IT-resurser är att medarbetarna fått information om vilka kontroller som kan komma att ske och kontrollerna får inte vara mer ingripande än nödvändigt. Vid en bedömning av vilka åtgärder som kan anses motiverade och proportionerliga i det enskilda fallet måste medarbetarens rätt till integritet beaktas.

Alla medarbetare har en grundläggande rätt till skydd för sin kommunikation och sitt privatliv. Rätten till skydd för privatlivet skyddas bland annat i olika internationella rättsakter som artikel 8 i Europakonventionen om mänskliga rättigheter (EKMR). En arbetsgivare får normalt inte ta del av innehållet i en medarbetares privata filer eller e-postmeddelanden. Undantag från detta gäller emellertid vid till exempel misstanke om oegentligheter såsom brott, allvarliga avvikelser mot interna regler och riktlinjer i tjänsten, brott mot anställningsavtalet eller annat illojalt beteende. I de fall nödvändiga kontroller innebär att arbetsgivaren behandlar uppgifter om medarbetare ska arbetsgivaren följa dataskyddsförordningen.

I de delar som gäller IT-användarens hantering av den egna e-posten grundar sig regeln i flera delar på bestämmelser i tryckfrihetsförordningen (1949:105) och offentlighets- och sekretesslagen (2009:400). Ett e-postmeddelande som kommer in till en medarbetares e-postbrevlåda och som rör myndighetens verksamhet är att anse som en inkommen handling hos myndigheten. Mot bakgrund av reglerna i tryckfrihetsförordningen och offentlighets- och sekretesslagen måste inkomna e-postmeddelanden läsas löpande samt eventuellt tas om hand för registrering och ytterligare handläggning. Justitieombudsmannen har uttalat att det inte är tillräckligt att aktivera ett frånvaromeddelande och avstå från att hantera inkomna e-postmeddelanden varför var och en antingen själv behöver kontrollera sin e-post vid frånvaro eller delegera e-posten till en kollega (se till exempel JO:s beslut dnr 2668–2000 och dnr 3987–2009). Beskrivningar av detta finns även i Göteborgs Stads rutin för hantering av begäran om utlämnande av allmänna handlingar. Om en medarbetare är oplanerat frånvarande är det ett ansvar för myndigheten att säkerställa att de krav som ställs i tryckfrihetsförordningen och offentlighets- och sekretesslagen upprätthålls.

Utifrån beslutet i kommunstyrelsen om återremiss har den juridiska utredningen i ärendet kompletterats. I bilaga 5, PM - rättslig reglering, finns både en mer utförlig beskrivning av de juridiska förutsättningar som beskrivits ovan och en analys av konsekvenser av privat användning av Göteborgs Stads digitala arbetsverktyg.

Hur det ser ut i staden idag

Intraservice tjänstekatalog för mobila enheter innehåller tjänsteerbjudandena Staden-mobil och Staden-surfplatta som möjliggör för användare att på ett säkert sätt ta del av information inom Göteborgs Stad samt använda de applikationer som krävs för tjänsten/uppdraget. Med tjänsteerbjudandena erhålls också andra säkerhetshöjande funktioner, till exempel möjligheten att låsa, återställa eller radera en förlorad enhet, central administration av uppdateringar av operativsystem och arbetsrelaterade appar. Till

tjänsten hör även Göteborgs Stads app-butik där användaren kan ladda ner verksamhetens appar samt publika appar som verksamheten valt att publicera för sina användare. Via Serviceportalen beställs de appar som ska publiceras för verksamheten i app-butiken. Tjänsteerbjudandena Staden-mobil och Staden-surfplatta tillåter idag användaren att utöver de appar som tillhandahålls genom Göteborgs Stads app-butik, även installera appar från Apple Store och Google play butik.

Intraservice administrerar ca femtiotusen mobila enheter, vilket bedöms utgöra ca 70 % av stadens enheter. Resterande enheter ägs och administrerats av respektive förvaltning eller bolag. Det är svårt att göra en uppskattning av hur många av dessa som används även för privat bruk. En omständighet som talar för att det kan vara en betydande del är att det de senaste åren, i strid med vad nuvarande regel säger, i princip har varit tillåtet att använda den mobiltelefon som staden tillhandahåller för privata ändamål.

Intraservice utredning av privat användning av Göteborgs stads digitala arbetsverktyg:

Som en del av utredningen enligt kommunstyrelsens återremiss har Intraservice utrett möjligheterna att tillåta privat användning av mobila enheter (SLK-2024-00392). En fullständig utredning av samtliga IT-resurser bedömdes kräva ytterligare resurser, varför stadsledningskontoret prioriterade möjligheter till privat användning av mobila enheter.

Utredningen visar att Göteborgs Stad i slutet av 2024 har cirka 45 000 mobiltelefoner i bruk, varav 36 000 är hanterade genom Intraservice och omfattas av grundläggande säkerhetsfunktioner. Ytterligare 13 500 enheter använder Office 365 utan att vara hanterade, vilket innebär ökad säkerhetsrisk. Totalt används över 1 700 appar via ”Stadens Appar”, många av dem publika utan avancerade säkerhetsinställningar.

Intraservice ser att det ur ett tekniskt perspektiv finns möjligheter att öka skyddet för Göteborgs Stads information på ett sådant sätt att privat användning av mobila digitala arbetsverktyg är möjlig och att samtidigt uppnå en adekvat skyddsnivå utifrån vad som anges i Göteborgs Stads riktlinje för informationssäkerhet samt lagar och förordningar. Vidare anger Intraservice att en förutsättning för att åtgärderna ska vara genomförbara krävs att nämnden får ett tydligare mandat i relation till övriga förvaltningar och bolag samt tydliggörande av ansvarsförhållanden och personuppgifter vid privat användning. Det kommer även innebära förhöjda krav på alla Göteborgs Stads verksamheter, som till exempel regelverk samt utbildning och information till IT-användare. Samtidigt anger utredningen att ett möjliggörande av privat användning innebär en ökad riskbild, vilket behöver tas i beaktning då varken tekniska eller administrativa åtgärder kommer att kunna garantera att användare inte använder Göteborgs Stads information felaktigt eller utsätter den för hot, oavsett om det sker avsiktligt eller oavsiktligt.

Tekniska lösningar och åtgärder:

För att möjliggöra säker privat användning föreslår Intraservice flera åtgärder:

- **Staden-mobil:** En tjänst för central hantering av mobila enheter som möjliggör fjärrlåsning, kryptering, inventering och uppdateringar. Tjänsten föreslås bli obligatorisk vid beställning av nya enheter.
- **Mobile Threat Defense (MTD):** System för realtidsövervakning av de mobila enheterna och skydd mot skadlig kod, nätfiske, sårbarheter och osäkra nätverksanslutningar.

- **Skärpta säkerhetskrav:** Exempelvis krav på sexsiffrig PIN-kod, teknisk separering av arbets- och privatdata, samt säkra VPN-anslutningar för arbetsappar.
- **Ramverk för appar:** Ett ramverk föreslås för upphandling och utveckling av appar så att dessa möjliggör tekniska säkerhetsåtgärder.
- **Central livscykelhantering:** Befintlig funktion för datorprogram föreslås utökas till att även omfatta mobila appar för att säkerställa löpande uppdateringar och hantering av sårbara applikationer.

Intraservice bedömning är att privat användning medför risker såsom skadlig kod, informationsläckage och förlorade mobila enheter. Ett strikt förbud riskerar däremot att leda till att medarbetare använder privata mobila enheter i tjänsten genom att ladda ner stadens appar på dessa, vilket försvårar kontroll och ökar riskerna ytterligare.

Förslaget till reviderad regel innehåller förtydliganden och skärpningar

Som framgår av ärendet är Göteborgs Stads regel för IT-användare i behov av revidering på grund av ett mer allvarligt omvärldsläge, ökad digitalisering samt ändrad och tillkommen lagstiftning på området. Hanteringen av stadens IT-resurser utgör en stor del i det systematiska informationssäkerhetsarbetet, vilket ställer höga krav på tydlig styrning inom området.

Allmänt om regeln

Syftet med regeln är att redogöra för det ansvar och de åtaganden som gäller för IT-användare i Göteborgs Stad vid användning av stadens IT-resurser, såsom e-post, datorer, mobila enheter och kringutrustning. Syftet är inte att utgöra information till IT-användare om hur staden hanterar deras personuppgifter. Denna informationsplikt är en fråga för respektive personuppgiftsansvarig verksamhet att omhänderta.

Samtliga nämnder och styrelser omfattas av regeln. I regeln definieras vem som omfattas av begreppet IT-användare, vilket är Göteborgs Stads anställda, förtroendevalda, entreprenörer, inhyrd personal, konsulter och leverantörer som arbetar i och med stadens IT-resurser. Exempel på grupper som inte omfattas är skolelever och brukare inom till exempel daglig verksamhet eller som bor på kommunens boenden. En reglering av dessa användares IT-säkerhet är ett ansvar för respektive verksamhet, där den stadenövergripande regeln kan vara en utgångspunkt.

Tillåten användning av stadens IT-resurser

Privat användning medför ökade säkerhetsrisker för staden. En obehörig som skaffar sig tillgång till en IT-användares inloggningsuppgifter inom en verksamhet kan leda till att flera verksamheter påverkas negativt och drabbas av IT-avbrott. Genom att endast använda stadens IT-resurser som arbetsredskap minimeras Göteborgs Stads risker att information sprids till obehörig eller att stadens information blir otillgänglig.

Stadsledningskontoret har tydliggjort och skärpt regeln vad gäller privat användning av stadens IT-resurser i syfte att stärka säkerhetsperspektivet. I nuvarande formulering står att privat användning endast får ske i mycket begränsad omfattning och inte påverka ordinarie arbetsuppgifter eller inverka menligt på stadens IT-resurser i form av kostnader, lagringsutrymme, prestanda etcetera. Förslaget till ny formulering lyder i stället som följande ”Göteborgs Stads IT-resurser får endast användas som arbetsredskap och utifrån vederbörandes roll och arbetsuppgifter.

Privat användning får inte ske, annat än i ytterst begränsad omfattning, eftersom det kan medföra onödiga säkerhetsrisker och ökade kostnader för Göteborgs Stad".

Med begreppet privat användning avses sådan användning av stadens digitala arbetsverktyg som sker utanför anställningen eller det uppdrag som en person har för stadens räkning. Det spelar ingen roll var IT-användaren befinner sig eller vilken tid på dygnet det är, det viktiga är om han eller hon utför uppgifter för stadens räkning. Användning av stadens digitala arbetsverktyg som sker inom ramen för ett fackligt förtroendeuppdrag gentemot arbetsgivaren är relaterat till anställningen och ses inte som privat användning. Vid oklarheter kring vad som avses med användande utifrån roll och arbetsuppgifter bör frågan hanteras av respektive verksamhet.

Stadsledningskontorets bedömning är att det inte är möjligt att helt begränsa det privata användandet. Ett absolut förbud skulle vara svårt att kontrollera och det kan även finnas tillfällen då det är rimligt att använda en IT-resurs i egenskap av privatperson. Sådana tillfällen kan vara att IT-användare behöver vara nåbara för inkommande privata samtal, exempelvis från förskola eller vården. Ett annat exempel kan vara att använda IT-resurser för att planera resor till och från arbetsplatsen. Exempel som inte bedöms ingå i ytterst begränsad omfattning är installation och användning av appar eller program för privat bruk, användning av privata sociala medier, streamingtjänster eller privata e-postkonton.

Regeln har även skärpts vad gäller användning utomlands. Att ta med Göteborgs Stads IT-resurser utomlands innebär större säkerhetsrisk eftersom de flesta öppna nätverk på hotell, flygplatser, restauranger saknar kryptering. Många öppna nätverk kräver inte autentisering och alla användare använder samma lösenord för att logga in. Det innebär att vem som helst i närheten kan ta del av den information som skickas och tas emot. IT-resurser ska därför inte kopplas upp på offentliga nätverk. Regeln tydliggör att IT-resurser enbart ska tas med utomlands efter behovs- och riskbedömningar.

Nedladdning av programvaror och appar

När nuvarande regel beslutades 2009 var användning av appar på mobila enheter ytterst begränsat varför hantering av dessa inte har reglerats. Vissa program och appar har koppling till cyberkriminella eller främmande makt som via skadlig kod, utpressningsvirus eller avlyssningsfunktioner kan skada staden. Installation av program för datorer styrs sedan tidigare antingen av nämnden för Intraservice eller verksamheternas egna IT-organisationer. Appar styrs inte på samma sätt utan IT-användarna kan själva ladda ner även från andra plattformar än stadens, vilket utgör en stor säkerhetsrisk för en stad av Göteborgs storlek med många IT-användare.

Stadsledningskontorets förslag till regel innebär att IT-användare har ett ansvar för att inte ladda ner appar som inte är godkända av stadens tjänsteleverantörer eller av respektive förvaltnings eller bolags verksamhetsspecifika IT-organisation. Tydligare styrning innebär inte att IT-användare ska begränsas i sin användning av appar som behövs för vederbörande roll och arbete, förutsatt att appen inte innebär en säkerhetsrisk för Göteborgs Stad. Regeln tydliggör att det är respektive verksamhet som behovs- och riskbedömer de verksamhetsspecifika apparna.

Utifrån risker som framkommit i den fördjupade utredningen har stadsledningskontoret i regeln även tydliggjort att det inte är tillåtet att ladda ner arbetsrelaterade appar och programvaror till privata enheter. I dessa fall är stadens information än mer oskyddad, vilket innebär stora risker ur både säkerhets- och integritetsperspektiv.

Tillgång till IT-resurser vid frånvaro samt tillgång och kontroll vid oegentligheter
I förslaget till ny regel beskrivs två situationer när arbetsgivaren kan komma att bereda sig tillgång till och genomföra kontroller av en medarbetares IT-resurser. Som en övergripande förutsättning anges att bedömningen av om en åtgärd är motiverad alltid ska ske med utgångspunkt i gällande lagar, regler och god sed. Med den utgångspunkten beskrivs sedan två typsituationer. Den första situationen är tillgång vid medarbetarens frånvaro och här avses oplanerad frånvaro, avslutad anställning eller frånvaro utan delegering av den individuella e-postlådan. I det här fallet är det primärt de lagkrav som ställs på myndigheten när det gäller hanteringen av allmänna handlingar som motiverar åtgärder ur ett rättsligt perspektiv. Den andra situationen är tillgång och kontroll vid misstanke om och utredning av oegentligheter samt misstanke om och utredning av informationssäkerhetsincident.

I regeln tydliggörs även att åtgärderna ska vara proportionerliga och ske med beaktande av den enskildes integritet.

Bakgrunden till skärpningen vad gäller privat användning är att detta medför ökade säkerhetsrisker för staden. Ytterligare en aspekt är emellertid att det finns situationer vid oplanerad frånvaro då Göteborgs Stad kan behöva skaffa sig tillgång till en IT-användares nyttjade IT-resurser, såsom individuell e-postlåda eller mobila enheter, och en sammanblandning av privat och arbetsrelaterad information kan i dessa fall få negativa konsekvenser för den personliga integriteten.

Säkerhetsuppdatering och skadliga länkar
En säkerhetsuppdatering innebär att leverantören har identifierat en eller ett flertal sårbarheter som måste åtgärdas direkt. Sårbarheter kan utnyttjas av kriminella och orsaka skada för Göteborgs Stads verksamheter. Regeln tydliggör att det är IT-användarens ansvar att installera säkerhetsuppdateringar så snart det kommer till IT-användarens kännedom att sådan finns. Genom den reviderade regeln uppmärksammas även IT-användaren på inte att klicka på konstiga och skadliga länkar. Om IT-användaren av misstag råkat klicka på en länk eller orsakat annan skada ska detta rapporteras omgående enligt verksamhetens rutin för informationssäkerhetsincidenter.

Information som flyttats till andra styrande dokument
Vid översynen av de två reglerna framkom att de i vissa delar innehöll reglering som inte avser IT-användarnas ansvar gentemot stadens IT-resurser. Exempel är skrivningarna om hantering av inkomna allmänna handlingar, immaterialrättsligt skyddad information och informationsspridning med hjälp av IT. Skrivningarna utgår från regeln och omhändertas i stället på annat sätt.

Två styrande dokument blir ett
Stadsledningskontoret har i detta ärende reviderat regel för IT-användare och även inarbetat innehåll från regel för e-post. Stadsledningskontoret konstaterar att e-post utgör en IT-resurs och bedömer det därmed lämpligt att hantera dessa gemensamt. Information som tidigare fanns i Göteborgs Stads regler för e-post finns nu i huvudsak under avsnittet ”Använda och sköta sin individuella e-postlåda”. De förändringar som skett i relation till nuvarande regel är enbart av redaktionell karaktär.

Revideringen av regeln har visat på utmaningar som behöver hanteras
De dialoger som har förts inom ramen för revideringen har visat att en tydligare reglering är nödvändig och önskvärd, men att det finns aspekter som försvårar implementering och

efterlevnad och som behöver hanteras. Översynen har visat att förvaltningar och bolag har valt olika tekniska och organisatoriska lösningar för sina respektive IT-resurser. Detta innebär att förutsättningarna för att omedelbart efterleva regeln varierar och att respektive organisation behöver anpassa sina åtgärder utefter förutsättningarna.

En utmaning som lyfts är att den reviderade regeln inte i så stor omfattning skiljer sig från den förra, men att omvärldsläget och nya digitala arbetssätt kräver ett förändrat beteende gällande användning av stadens IT-resurser i praktiken. Risken finns således att följsamheten även till den reviderade regeln brister då det för medarbetare kan tyckas otydligt vad förändringen egentligen innebär, exempelvis vad gäller den reviderade skrivningen om att arbetsgivarens IT-resurser bara får användas privat i ytterst begränsad omfattning. Även skrivningarna om hur IT-resurser får användas utomlands riskerar att skapa osäkerhet hos stadens IT-användare. Samtidigt som det konstateras att revideringen inte är så omfattande så lyfts risken att anställda kan uppleva revideringen som en försämring, då privat användande av exempelvis mobiltelefoner har varit sanktionerat i praktiken. I dessa avseenden efterfrågas kommunikationsinsatser, kompetenshöjande material och ett ansvar för nämnder och styrelser att löpande arbeta med rutiner som förenklar IT-användarnas möjligheter att göra rätt.

Inom ramen för implementering av regeln så kommer stadsledningskontoret att genomföra kommunikationsinsatser och ta fram ett exempelvis ett gemensamt APT - material. Som en del i implementeringen och uppföljningen kommer bland annat stadens nätverk för informationssäkerhet bestående av representanter från alla stadens förvaltningar och bolag involveras, vilket möjliggör samordning av kommunikations- och utbildningsinsatser. Övriga insatser för att stärka informationssäkerheten är ett ansvar som åligger samtliga nämnder och styrelser i enlighet med riktlinjen för informationssäkerhet, vilket kan ske med stadsledningskontorets kommunikationsinsatser som grund. Information om regeln bör med fördel även ingå i nämnders och styrelsers rutiner vid nyanställning och utlämnande av IT-resurser, för att på så sätt stödja efterlevnad även bland nyanställda.

En konsekvens som framkommit i arbetet är att reglerna om hur IT-användare ska använda och sköta sin individuella e-postlåda under nuvarande omständigheter är svåra att leva upp till för de fackligt förtroendevalda. I dagsläget är det ett flertal av dessa som enbart har stadens e-post som kommunikationskanal, även inom det fackliga uppdraget. Möjligheten för dessa att delegera sin e-post vid planerad frånvaro är begränsad, då andra medarbetare inom arbetsplatsen inte ska få information som rör det fackliga uppdraget. Dialogerna visar att vissa fackförbund redan har säkerställt att deras förtroendevalda har e-postadresser kopplat till sitt fackliga uppdrag, men att detta inte gäller för alla. Vid dialogerna framkommer även att problematiken inte bara berör IT-resursen e-post, utan även innefattar frågor kopplat till lagring av information och behandling av personuppgifter. Stadsledningskontoret kommer att hantera denna fråga separat tillsammans med fackliga organisationer för att möjliggöra en långsiktig och ändamålsenlig lösning för den problematik som har uppmärksammats.

Vid dialogerna lyfts en oro för att samtliga nämnder och styrelser inte har de förutsättningar som krävs, i form av systemstöd och rutiner, för att underlätta för IT-användare att efterleva regeln omedelbart. Ett exempel är systemstöd som krävs för att användare inte ska riskera att ladda ner skadliga eller icke nödvändiga appar och programvaror på de mobila enheterna. Nämnden för Intraservice erbjuder en tilläggstjänst

i sin befintliga tjänstekatalog som möjliggör för användare att på ett säkert sätt använda de appar som krävs för anställningen. Denna tjänst gäller dock enbart de mobila enheter som administreras av Intraservice. Nämnder och styrelser som har denna tjänst behöver ta fram rutiner för att hantera de verksamhetsspecifika appar som ska få användas. För de nämnder och styrelser som inte använder Intraservice tjänsteerbjudande så behövs en kartläggning av vilka appar som bedöms nödvändiga för verksamheten göras och företrädelsevis ett systemstöd införas som minimerar risken för IT-användare att göra fel. En angränsande fråga är att medarbetare, utifrån de tekniska lösningar som finns för närvarande, ibland behöver identifiera sig via sitt privata Bank-Id. Detta är en fråga som även diskuteras nationellt utifrån behovet av lösningar för e-legitimering i tjänsten.

Vid dialogerna lyfts även risken att stadens IT-användare i större utsträckning kommer att känna sig övervakade av arbetsgivaren då reglerna tydliggör arbetsgivarens rätt till kontroller och vid vilka tillfällen detta kan ske. Stadsledningskontoret har beaktat den här risken i arbetet med revideringen och tydliggjort i regeln att kontroller enbart får ske vid konkreta misstankar, att de kontrollerande åtgärderna ska vara proportionerliga och att medarbetarens personliga integritet ska beaktas vid bedömningen av vilka åtgärder som kan anses motiverade i det enskilda fallet. Den övervakning som berörs i regeln innebär systematisk övervakning av nätverkstrafik för att identifiera hot, förhindra dataintrång, felsöka problem på nätverk, identifiera överbelastning med mera och inte övervakning av enskilda personer. Vid identifierad oegentlighet inom Intraservice tjänsteleveranser som rör en specifik användare, eller där användaren är fokuset i oegentligheten, kontaktas närmste chef för att säkerställa om orsaken till larmet ligger inom ramen för användarens ordinarie arbetsuppgifter eller inte. Hur dessa identifierade oegentligheter sedan hanteras i relation till IT-användaren är en fråga för respektive nämnd och styrelse att ha rutiner för.

Förvaltningar och bolag i dag har olika interna rutiner, anvisningar och instruktioner för hur och i vilken omfattning användarna kan nyttja resurserna privat. Det är därmed svårt att på en övergripande nivå redogöra för den föreslagna regeln kommer att påverka olika yrkesgrupper. En konsekvens av förändringen som lyfts är att medarbetare kan behöva bära två telefoner under arbetsdagen samt att möjligheterna till kontinuerlig omvärldsbevakning minskar. Vissa har även lyft att det kan bli svårare att kontakta medarbetare utanför arbetstid, exempelvis när lediga pass behöver tillsättas. Dialogerna framhåller även arbetstagarens rätt att vara ledig och inte alltid vara nåbar utanför tjänsten. Dialogerna visar att, beroende av nuvarande rutiner och arbetssätt i olika yrkesgrupper, kan dessa behöva omvärderas i syfte att efterleva regeln.

Samtidigt vittnar i princip alla dialoger inom ramen för ärendet om att de risker som en privat användning medför, både vad gäller den personliga integriteten och informationssäkerheten, överväger de eventuella nackdelar som förändringen kan medföra.

Omvärldsbevakning

Inom säkerhetsområdet är det svårt att jämföra sig med andra kommuner och regioner eftersom alla utifrån egna riskbedömningar måste vidta åtgärder för att minska sina säkerhetsrisker. Förändringar i säkerhetsläget sker fort och nya sårbarheter upptäcks varje dag. Alla kommuner måste arbeta både förebyggande och agera på incidenter för att stärka sitt skydd mot ovälkomna avbrott i IT-miljön. De kommuner som tillfrågades (Kungsbacka kommun, Solna Stad och Malmö Stad) arbetar med övervakning och kontroll av IT-resurser.

Gällande privat användning tillåter dessa kommuner privat användning av IT-resurser i mycket begränsad omfattning, men det får inte påverka kostnader, inverka på arbetet, prestanda eller säkerheten. Någon av de tillfrågade kommunerna har även styrning av appar redan på plats. De upplyser även sina medarbetare om arbetsgivarens rätt till stadens IT-resurser vid frånvaro och vid oegentligheter.

Under beredningen av återremissen har stadsledningskontoret varit i kontakt med fler kommuner om hur de har reglerat privat användning av digitala resurser. Stockholms stad har stadengemensamma policys och riktlinjer gällande informationssäkerhet utifrån vilka respektive förvaltning och bolag ska ta fram egna riktlinjer för användandet av de anställdas telefoner. Den centrala rekommendationen är att telefonen och datorn endast ska användas arbetsrelaterat. Detsamma gäller många andra kommuner, vars regler i princip liknar stadsledningskontorets förslag, även om praxis har utvecklats åt ett sanktionerande av privat användning. Stadsledningskontoret har även fått frågor från kommuner som ser över möjligheterna att, i syfte att stärka informationssäkerheten, uppdatera och tydliggöra reglering av privat användning.

Stadsledningskontorets bedömning

Göteborgs Stad är en stor stad med många IT-användare och flera samhällsviktiga verksamheter. Detta innebär en stor risk och ställer höga krav på informationssäkerhetsarbetet. Översynen av de styrande dokumenten inom informationssäkerhet visade därmed på ett behov av revidering för att öka stadens informationssäkerhet. Samtidigt visade översynen att de faktiska behoven av revidering var marginella men att det sedan de nuvarande reglerna antogs har utvecklats en tolkning och praxis kring användande av stadens IT-resurser som inte är ändamålsenlig utifrån dagens utmaningar. När nuvarande reglering togs fram var säkerhetsläget annorlunda och stadens IT-resurser användes i mer begränsad omfattning. Idag är säkra digitala system en förutsättning för att medarbetare ska kunna utföra sina arbetsuppgifter, vilket kräver nya arbetssätt avseende säkerhet och hantering av IT-resurser.

Översynen och revideringen har skett i dialog med förvaltningar, bolag och fackliga organisationer. Dialogerna har visat på en samsyn i behovet av revideringen men att förutsättningarna för implementering kan förbättras och för närvarande skiljer sig åt mellan olika nämnder och styrelser. Trots detta bedömer stadsledningskontoret att det är väsentligt att användandet av stadens IT-resurser regleras tydligare då de risker som följer av en bristande informationssäkerhet är allvarliga.

Regeln syftar till att tydliggöra hur IT-användare får använda stadens IT-resurser. Som sådan bedöms regeln kunna börja gälla omedelbart då det i princip handlar om ett ändrat agerande. Samtidigt visar arbetet med revideringen att ett förändrat beteende bör stödjas genom att nämnder och styrelser vidtar åtgärder för att underlätta för stadens IT-användare att efterleva regeln. Åtgärderna är beroende av verksamhetens nuvarande tekniska och organisatoriska systemlösningar, men övergripande bedöms dessa handla om tydlig kommunikation, höjd kompetens om informationssäkerhet och ett arbete med interna rutiner. Stadsledningskontorets bedömning är således att regeln bör träda i kraft först 2026-01-01, vilket bedöms ge nämnder och styrelser tid att arbeta med de mest prioriterade åtgärderna.

Inför regelns ikraftträdande bedömer stadsledningskontoret det rimligt att nämnder och styrelser har gjort en kartläggning över godkända appar utifrån verksamhetens uppdrag,

tagit fram och implementerat rutiner för hantering av appar och kommunicerat detta med sina IT-användare. Stadsledningskontoret bedömer att detta ingår i respektive nämnds och styrelses ansvar enligt Göteborgs Stads riktlinje för informationssäkerhet, som är att säkerställa att verksamheten har en förteckning över sina informationstillgångar, exempelvis appar. Därmed bedöms inget särskilt uppdrag för detta vara nödvändigt. Med tiden bedöms det även rimligt att tekniska systemlösningar finns på plats för att stödja regeln inom respektive IT-organisation, oavsett om verksamheten har valt Intraservice tjänsteerbjudanden eller en egen hantering av mobila tjänster.

Att staden idag saknar ett övergripande och gemensamt arbetssätt för styrning av appar är en komplicerande faktor. Stadsledningskontoret kommer se över möjligheten att tydligare styra inköp av IT-resurser, såsom mobila enheter, för att en större andel av dessa ska hanteras av Intraservice. Den fördjupade utredningen visar att allt fler av stadens enheter har tjänsten staden-mobil, men att det fortfarande finns mobila enheter som riskerar att inte ha det grundläggande skydd som tjänsten innebär. Även detta är en försvårande omständighet för att kunna implementera de tekniska åtgärder som föreslås i utredningen. Stadsledningskontoret konstaterar att det finns åtgärder om kan vidtas för att öka säkerheten för stadens IT-resurser samt att det som framkommer avseende mobila enheter inte ingår i årlig analys för 2026. Oaktat om kommunfullmäktige beslutar att tillåta privat användning eller anta förslaget till regel, så bedömer stadsledningskontoret det av yttersta vikt att nämnden för Intraservice fortsätter arbeta för en högre digital säkerhet inom ramen för sitt grunduppdrag. Frågorna bör omhändertas i arbetet med årlig analys- samt budgetförutsättningar.

Kommunstyrelsen ansvarar genom uppsiktsplikten för att utvecklingen går åt rätt håll och att nämnder och styrelser efterlever stadens gemensamma styrning. Stadsledningskontoret kommer inom ramen för implementeringen ta fram övergripande kommunikationsmaterial och kompetenshöjande insatser, samt i övrigt vara ett stöd för förvaltningar och bolag. Detta bedöms kunna påbörjas under hösten 2025 för att ge IT-användare tid att förbereda sig innan regelns ikraftträdande. Stadsledningskontoret bedömer att en uppföljning av regelns efterlevnad och nödvändiga anpassningar bör genomföras ett år efter regelns ikraftträdande.

Göteborgs Stads plan för digitalisering 2023-2026 innehåller mål och insatser som ska bidra till att skapa förutsättningar för det fortsatta arbetet med digitalisering i staden. I samband med föreliggande revidering bedöms insatsen om översyn av riktlinjen för informationssäkerhet, samt angränsande styrande dokument, vara omhändertagen.

Regeln syftar till att fastställa och redogöra för det ansvar och de åtagande som gäller för IT-användare i Göteborgs Stad. En tydligare reglering bedöms underlätta för användarna att göra rätt och minska risken för informationssäkerhetsincidenter som kan skada stadens verksamheter, medarbetare, brukare och invånare.

Stadsledningskontoret bedömer även att de omarbetade reglerna är en förutsättning för att efterleva lagkrav, minska stadens säkerhetsrisker och möta de utmaningar som kommer med digitaliseringen kring bland annat tillgänglighet, informations- och cybersäkerhet. Att arbeta med informationssäkerhet och användning av IT-resurser är en förebyggande åtgärd för att kunna upprätthålla Göteborgs Stads verksamheter i ett förändrat omvärldsläge som kräver robustare skydd.

Sammantaget bedöms de ändringar och tillägg som gjorts i regeln, samt sammanslagningen av två styrande dokument, bidra till ökad användbarhet och en tydligare styrning med ökade förutsättningar för efterlevnad.

Sedan ärendet behandlades av kommunstyrelsen i juni 2024 har ett flertal rapporteringar skett om ökade säkerhetshot och sårbarheten i verksamhetskritiska system. I enlighet med återremissyrkandet från kommunstyrelsen har stadsledningskontoret kompletterat utredningen med konsekvenser av privat användning av Göteborgs Stads digitala arbetsverktyg med hänsyn till säkerhet, ekonomi och juridik.

Utredningen visar att det finns tekniska åtgärder som kan införas för att öka säkerheten för mobila enheter i de fall privat användning tillåts. Ur ett informationssäkerhetsperspektiv förutsätts att dessa tekniska åtgärder kompletteras med ytterligare organisatoriska åtgärder, samt ett förändrat beteende hos stadens IT-användare. Samtidigt visar utredningen att det trots ett införande av förslagna åtgärder finns tydliga risker avseende säkerheten.

Ur ett ekonomiskt perspektiv bedömer stadsledningskontoret att ett tillåtande av privat användning innebär kostnader för införande och förvaltning. Det kommer även krävas vidare utredningar av vissa åtgärder, vars ekonomiska konsekvenser i dagsläget inte kan uppskattas. Kostnaderna skulle främst tillfalla nämnden för Intraservice och behöver finansieras via kommunbidrag eller ökad självfinansiering av kunderna. Oavsett finansieringsmodell kommer kostnaderna att öka för stadens nämnder och styrelser, i form av framtagande av styrdokument, organisering för upprätthållande samt utbildning av IT-användare. Övriga tillkommande administrativa kostnader för nämnder och styrelser avser rutiner för hanteringen av frågan om förmånsbeskattning. Utredningen visar även att en privat användning är förknippat med risker avseende personuppgifts-, informationssäkerhets- och cybersäkerhetsincidenter, vilket i sig kan innebära höga sanktionsavgifter för nämnder och styrelser. Därtill kommer risken för allvarliga IT-avbrott där erfarenheten för utsatta kommuner och myndigheter varit avsevärda ekonomiska förluster.

Utredningen visar även att de tekniska åtgärder som behöver vidtas är förknippade med ökade juridiska risker. Det övervakningssystem som föreslås för de mobila enheterna i syfte att öka säkerheten möjliggör inte särskiljning av privat datatrafik från den arbetsrelaterade. Detta skulle innebära att stadens IT-användare även övervakas i egenskap av privatperson och i händelse av en oegentlighet kan arbetsgivaren behöva ges tillgång till privat information. Ytterligare en slutsats ur juridiskt perspektiv är att nämnder och styrelser i olika situationer kan komma att behandla privata personuppgifter om en IT-användare, eller uppgifter om andra externa personer, och då få ett personuppgiftsansvar för dessa behandlingar. Eftersom nämnden/styrelsen inte kommer ha kontroll över vilken slags uppgifter IT-användaren hanterar på sina mobila enheter kan detta även inkludera känsliga personuppgifter.

I ärendet hänvisas till det ökade beroendet av säkra digitala resurser för stadens verksamheter. Det ökade beroendet och den ökade sårbarheten gäller även som privatperson, där allt fler ärenden sker digitalt och inte sällan genom utländska appar. Även om riskerna i viss utsträckning kan motverkas av till exempel tekniska säkerhetsåtgärder, rutiner och utbildning i säker hantering av IT-resurserna så kommer en privat användning öka befintliga risker.

Detta kommer att innebära ett stort ansvar för den enskilde IT-användaren att även privat hantera sina arbetsrelaterade IT-verktyg på ett sätt som innebär att det inte medför risker som påverkar staden.

Om stadens regel för IT-användare ska ändras på så sätt att privat användning av stadens IT-resurser tillåts fullt ut kommer innehållet i nu föreslagen regel behöva justeras för att möta de risker detta innebär. Den tekniska utredning som genomförts avser privat användning av mobila enheter då stadsledningskontoret bedömde det som prioriterat inom ramen för återremissen. Samtidigt visar utredningen att privat användning av andra IT-resurser, såsom datorer, är förknippat med säkerhetsrisker. För att möjliggöra ytterligare privat användning än förslaget till IT-regel medger, så bedöms det nödvändigt att även utreda vilka åtgärder som kan vidtas för att öka säkerheten avseende övriga IT-resurser. Stadsledningskontoret kommer i detta fall behöva göra ytterligare utredningar för att återkomma med ett reviderat förslag på styrning, samt mer exakta kostnader och förutsättningar för genomförande.

Christina Eide	Eva Hessman
Direktör Utveckling och hållbarhet	Stadsdirektör

Göteborgs Stad

Protokollsutdrag
Sammanträdesdatum: 2024-06-12

§ 568 Ärendenummer SLK-2024-00392

Revidering av Göteborgs Stads regel för IT-användare

Beslut

Enligt återremissyrkande från S, V och MP:

Förslag till revidering av Göteborgs Stads regel för IT-användare återremitteras till stadsledningskontoret för utredning av konsekvenser av privat användning av Göteborgs Stads digitala arbetsverktyg med hänsyn till säkerhet, ekonomi och juridik.

Tidigare behandling

Bordlagt den 15 maj 2024, § 431 och den 29 maj 2024, § 502.

Handlingar

Stadsledningskontorets tjänsteutlåtande den 11 april 2024.
Återremissyrkande från S, V och MP den 10 juni 2024.
Återremissyrkande från M, D, L och KD den 10 juni 2024.

Yrkanden

Ordföranden Jonas Attenius (S) yrkar att ärendet ska återremitteras enligt yrkande från S, V och MP den 10 juni 2024.

Axel Josefson (M) yrkar att ärendet ska återremitteras enligt yrkande från M, D, L och KD den 10 juni 2024 och avslag på återremissyrkande från S, V och MP den 10 juni 2024.

Propositionsordning

Ordföranden Jonas Attenius (S) ställer först propositioner på bifall respektive avslag på återremissyrkandet från S, V och MP och finner att det bifallits.

Ordföranden ställer härefter propositioner på bifall respektive avslag på återremissyrkandet från M, D, L och KD och finner att det avslagits.

Protokollsutdrag skickas till

Stadsledningskontoret - Återremiss

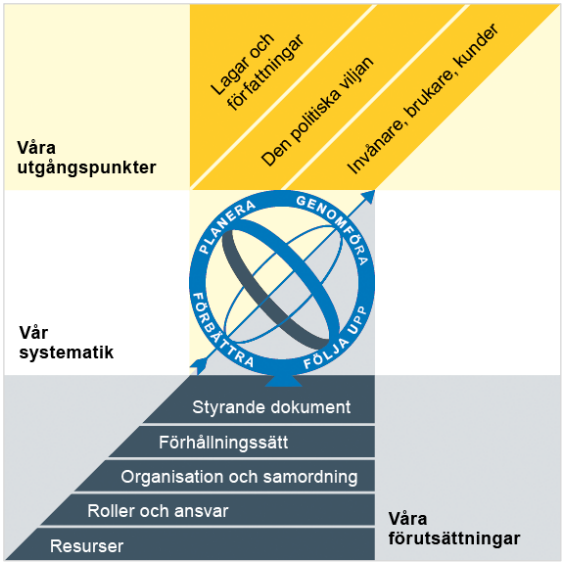
Göteborgs Stad

Göteborgs Stads regel för IT-användare

Reglerande styrande dokument

- Policy
- Riktlinje
- ► **Regel**
- Anvisning
- Rutin
- Instruktion

Göteborgs Stads styrsystem



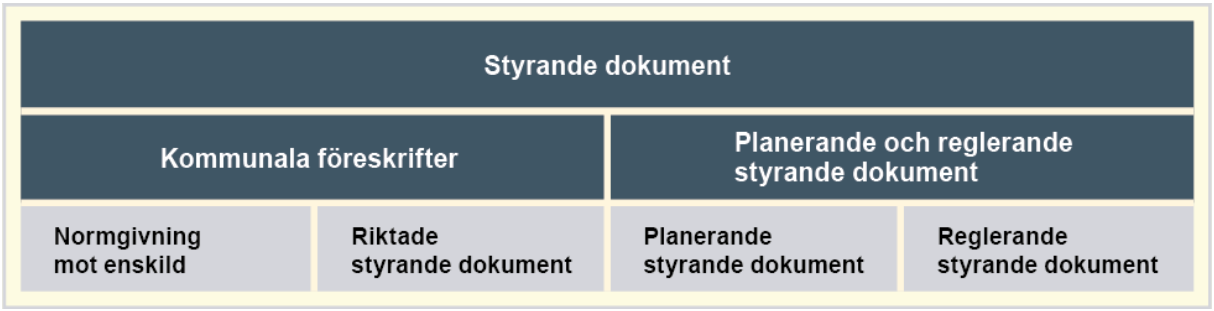
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera den politiska viljan. Inom Göteborgs Stad gäller de styrande dokument som antas av kommunfullmäktige och kommunstyrelsen. Därutöver fastställer nämnder och bolagsstyrelser egna styrande dokument för sin egen verksamhet. Kommunfullmäktiges budget är det övergripande och överordnade styrande dokumentet för Göteborgs Stads nämnder och bolagsstyrelser.

Om Göteborgs Stads styrande dokument

Göteborgs Stads styrande dokument är våra förutsättningar för att vi ska göra rätt saker på rätt sätt. De anger vad nämnder/styrelser och förvaltningar/bolag ska göra, vem som ska göra det och hur det ska göras. Styrande dokument är samlingsbegreppet för dessa dokument.

Stadens grundläggande principer såsom demokratisk grundsyn, principer om mänskliga rättigheter och icke-diskriminering omsätts i praktisk verksamhet genom att de integreras i stadens ordinarie beslutsprocesser. Beredning av och beslut om styrande dokument har en stor betydelse för förverkligandet av dessa principer i stadens verksamheter.

De styrande dokumenten ska göra det tydligt både för organisationen och för invånare, brukare, kunder, leverantörer, samarbetspartners och andra intressenter vad som förväntas av förvaltningar och bolag. De styrande dokumenten ligger till grund för att utkräva ansvar när vi inte arbetar i enlighet med vad som är beslutat.



Dokumentnamn: Göteborgs Stads regel för IT-användare

Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Kommunfullmäktige	Nämnder och styrelser	SLK-2024-00932	[Text]
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Regel	Tills vidare	[Datum]	Säkerhetschef Stadsledningskontoret

Innehåll

Inledning 4

Syftet med denna regel 4

Vem omfattas av dessa regler 4

Avgränsning 4

Koppling till andra styrande dokument 4

Avsteg 4

Regler 5

Tillåten användning av stadens IT-resurser 5

Informationssäkerhet - säker hantering av information och IT-resurser 5

Allmänt 5

Åtkomst till information 5

Säkerhetsuppdatering 5

Appar och programvaror 6

Rapportering av incidenter 6

Användning utomlands 6

Använda och sköta sin individuella e-postlåda 6

Arbetsgivarens tillgång till och kontroll av IT-resurser samt innehåll 7

Tillgång vid frånvaro 7

Tillgång och kontroll vid misstankar om oegentligheter m.m. 7

Åtgärder för övervakning och kontroll 7

Inledning

Syftet med denna regel

Dessa regler fastställer och redogör för det ansvar och de åtagande som gäller för IT-användare i Göteborgs Stad vid användning av stadens IT-resurser, såsom e-post, datorer, mobila enheter och kringutrustning.

Reglerna redogör också för Göteborgs Stads rättigheter att under vissa förutsättningar skaffa sig tillgång till och genomföra kontroller av IT-användares användning av stadens IT-resurser, inklusive av innehållet på stadens IT-resurser.

Vem omfattas av dessa regler

Reglerna gäller tills vidare för Göteborgs Stads nämnder och styrelser samt för kommunfullmäktige.

Med IT-användare i Göteborgs Stad omfattas anställda, förtroendevalda, entreprenörer, inhyrd personal, konsulter och leverantörer som arbetar i och med stadens IT-resurser.

Avgränsning

Ansvar och åtagande för personer som nyttjar Göteborgs Stads IT-resurser via så kallade offentliga e-tjänster regleras separat inom respektive e-tjänst.

Koppling till andra styrande dokument

Dessa regler konkretiserar Göteborgs Stads säkerhetspolicy och Göteborgs Stads riktlinje för informationssäkerhet.
Utöver ovanstående stadenövergripande styrning kan det finnas verksamhetsspecifika styrande och stödjande dokument.

Avsteg

Eventuella avsteg ska hanteras i enlighet med Göteborgs Stads riktlinje för styrande dokument.

Regler

Tillåten användning av stadens IT-resurser

Göteborgs Stads IT-resurser, såsom e-post, datorer, mobila enheter och kringutrustning, är Göteborgs Stads egendom och får endast användas som arbetsredskap och utifrån IT-användarens roll och arbetsuppgifter. Privat användning får inte ske, annat än i ytterst begränsad omfattning, eftersom det kan medföra onödiga säkerhetsrisker och ökade kostnader för Göteborgs Stad. Vid oklarheter kring vad som avses med användande utifrån roll och arbetsuppgifter så bör frågan hanteras av respektive verksamhet.

Göteborgs Stads IT-resurser får inte användas för ändamål som kan uppfattas oetiskt eller stötande, till exempel hantering av information och material som är pornografiskt, diskriminerande eller har anknytning till kriminell verksamhet.

Informationssäkerhet - säker hantering av information och IT-resurser

Allmänt

IT-användare ska informera sig om och efterleva de regelverk, rutiner och processer som är tillämpliga i staden som helhet samt i respektive nämnd och styrelse.

Åtkomst till information

Användaridentiteter, lösenord, passerkort, pinkoder och andra inloggningsuppgifter är personliga och får aldrig lånas ut eller bli kända för andra. Vid minsta misstanke om att lösenord eller pinkod röjts till obehörig ska IT-användaren utan dröjsmål ändra till ett nytt.

Lösenord ska vara unika, inte användas i privata sammanhang och konstrueras så att de inte lätt går att gissa eller pröva sig fram till.

IT-användare ska hantera Göteborgs Stads IT-resurser och information på sätt som minimerar risken för stöld, att obehörig får tillgång till information alternativt att den går förlorad på annat sätt. Behörigheter är personliga och tidsbegränsade och upphör när anställningen avslutas, vid byte av tjänst eller arbetsuppgifter.

IT-användare har en skyldighet att överföra eller på annat sätt göra tillgänglig all relevant information som tillhör Göteborgs Stad till närmaste chef vid avslut eller förändring av uppdrag.

Säkerhetsuppdatering

Göteborgs Stads IT-resurser ska alltid hållas uppdaterade och säkerhetsuppdateringar ska installeras skyndsamt.

Appar och programvaror

IT-användare får endast installera och använda programvaror, system eller appar på stadens IT-resurser som godkänts av Göteborgs Stads leverantörer eller respektive förvaltnings eller bolags verksamhetsspecifika IT-organisation.

IT-användare ska vara uppmärksam och undvika att klicka på länkar och filer i e-post från okända avsändare eller på webbsidor med okänt eller tveksamt innehåll. Genom att klicka på länken kan en IT-användare oavsiktligt godkänna att en skadlig kod laddas ner på enheten och orsaka skada.

Rapportering av incidenter

Avvikelser i säkerheten - informationssäkerhetsincidenter - såsom exempelvis röjande av lösenord och pinkoder, förlust av passerkort och viktig information, mottagande av e-post där IT-användare uppmanas att klicka på en okänd eller tveksam länk, ska rapporteras direkt enligt gällande rutiner för informationssäkerhetsincidenter. Vid osäkerhet ska anmälan alltid göras.

Användning utomlands

Göteborgs Stads IT-resurser ska inte tas med eller användas på utlandsresor eftersom det kan medföra onödiga säkerhetsrisker och ökade kostnader för Göteborgs Stad. Detta är särskilt viktigt vid resor utanför EU och EES. Om behov uppstår kan undantag medges efter behovs- och riskbedömning och beslut i det enskilda fallet utifrån verksamhetsspecifika rutiner.

Använda och sköta sin individuella e-postlåda

E-post är en av de vanligaste och mest använda kommunikationskanalerna i Göteborgs Stad, såväl inom staden som mellan staden och dess omvärld. Individuella e-postadresser och individuella e-postlådor utgör IT-resurser som tillhör Göteborgs Stad. Generella regler för användning, informationssäkerhet med mera som gäller för stadens IT-resurser, gäller alltså även för samtliga individuella e-postlådor. IT-användare som tilldelats en staden-e-postadress ska använda den vid utförande av uppdrag eller uppgifter för Göteborgs Stad bland annat för att undvika att information hanteras och sprids på ett felaktigt sätt.

Utöver att följa generella regler för IT-resurser gäller att varje IT-användare i Göteborgs Stad har ett personligt ansvar vid användandet av e-post att:

- Kontrollera sin e-post minst en gång per dag, varje helgfri måndag till fredag. Vid behov, exempelvis vid frånvaro, ska en IT-användare ge fullmakt till någon annan inom organisationen att kontrollera e-posten.
  För fackligt förtroendevalda kan frågan om fullmakt behöva hanteras i särskild ordning.
- Hantera skyddsvärd information som är klassificerad i klass 2 (utökad skyddsnivå) avseende konfidentialitet och riktighet med godkänd kryptering. Klass 3 (hög skyddsnivå) avseende konfidentialitet och riktighet ska hanteras i andra kanaler med högre säkerhet.
- Inte genomföra automatisk extern vidarebefordran av stadens e-post.

Arbetsgivarens tillgång till och kontroll av IT-resurser samt innehåll

Som IT-användare är det viktigt att vara medveten om Göteborgs Stads rätt att under vissa förutsättningar genomföra kontroller av IT-användares användning av stadens IT-resurser, inklusive av innehållet. Göteborgs Stad kan komma att skaffa sig tillgång till och/eller genomföra kontroller av IT-användares användning av och innehållet på stadens IT-resurser när en sådan åtgärd är motiverad. Göteborgs Stad kan då också vidta de praktiska åtgärder som krävs för att möjliggöra sådan tillgång och kontroll.

De situationer som det gäller finns att läsa om nedan. Vid bedömningen av om en åtgärd är motiverad samt vilka praktiska åtgärder som ska vidtas tar Göteborgs Stad hänsyn till gällande lagar, regler och god sed. Åtgärderna ska vara proportionerliga och IT-användarens personliga integritet ska beaktas vid bedömningen av vilka åtgärder som kan anses motiverade i det enskilda fallet.

Tillgång vid frånvaro

Situationer som kan motivera att Göteborgs Stad skaffar sig tillgång till IT-användares nyttjade IT-resurser, såsom individuell e-postlåda, mobila enheter och dator, är exempelvis

- oplanerad frånvaro,
- avslutad anställning eller
- frånvaro utan att kontrollera sin e-post eller ge fullmakt till någon annan inom organisationen att kontrollera den.

Göteborgs Stad kan i denna typ av situationer komma att skaffa sig tillgång till IT-användares nyttjade IT-resurser, om verksamheten har ett konkret behov av att komma åt information i IT-resursen. Det kan exempelvis handla om hantering av en begäran om allmän handling eller sökning efter dokument.

Tillgång och kontroll vid misstankar om oegentligheter m.m.

Situationer som kan motivera att Göteborgs Stad skaffar sig tillgång till och genomför kontroller av IT-användares användning av stadens IT-resurser, inklusive av innehållet på IT-resurserna, är exempelvis:

- Konkret misstanke om/utredning av oegentligheter, såsom brott, allvarliga avvikelser mot interna regler och riktlinjer i tjänsten, brott mot anställningsavtalet eller annat illojalt beteende.
- Konkret misstanke om/utredning av informationssäkerhetsincident, såsom obehörig åtkomst till stadens system eller nätverk.

Åtgärder för övervakning och kontroll

Vid användning av IT-resurser lämnas elektroniska spår (loggar). Loggning sker av säkerhetsmässiga, juridiska och tekniska skäl. Information i loggar kan även användas för

att kontrollera användningen av IT-resurser när sådan kontroll är motiverad. Detta innefattar även kontroll av internetanvändning.

I situationer där det är motiverat utifrån konkret misstanke/utredning av oegentligheter kan Göteborgs Stad tillfälligt frysa en IT-användares individuella e-postlåda och därmed förhindra radering av information i e-postlådan.

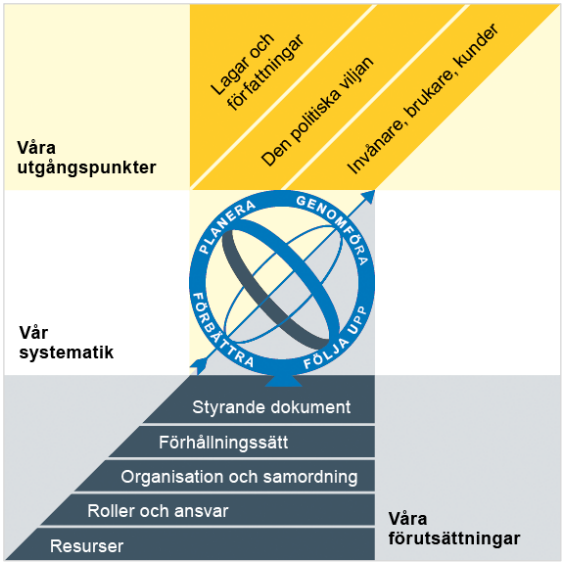
Göteborgs Stad

Göteborgs Stads regel för IT-användare

Reglerande styrande dokument

- Policy
- Riktlinje
- ► **Regel**
- Anvisning
- Rutin
- Instruktion

Göteborgs Stads styrsystem



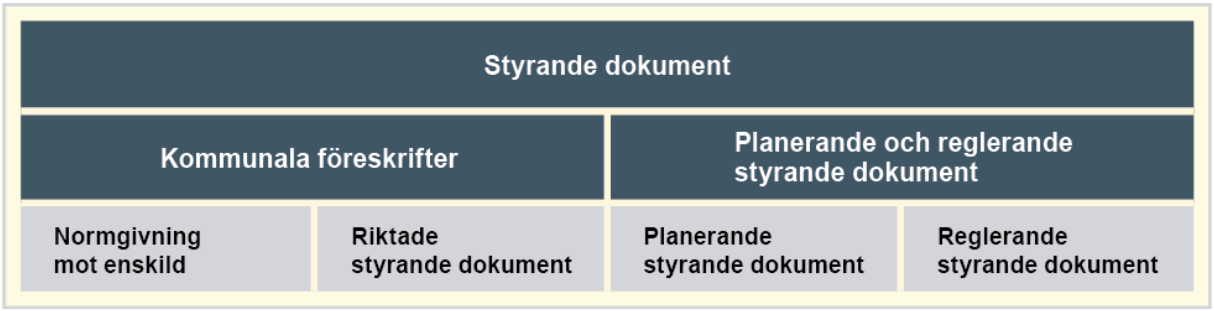
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera den politiska viljan. Inom Göteborgs Stad gäller de styrande dokument som antas av kommunfullmäktige och kommunstyrelsen. Därutöver fastställer nämnder och bolagsstyrelser egna styrande dokument för sin egen verksamhet. Kommunfullmäktiges budget är det övergripande och överordnade styrande dokumentet för Göteborgs Stads nämnder och bolagsstyrelser.

Om Göteborgs Stads styrande dokument

Göteborgs Stads styrande dokument är våra förutsättningar för att vi ska göra rätt saker på rätt sätt. De anger vad nämnder/styrelser och förvaltningar/bolag ska göra, vem som ska göra det och hur det ska göras. Styrande dokument är samlingsbegreppet för dessa dokument.

Stadens grundläggande principer såsom demokratisk grundsyn, principer om mänskliga rättigheter och icke-diskriminering omsätts i praktisk verksamhet genom att de integreras i stadens ordinarie beslutsprocesser. Beredning av och beslut om styrande dokument har en stor betydelse för förverkligandet av dessa principer i stadens verksamheter.

De styrande dokumenten ska göra det tydligt både för organisationen och för invånare, brukare, kunder, leverantörer, samarbetspartners och andra intressenter vad som förväntas av förvaltningar och bolag. De styrande dokumenten ligger till grund för att utkräva ansvar när vi inte arbetar i enlighet med vad som är beslutat.



Beslutad av:	**Gäller för:**	**Diarienummer:**	**Datum och paragraf för beslutet:**
Kommunfullmäktige	Nämnder och styrelser	SLK-2024-00932	[Text]
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Regel	Tills vidare	[Datum]	Säkerhetschef Stadsledningskontoret

Innehåll

Inledning 4
Syftet med denna regel 4
Vem omfattas av dessa regler 4
Avgränsning 4
Koppling till andra styrande dokument 4
Avsteg 4
Regler 5
Tillåten användning av stadens IT-resurser 5
Informationssäkerhet - säker hantering av information och IT-resurser 5
Allmänt 5
Åtkomst till information 5
Säkerhetsuppdatering 6
Appar och programvaror 6
Rapportering av incidenter 6
Användning utomlands 6
Använda och sköta sin individuella e-postlåda 6
Arbetsgivarens tillgång till och kontroll av IT-resurser samt innehåll 7
Tillgång vid frånvaro 7
Tillgång och kontroll vid misstankar om oegentligheter m.m. 7
Åtgärder för övervakning och kontroll 8

Inledning

Syftet med denna regel

Dessa regler fastställer och redogör för det ansvar och de åtagande som gäller för IT-användare i Göteborgs Stad vid användning av stadens IT-resurser, såsom e-post, datorer, mobila enheter och kringutrustning.

Reglerna redogör också för Göteborgs Stads rättigheter att under vissa förutsättningar skaffa sig tillgång till och genomföra kontroller av IT-användares användning av stadens IT-resurser, inklusive av innehållet på stadens IT-resurser.

Vem omfattas av dessa regler

Reglerna gäller tills vidare för Göteborgs Stads nämnder och styrelser samt för kommunfullmäktige.

Med IT-användare i Göteborgs Stad omfattas anställda, förtroendevalda, entreprenörer, inhyrd personal, konsulter och leverantörer som arbetar i och med stadens IT-resurser.

Avgränsning

Ansvar och åtagande för personer som nyttjar Göteborgs Stads IT-resurser via så kallade offentliga e-tjänster regleras separat inom respektive e-tjänst.

Koppling till andra styrande dokument

Dessa regler konkretiserar Göteborgs Stads säkerhetspolicy och Göteborgs Stads riktlinje för informationssäkerhet.

Utöver ovanstående stadenövergripande styrning kan det finnas verksamhetsspecifika styrande och stödjande dokument.

Avsteg

Eventuella avsteg ska hanteras i enlighet med Göteborgs Stads riktlinje för styrande dokument.

Regler

Tillåten användning av stadens IT-resurser

Göteborgs Stads IT-resurser, såsom e-post, datorer, mobila enheter och kringutrustning, är Göteborgs Stads egendom och får endast användas som arbetsredskap och utifrån IT-användarens roll och arbetsuppgifter. Privat användning får inte ske, annat än i ytterst begränsad omfattning, eftersom det kan medföra onödiga säkerhetsrisker och ökade kostnader för Göteborgs Stad.

Med begreppet privat användning avses sådan användning av stadens digitala arbetsverktyg som sker utanför anställningen eller det uppdrag som en person har för stadens räkning. Det spelar ingen roll var IT-användaren befinner sig eller vilken tid på dygnet det är, det viktiga är om han eller hon utför uppgifter för stadens räkning. Användning av stadens digitala arbetsverktyg som sker inom ramen för ett fackligt förtroendeuppdrag gentemot arbetsgivaren är relaterat till anställningen och ses inte som privat användning. Vid oklarheter kring vad som avses med användande utifrån roll och arbetsuppgifter så bör frågan hanteras av respektive verksamhet.

Göteborgs Stads IT-resurser får inte användas för ändamål som kan uppfattas oetiskt eller stötande, till exempel hantering av information och material som är pornografiskt, diskriminerande eller har anknytning till kriminell verksamhet.

Informationssäkerhet - säker hantering av information och IT-resurser

Allmänt

IT-användare ska informera sig om och efterleva de regelverk, rutiner och processer som är tillämpliga i staden som helhet samt i respektive nämnd och styrelse.

Åtkomst till information

Användaridentiteter, lösenord, passerkort, pinkoder och andra inloggningsuppgifter är personliga och får aldrig lånas ut eller bli kända för andra. Vid minsta misstanke om att lösenord eller pinkod röjts till obehörig ska IT-användaren utan dröjsmål ändra till ett nytt.

Lösenord ska vara unika, inte användas i privata sammanhang och konstrueras så att de inte lätt går att gissa eller pröva sig fram till.

IT-användare ska hantera Göteborgs Stads IT-resurser och information på sätt som minimerar risken för stöld, att obehörig får tillgång till information alternativt att den går förlorad på annat sätt. Behörigheter är personliga och tidsbegränsade och upphör när anställningen avslutas, vid byte av tjänst eller arbetsuppgifter.

IT-användare har en skyldighet att överföra eller på annat sätt göra tillgänglig all relevant information som tillhör Göteborgs Stad till närmaste chef vid avslut eller förändring av uppdrag.

Säkerhetsuppdatering

Göteborgs Stads IT-resurser ska alltid hållas uppdaterade och säkerhetsuppdateringar ska installeras skyndsamt.

Appar och programvaror

IT-användare får endast installera och använda programvaror, system eller appar på stadens IT-resurser som godkänts av Göteborgs Stads leverantörer eller respektive förvaltnings eller bolags verksamhetsspecifika IT-organisation.

Stadens programvaror, system eller appar ska inte laddas ner på andra enheter än de som tillhandahålls av Göteborgs Stad.

IT-användare ska vara uppmärksam och undvika att klicka på länkar och filer i e-post från okända avsändare eller på webbsidor med okänt eller tveksamt innehåll. Genom att klicka på länken kan en IT-användare oavsiktligt godkänna att en skadlig kod laddas ner på enheten och orsaka skada.

Rapportering av incidenter

Avvikelser i säkerheten - informationssäkerhetsincidenter - såsom exempelvis röjande av lösenord och pinkoder, förlust av passerkort och viktig information, mottagande av e-post där IT-användare uppmanas att klicka på en okänd eller tveksam länk, ska rapporteras direkt enligt gällande rutiner för informationssäkerhetsincidenter. Vid osäkerhet ska anmälan alltid göras.

Användning utomlands

Göteborgs Stads IT-resurser ska inte tas med eller användas på utlandsresor eftersom det kan medföra onödiga säkerhetsrisker och ökade kostnader för Göteborgs Stad. Detta är särskilt viktigt vid resor utanför EU och EES. Om behov uppstår kan undantag medges efter behovs- och riskbedömning och beslut i det enskilda fallet utifrån verksamhetsspecifika rutiner.

Använda och sköta sin individuella e-postlåda

E-post är en av de vanligaste och mest använda kommunikationskanalerna i Göteborgs Stad, såväl inom staden som mellan staden och dess omvärld. Individuella e-postadresser och individuella e-postlådor utgör IT-resurser som tillhör Göteborgs Stad. Generella regler för användning, informationssäkerhet med mera som gäller för stadens IT-resurser, gäller alltså även för samtliga individuella e-postlådor. IT-användare som tilldelats en staden-e-postadress ska använda den vid utförande av uppdrag eller uppgifter för Göteborgs Stad bland annat för att undvika att information hanteras och sprids på ett felaktigt sätt.

Utöver att följa generella regler för IT-resurser gäller att varje IT-användare i Göteborgs Stad har ett personligt ansvar vid användandet av e-post att:

- Kontrollera sin e-post minst en gång per dag, varje helgfri måndag till fredag. Vid behov, exempelvis vid frånvaro, ska en IT-användare ge fullmakt till någon annan inom organisationen att kontrollera e-posten.

För fackligt förtroendevalda kan frågan om fullmakt behöva hanteras i särskild ordning.
- Hantera skyddsvärd information som är klassificerad i klass 2 (utökad skyddsnivå) avseende konfidentialitet och riktighet med godkänd kryptering. Klass 3 (hög skyddsnivå) avseende konfidentialitet och riktighet ska hanteras i andra kanaler med högre säkerhet.
- Inte genomföra automatisk extern vidarebefordran av stadens e-post.

Tillgång till och kontroll av IT-resurser samt innehåll

Som IT-användare är det viktigt att vara medveten om Göteborgs Stads rätt att under vissa förutsättningar genomföra kontroller av IT-användares användning av stadens IT-resurser, inklusive av innehållet. Göteborgs Stad kan komma att skaffa sig tillgång till och/eller genomföra kontroller av IT-användares användning av och innehållet på stadens IT-resurser när en sådan åtgärd är motiverad. Göteborgs Stad kan då också vidta de praktiska åtgärder som krävs för att möjliggöra sådan tillgång och kontroll.

De situationer som det gäller finns att läsa om nedan. Vid bedömningen av om en åtgärd är motiverad samt vilka praktiska åtgärder som ska vidtas tar Göteborgs Stad hänsyn till gällande lagar, regler och god sed. Åtgärderna ska vara proportionerliga och IT-användarens personliga integritet ska beaktas vid bedömningen av vilka åtgärder som kan anses motiverade i det enskilda fallet.

Tillgång vid frånvaro

Situationer som kan motivera att Göteborgs Stad skaffar sig tillgång till IT-användares nyttjade IT-resurser, såsom individuell e-postlåda, mobila enheter och dator, är exempelvis

- oplanerad frånvaro,
- avslutad anställning eller
- frånvaro utan att kontrollera sin e-post eller ge fullmakt till någon annan inom organisationen att kontrollera den.

Göteborgs Stad kan i denna typ av situationer komma att skaffa sig tillgång till IT-användares nyttjade IT-resurser, om verksamheten har ett konkret behov av att komma åt information i IT-resursen. Det kan exempelvis handla om hantering av en begäran om allmän handling eller sökning efter dokument.

Tillgång och kontroll vid misstankar om oegentligheter m.m.

Situationer som kan motivera att Göteborgs Stad skaffar sig tillgång till och genomför kontroller av IT-användares användning av stadens IT-resurser, inklusive av innehållet på IT-resurserna, är exempelvis:

- Konkret misstanke om/utredning av oegentligheter, såsom brott, allvarliga avvikelser mot interna regler och riktlinjer i tjänsten, brott mot anställningsavtalet eller annat illojalt beteende.

- Konkret misstanke om/utredning av informationssäkerhetsincident, såsom obehörig åtkomst till stadens system eller nätverk.

Åtgärder för övervakning och kontroll

Vid användning av IT-resurser lämnas elektroniska spår (loggar). Loggning sker av säkerhetsmässiga, juridiska och tekniska skäl. Information i loggar kan även användas för att kontrollera användningen av IT-resurser när sådan kontroll är motiverad. Detta innefattar även kontroll av internetanvändning.

I situationer där det är motiverat utifrån konkret misstanke/utredning av oegentligheter kan Göteborgs Stad tillfälligt frysa en IT-användares individuella e-postlåda och därmed förhindra radering av information i e-postlådan.

Göteborgs Stad

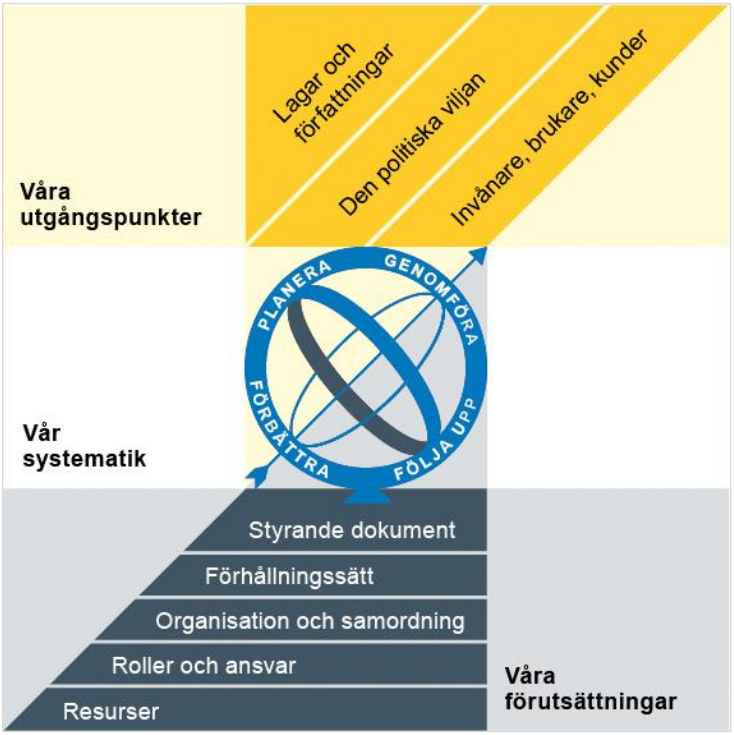
Göteborgs Stads regler för användande av e-post

Reglerande styrande dokument

- Policy
- Riktlinje
- ► **Regel**
- Anvisning
- Rutin
- Instruktion

Göteborgs Stads styrsystem

Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera den politiska viljan. Inom Göteborgs Stad gäller de styrande dokument som antas av kommunfullmäktige och kommunstyrelsen. Därutöver fastställer nämnder och bolagsstyrelser egna styrande dokument för sin egen verksamhet. Kommunfullmäktiges budget är det övergripande och överordnade styrande dokumentet för Göteborgs Stads nämnder och bolagsstyrelser.

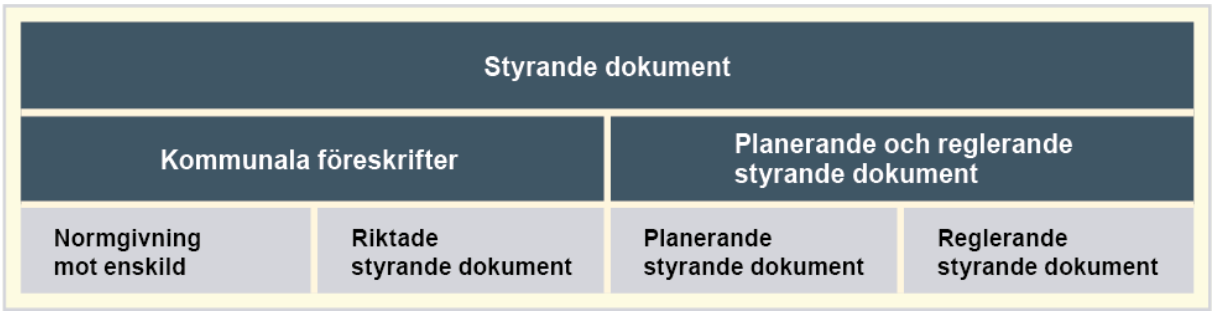


Om Göteborgs Stads styrande dokument

Göteborgs Stads styrande dokument är våra förutsättningar för att vi ska göra rätt saker på rätt sätt. De anger vad nämnder/styrelser och förvaltningar/bolag ska göra, vem som ska göra det och hur det ska göras. Styrande dokument är samlingsbegreppet för dessa dokument.

Stadens grundläggande principer såsom demokratisk grundsyn, principer om mänskliga rättigheter och icke-diskriminering omsätts i praktisk verksamhet genom att de integreras i stadens ordinarie beslutsprocesser. Beredning av och beslut om styrande dokument har en stor betydelse för förverkligandet av dessa principer i stadens verksamheter.

De styrande dokumenten ska göra det tydligt både för organisationen och för invånare, brukare, kunder, leverantörer, samarbetspartners och andra intressenter vad som förväntas av förvaltningar och bolag. De styrande dokumenten ligger till grund för att utkräva ansvar när vi inte arbetar i enlighet med vad som är beslutat.



Dokumentnamn: Göteborgs Stads regler för användande av e-post			
Beslutad av: Kommunfullmäktige	Gäller för: Stadens nämnder och bolag	Diarienummer: [Nummer]	Datum och paragraf för beslutet: 2011-06-09, § 13
Dokumentsort: Regel	Giltighetstid: Tillsvidare	Senast reviderad: 2018-11-12 (dnr 0110/18)	Dokumentansvarig: Stadens säkerhetschef, Stadsledningskontoret
Bilagor: [Bilagor]			

Innehåll

Inledning 3

Syftet med dessa regler 3

Vem omfattas av dessa regler 3

Bakgrund 3

Avsteg 3

Regler 4

Inledning

Syftet med dessa regler

E-post är en av de vanligaste kommunikationsformerna inom staden samt mellan staden och dess omvärld. De tekniska lösningar som nyttjas för e-post ger väldigt många hanteringsmöjligheter. I och med att e-post lyder under samma offentligrättsliga regler som vanlig post är det viktigt att tydliggöra vilka regler som gäller för användandet av e-post i Göteborgs Stad.

Vem omfattas av dessa regler

Reglerna gäller tillsvidare för alla delar inom Göteborgs Stad dvs alla verksamheter där Göteborgs Stad har avgörande ägarinflytande. Utöver dessa regler kan det finnas stadsövergripande och lokala kompletterande regelverk.

Bakgrund

E-posten i en myndighets eller ett offentligt ägt bolags officiella e-brevlåda och i de anställdas individuella e-brevlådor utgörs oftast av allmänna handlingar och ska därmed hanteras på motsvarande sätt som gäller för traditionella brev och andra pappershandlingar. Samma grundläggande regler som för dessa handlingar gäller avseende offentlighet och sekretess, diarieföring, bevarande och gallring av e-post. Myndigheten eller bolaget har fullständigt ansvar för e-posten i de aktuella brevlådorna. Det får därmed anses vara av stor vikt att säkerställa en korrekt och likformig hantering av de allmänna handlingar som kommer in till stadens verksamheter via e-post.

Avsteg

Eventuella avsteg ska hanteras i enlighet med ” Göteborgs Stads riktlinje för styrande dokument”.

Regler

Varje förvaltning/bolag inom Göteborgs Stad ska:

- Inneha minst en officiell e-postadress som kontrolleras minst en gång per dag, varje helgfri måndag till fredag
- Säkerställa att inkommen[1] e-post till verksamheten hanteras utan dröjsmål
- Säkerställa att allmänna handlingar[2] i inkommen e-post handläggs enligt gällande författningar och interna styrdokument såsom
    - Registrering/diarieföring
    - Informationsklassificering
    - Gallring
    - Arkivering
- Säkerställa att automatisk extern vidarebefordran[3] av verksamhetens e-post ej sker
- Uppmana medarbetare att ge fullmakt till någon annan i verksamheten att ha tillgång till den egna e-posten för att undvika handläggningsproblem vid semester, föräldraledighet, sjukskrivning etc.

Var och en som använder e-post i Göteborgs Stad har ett personligt ansvar att:

- Kontrollera sin e-post minst en gång per dag, varje helgfri måndag till fredag Medarbetare som inte ger fullmakt till någon annan vid förvaltningen/bolaget att ha tillgång till den egna e-posten är själv ansvarig att kontrollera e-posten även vid frånvaro såsom semester, barnledighet, sjukskrivning etc
- I sin e-post skilja ut och utan dröjsmål hantera allmänna handlingar[2] enligt gällande regelverk såsom informationsklassificering, registrering/diarieföring, arkivering etc
- Säkerställa att det finns gallringsbeslut innan någon allmän handling eller uppgift förstörs eller raderas
- Skydda de lösenord, pinkoder etc som man erhållit för åtkomst till e-post. Dessa är personliga och får ej delas med andra
- Konstruera lösenord så att de inte lätt går att pröva sig fram till eller gissa samt omedelbart byta lösenordet om det kan misstänkas att någon annan känner till det
- Till ansvarig[4] eller enligt formell beslutad rutin direkt rapportera störningar eller avvikelser i säkerheten eller om man fått e-post som strider mot lagar och förordningar

[1] Med inkommen avses här e-postmeddelande som anlänt till någon av förvaltningens/bolagets e-postservrar.
[2] Innehållet avgör alltid om en handling är allmän eller inte. Om e-postmeddelandet berör förvaltningens/bolagets verksamhet blir meddelandet allmän handling direkt när det är inkommet. Den information om meddelanden som finns i loggar/förteckningar utgör alltid allmän handling. Den e-post som utväxlas internt inom en verksamhet mellan medarbetare såsom utkast, koncept eller annat internt arbetsmaterial är normalt inte allmän handling.
[3] Med extern vidarebefordran menas att e-post som ska hanteras i stadens e-postsystem istället med automatik skickas vidare och hanteras i ett e-postssystem som finns utanför stadens nät och utanför stadens kontroll. Exempel på sådana e-postsystem är Hotmail och Gmail.
[4] Med ansvarig avses här den närmast verksamhetsansvariga personen för respektive e-post-användare såsom närmaste chef, uppdragsgivare etc.

- Använda Göteborgs Stads e-post utifrån vederbörandes roll och arbetsuppgifter. Privat användning får endast ske i mycket begränsad omfattning och får inte påverka ordinarie arbetsuppgifter eller inverka menligt på stadens IT-resurser i form av kostnader, lagringsutrymme, prestanda etc
- Ej formulera e-post, som inte ingår i ordinarie arbetsuppgifter från Göteborgs Stad, så att de som läser får uppfattningen att e-posten är skickad på uppdrag av Göteborgs Stad
- Ej genomföra automatisk extern vidarebefordran[3] av stadens e-post
- Ej hantera information som är klassad i nivå 2[5] avseende konfidentialitet (sekretess) och riktighet utan vederhäftiga kryptografiska funktioner i e-posten[6]

[5] Exempel på information i nivå 2 är känsliga personuppgifter enligt dataskyddsförordningen eller sekretessbelagd information. Kontakta förvaltningens/bolagets säkerhetsfunktion för stöd och mer information.

[6] De kryptografiska funktionerna bör ligga i nivå med nationellt godkända kryptografiska funktioner. Kontakta förvaltningens/bolagets säkerhetsfunktion för stöd och mer information.

Stadsledningskontoret

2025-03-31

PM - Rättslig reglering

Ärendet

Stadsledningskontoret har reviderat Göteborgs Stads regel för IT-användare utifrån behov av tydligare styrning och vägledning, ökad användbarhet samt ändrad och tillkommen lagstiftning inom informations- och cybersäkerhetsområdet. De ändringar som gjorts i regeln innefattar i huvudsak ett förtydligande gällande privat användning, nedladdning av applikationer (appar) samt arbetsgivarens rätt till tillgång och kontroll över IT-resurser. Vid revideringen av regel för IT-användare har även innehåll från stadens regel för e-post omhändertagits.

Stadsledningskontoret har utifrån beslut i kommunstyrelsen om återremiss kompletterat utredningen i ärendet med ”konsekvenser av privat användning av Göteborgs Stads digitala arbetsverktyg med hänsyn till säkerhet, ekonomi och juridik”.

Stadsledningskontoret har bedömt det som prioriterat att fokusera den fördjupade utredningen på privat användning av stadens mobila enheter, såsom mobiltelefoner och surfplattor. Resonemangen i det här underlaget är emellertid giltiga avseende alla sorters IT-resurser. Denna PM är upprättad för att biläggas tjänsteutlåtandet i ärendet.

Vad menas med privat användning?

Göteborgs Stads regel för IT-användare beskriver ansvaret vid användning av stadens IT-resurser, såsom e-post, datorer, mobila enheter och kringutrustning. Reglerna gäller för stadens nämnder och styrelser samt för kommunfullmäktige. Begreppet IT-användare omfattar anställda, förtroendevalda, entreprenörer, inhyrd personal, konsulter och leverantörer som arbetar i och med stadens IT-resurser.

I både nu gällande regel och i förslaget till ny regel används begreppet ”privat användning”. Med privat användning avses sådan användning av stadens digitala arbetsverktyg som sker utanför tjänsten eller, när det gäller andra användare än medarbetare, utanför det uppdrag som en person har för stadens räkning.

Utifrån den här avgränsningen omfattar begreppet inte bara användning som sker i egenskap av privatperson. Även annan användning utanför tjänsten/uppdraget kan ses om privat användning i det här sammanhanget. Exempel på sådana situationer är att medarbetare har bisysslor och bedriver näringsverksamhet eller har ideella uppdrag. Användning av stadens digitala arbetsverktyg som sker inom ramen för ett fackligt förtroendeuppdrag gentemot arbetsgivaren är relaterat till anställningen och ses inte som privat användning. För att användningen ska vara relaterad till tjänsten/uppdraget spelar det ingen roll var IT-användaren befinner sig eller vilken tid på dygnet det är, det viktiga är om han eller hon utför uppgifter för stadens räkning.

Informations- och cybersäkerhet

Göteborgs Stad ansvarar för att upprätthålla flera viktiga samhällsfunktioner. Hanteringen av stadens IT-resurser utgör en viktig del i det systematiska informationssäkerhetsarbetet, vilket medför ett behov av tydlig styrningen på området. Ett av de huvudsakliga syftena med att justera nu gällande regler är att minska risken för uppkomsten av säkerhetsrisker.

Ur ett arbetsgivar-/medarbetarperspektiv är det centralt att arbetsgivaren ansvarar för organisationens informationssäkerhet. Arbetsgivaren behöver bestämma hur medarbetarna får använda sig av organisationens IT-resurser, formulera detta i regler och policys och informera medarbetarna om dessa. Nämndernas och styrelsernas ansvar för informationssäkerheten i sina verksamheter innebär att motsvarande krav behöver ställas för alla personer som använder stadens digitala arbetsverktyg, varför IT-regeln omfattar medarbetare, förtroendevalda, entreprenörer, inhyrd personal, konsulter och leverantörer som arbetar i och med stadens IT-resurser.

NIS-direktiven och kommande nationell lagstiftning

I syfte att uppnå en hög gemensam nivå på säkerhet i nätverks- och informationssystem antog Europaparlamentet och rådet år 2016 det s.k. NIS-direktivet (Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen). NIS-direktivet införlivades år 2018 i svensk rätt genom införandet av lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och förordningen (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Lagstiftningen har kompletterats av föreskrifter från bland annat Myndigheten för samhällsskydd och beredskap. Genom NIS-regleringen ställs omfattande krav som syftar till att säkerställa säkerhet i nätverks- och informationssystem. Reglerna omfattar i dagsläget leverantörer av samhällsviktiga tjänster inom sju sektorer, bland annat digital infrastruktur, energi, hälso- och sjukvård, leverans och distribution av dricksvatten och transport.

I oktober 2024 trädde det reviderade NIS-direktivet (NIS2) i kraft i Sverige. Revideringen av NIS-direktivet innebär bland annat att kraven skärps på systematiskt informationssäkerhetsarbete. Utredningen som haft i uppdrag att se över vilka anpassningar av svensk lagstiftning som är nödvändiga för att genomföra NIS2 har presenterat sina slutsatser och förslag i delbetänkandet Nya regler om cybersäkerhet (SOU 2024:18) och i slutbetänkandet Motståndskraft i samhällsviktiga tjänster (SOU 2024:64).

Regelverket är omfattande och komplext men kortfattat finns det två viktiga skillnader mellan gällande lagstiftning och förslaget till ny cybersäkerhetsreglering. Den första är att cybersäkerhetslagen föreslås omfatta betydligt fler aktörer och att antalet sektorer utökas till 18. Den andra viktiga skillnaden är att kraven kommer att gälla för hela verksamheten, inte bara för samhällsviktiga och digitala tjänster.

NIS2 ställer krav på medlemsländerna och medlemsländerna ska, genom nationell lagstiftning, i sin tur ställa krav på verksamhetsutövarna. Den svenska cybersäkerhetslagen förslogs träda i kraft i januari 2025 men har blivit fördröjd. Propositionen väntas komma under våren 2025. Den nya lagstiftningen kommer därför sannolikt som tidigast träda i kraft till sommaren. När den nya lagstiftningen trätt i kraft

ska utsedda myndigheter utfärda föreskrifter. Vilka myndigheter som får mandat att föreskriva om vad är ännu inte bestämt. Än så länge är alltså de specifika kraven för NIS2 inte fastställda nationellt men det är tydligt att direktivet höjer kraven på systematiskt informationsarbete brett i stadens verksamheter. För att staden ska vara väl förberedd är det därför av stor vikt att det bedrivs ett kontinuerligt arbete med utvecklingen av ett systematiskt och riskbaserat förebyggande arbete i organisationen.

Genom att endast använda stadens IT-resurser som arbetsredskap minimeras Göteborgs Stads risker att information sprids till obehörig eller att stadens information blir otillgänglig. Det kan konstateras att en obegränsad privat användning av stadens mobila enheter innebär att riskerna kopplat till informations- och cybersäkerhet kommer öka avsevärt. Även om riskerna i viss utsträckning kan motverkas av till exempel tekniska säkerhetsåtgärder, tydliga och kända rutiner och att IT-användare får utbildning i säker hantering av mobila enheter så kommer en ökad privat användning öka befintliga risker i stadens verksamheter. I det här sammanhanget bör det också betonas att den nya cybersäkerhetslagen innebär att det införs omfattandet krav när det gäller rapportering och utredning av incidenter som inträffar i stadens verksamheter.

Ur den enskilde IT-användarens perspektiv är en konsekvens att ett stort ansvar kommer läggas på den enskilde att inte råka hantera stadens mobila enheter privat på ett sätt som innebär att det uppstår säkerhetsrisker som påverkar staden.

Tryckfrihetsförordningen och offentlighets- och sekretesslagen

Varför måste e-postmeddelanden läsas kontinuerligt?

IT-användare med staden-e-postadresser har en individuell kanal för att kontakta den myndighet (nämnd/styrelse) som IT-användaren tillhör. Ett meddelande som kommer in till en av stadens e-postlådor och som rör myndighetens verksamhet är att anse som en inkommen handling hos myndigheten. Mot bakgrund av reglerna i tryckfrihetsförordningen och offentlighets- och sekretesslagen om allmänna handlingars offentlighet och om registrering av sådana handlingar måste inkomna e-postmeddelanden därför läsas löpande samt eventuellt tas om hand för registrering och ytterligare handläggning. Eftersom det inte är tillräckligt att aktivera ett frånvaromeddelande och avstå från att hantera inkomna e-postmeddelanden behöver var och en antingen själv läsa sin e-post vid frånvaro eller delegera e-posten till en kollega.

Ett röstmeddelande som har talats in på en mobiltelefon kan också utgöra en allmän handling. Att den som använder en av stadens mobiltelefoner är frånvarande på grund av semester eller av något annat skäl saknar betydelse för bedömningen av om meddelandet ska anses utgöra en allmän handling. Det är alltid ett ansvar för myndigheten att säkerställa att de krav som ställs i tryckfrihetsförordningen och offentlighets- och sekretesslagen upprätthålls.

En ytterligare aspekt av att delegera e-posten till en kollega vid semesterledighet är att alla medarbetare har rätt att vara helt lediga när de har semester. Semesterlagen är en skyddslagslagstiftning som bland annat syftar till att ge medarbetarna tid för vila och återhämtning. Arbetsgivarens sätt att organisera arbetet får därför inte förutsätta att medarbetarna är tillgängliga genom att kolla sin e-post eller mobiltelefon under semestern.

Konsekvenser av privat användning av stadens mobila enheter

Om IT-användare får använda stadens mobila enheter för privata ändamål utan begränsning kommer det vara oundvikligt att det sker en sammanblandning av privat information och verksamhetens information. Som exempel kommer det kunna finnas privat information sparad på en mobil enhet, i appar, i e-postlådan och i loggar som skapas vid användningen av enheterna. I vilken uträckning och vilken slags information beror emellertid på hur en IT-användare väljer att använda sina mobila enheter privat.

Om en förvaltning eller ett bolag får en begäran om att ta del av allmänna handlingar kan den som använder stadens mobila enheter behöva gå igenom olika privata handlingar för att bedöma vilka handlingar som ska anses vara allmänna. Om den som gjort en begäran nekas att ta del av handlingarna och överklagar myndighetens beslut kan privata handlingar behöva överlämnas till kammarrätten inom ramen för domstolsprocessen. Det beror på att kammarrätten behöver ta del av alla de handlingar som en begäran avser, oavsett om det faktiskt är allmänna handlingar eller inte, för att kunna göra en prövning av om beslutet att avslå var korrekt.

Rätten att göra en begäran om att ta del av allmänna handlingar är långtgående och även om regelverket innebär att rent privat information oftast inte behöver lämnas ut så krävs det alltid att det sker en prövning och den som nekas har alltid rätt att få ett överklagbart beslut.

När det gäller s.k. e-postloggar (loggar över inkommande och utgående e-postmeddelanden) är en sådan handling en allmän handling i sig. Det betyder att e-postloggen, om den begärs ut, ska lämnas ut i sin helhet och att information om in- och utgående e-postmeddelanden inte kan tas bort även om det rör privata meddelanden. Möjligheten att sekretessbelägga information i e-postloggar är också begränsad. Samma sak gäller för andra slags loggar som skapas vid användandet av stadens mobila enheter.

Tillgång till IT-resurser och kontroller

Som beskrivs i regeln finns det situationer när Göteborgs Stad behöver kunna skaffa sig tillgång till och genomföra kontroller av IT-användares användning av stadens IT-resurser, inklusive av innehållet på stadens IT-resurser. I förslaget till ny regel beskrivs två situationer när Göteborgs Stad kan komma att bereda sig tillgång till och genomföra sådana kontroller. Som en övergripande förutsättning anges att bedömningen av om en åtgärd är motiverad alltid ska ske med utgångspunkt i gällande lagar, regler och god sed. Åtgärderna måste vidare vara proportionerliga och IT-användarens personliga integritet ska beaktas vid bedömningen av vilka åtgärder som kan anses motiverade i det enskilda fallet. Med dessa utgångspunkter beskrivs sedan två typsituationer.

Den första situationen är tillgång vid IT-användarens frånvaro och här avses oplanerad frånvaro, avslutad anställning eller frånvaro utan delegering av den individuella e-postlådan. I det här fallet är det primärt de lagkrav som ställs när det gäller hanteringen av allmänna handlingar som motiverar åtgärder ur ett rättsligt perspektiv (jmf rubriken Tryckfrihetsförordningen och offentlighets- och sekretesslagen).

Den andra situationen är tillgång och kontroll vid misstanke om och utredning av oegentligheter (till exempel brott, allvarliga avvikelser mot interna regler och riktlinjer i tjänsten, brott mot anställningsavtalet eller annat illojalt beteende) samt misstanke om och

utredning av säkerhetsbrist eller annan informationssäkerhetsincident (till exempel obehörig åtkomst till stadens system eller nätverk).

När det gäller en arbetsgivares möjlighet att bereda sig tillgång till en medarbetares IT-resurser och genomföra kontroller vid misstanke om och utredning av oegentligheter betraktas detta som åtgärder grundade i arbetsledningsrätten. Arbetsgivarens arbetsledningsrätt är enligt äldre praxis en allmän rättsgrundsats som gäller även utan stöd i kollektivavtal. Möjligheten att genomföra kontroller och vissa övervakningsåtgärder härleds alltså inte från lagstiftning utan från den underliggande arbetsledningsrätten vilket innebär att arbetsgivaren bestämmer över arbetets utförande och även över arbetsplatsen och dess utrustning.

Arbetsgivarens arbetsledningsrätt kan emellertid inte utövas oinskränkt. Av praxis följer att arbetsgivaren inte får utöva sin rätt i strid mot lag och goda seder på arbetsmarknaden. Vid en bedömning av vilka åtgärder som kan anses motiverade och proportionerliga i det enskilda fallet måste medarbetarens rätt till integritet beaktas. Med skydd för medarbetarens integritet avses regler som syftar till att skydda mot ingrepp i dennes privata förhållanden. Rätten till skydd för privatlivet skyddas bland annat i olika internationella rättsakter, varav en central reglering är artikel 8 i Europakonventionen om mänskliga rättigheter (EKMR).

Av artikel 8 EKMR framgår att var och en har rätt till respekt för sitt privat- och familjeliv, sitt hem och sin korrespondens. Ingrepp i privatlivet kan enligt artikel 8 emellertid vara tillåtna om de har stöd i lag. Kravet på stöd i lag syftar till att säkerställa förutsebarhet för berörda personer. Europadomstolen har ansett att inskränkningar i den personliga integriteten som baseras på arbetsgivarens arbetsledningsrätt, i vart fall när den sker i enlighet med en av arbetsgivaren upprättad generell policy, har stöd i lag i konventionens mening. En förutsättning är emellertid att ingreppet i den personliga integriteten ska vara proportionellt i förhållande till ändamålen.

När det gäller andra användare av stadens mobila enheter än medarbetare är det inte arbetsledningsrätten som ger mandat att vid behov genomföra nödvändiga kontroller av stadens mobila enheter. Utifrån respektive nämnds/styrelses ansvar att säkerställa organisationens informations- och cybersäkerhet, samt att de mobila enheter som staden tillhandahåller och den verksamhetsrelaterade information som finns på dessa är stadens egendom oavsett om enheterna även får användas privat, krävs det att nämnden/styrelsen i vissa fall har möjlighet att bereda sig tillgång till dessa enheter.

Även dataskyddsförordningen innehåller regler som ger enskilda skydd för sin kommunikation och sitt privatliv och som innebär att en förutsättning för att nämnden/styrelsen ska få kontrollera IT-resurser är att IT-användaren fått information om vilka kontroller som kan komma att ske samt att kontrollerna inte är mer ingripande än nödvändigt. Dataskyddsperspektivet beskrivs mer utförligt nedan (se rubriken Dataskyddsförordningen).

När det finns anledning att misstänka en säkerhetsbrist eller informationssäkerhetsincident finns det en skyldighet att agera utifrån regelverket om informationssäkerhet (NIS-regleringen, dataskyddsförordningen och även stadens riktlinje för informationssäkerhet). Att det går att skydda stadens informationssystem och

den information som finns i dessa samt upprätthålla skyddet för personuppgifter är centralt för att stadens verksamheter ska kunna bedrivas på ett säkert sätt.

Konsekvenser av privat användning av stadens mobila enheter

En obegränsad privat användning av stadens mobila enheter innebär ökade risker både för den enskilde och för staden. Även om riskerna beror på hur en IT-användare väljer att använda enheterna privat och vilka säkerhetsåtgärder som kan vidtas så kan det konstateras att privat användning av stadens mobila enheter kommer innebära att det uppstår risker för intrång i den personliga integriteten. En nämnd/styrelse får som utgångspunkt inte bereda sig tillgång till rent privat information som finns på mobila enheter men som beskrivits ovan finns det situationer då det är nödvändigt att omhänderta en enhet eller skaffar sig tillgång till information som finns på denna. Om en person har använt den mobila enheten privat innebär detta att ett integritetsintrång kommer vara oundvikligt. En mer praktisk dimension är att IT-användarens tillgång till enheten kommer vara delvis eller helt begränsad, vilket naturligtvis kommer vara problematiskt beroende på hur enheten används i vardagen. De här riskerna innebär att det bland annat kommer ställas höga krav på tydlig information om möjliga konsekvenser så att IT-användaren kan göra ett välinformerat val i frågan om att använda stadens mobila enheter privat.

Dataskyddsförordningen

Dataskyddslagstiftningen är ett omfattande och komplext regelverk och det som beskrivs här är översiktliga resonemang inom ett antal områden. Detta är alltså inte en fullständig beskrivning av alla bedömningar som kan komma att aktualiseras om privat användning av stadens mobila enheter tillåts utan begränsning.

Dataskyddsförordningen grundar sig i de mänskliga rättigheterna. Ett av de huvudsakliga syftena med kraven i förordningen är att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter. Med personuppgifter menas varje upplysning som rör en identifierad eller identifierbar fysisk person. Exempel på personuppgifter är namn, personnummer, telefonnummer, ljudinspelningar, elektroniska identiteter som IP-adresser och s.k. cookies, om de kan kopplas till en fysisk person. Avgörande är alltså att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person.

Ansvaret för att dataskyddsförordningen följs åligger den som är personuppgiftsansvarig, dvs. den som bestämmer för vilka ändamål personuppgifter ska behandlas och hur behandlingen ska gå till. I en kommun är det som utgångspunkt nämnden eller styrelsen som är personuppgiftsansvarig för den behandling av personuppgifter som sker i dess verksamhet.

Dataskyddsförordningens tillämpningsområde är brett men av förordningen framgår att den inte ska tillämpas för privatpersoners egen privata behandling av personuppgifter. Detta följer av artikel 2 i dataskyddsförordningen där det framgår att fysiska personers behandling av personuppgifter som görs som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll inte omfattas av förordningens regler, det s.k. hushållsundantaget. Enligt hushållsundantaget är dataskyddsförordningen inte

tillämplig på sådan behandling som sker för privata ändamål eller för hushållsändamål och som alltså saknar koppling till yrkes- eller affärsmässig verksamhet.

Säkerheten för personuppgifter är en del av informationssäkerhetsarbetet. Flera skyldigheter enligt dataskyddsförordningen ska uppfyllas genom att implementera lämpliga tekniska och organisatoriska åtgärder för att uppnå syftet med skyldigheten. När det gäller kraven på informationssäkerhet handlar det om att skydda personuppgifterna och behandlingen av dem så att de registrerades fri- och rättigheter skyddas.

Om en nämnd/styrelse behöver vidta kontroller av mobila enheter och det medför en behandling av personuppgifter om till exempel en medarbetare ska dataskyddsförordningen följas. En förutsättning för att kunna kontrollera medarbetares digitala arbetsverktyg är som beskrivits ovan att medarbetaren fått information om vilka kontroller som kan komma att ske. Kontrollerna får inte heller vara mer ingripande än nödvändigt. Alla människor har en grundläggande rätt till skydd för sin kommunikation och sitt privatliv. En nämnd/styrelse får därför normalt inte ta del av innehållet i privata filer eller e-postmeddelanden. Undantag från detta gäller vid till exempel misstanke om oegentligheter såsom brott, allvarliga avvikelser mot interna regler och riktlinjer i tjänsten, brott mot anställningsavtalet eller annat illojalt beteende.

Konsekvenser av privat användning av stadens mobila enheter

Som beskrevs inledningsvis så omfattar begreppet ”privat användning” sådan användning som någon gör utanför tjänsten eller uppdraget för staden. Om en medarbetare har bisysslor som till exempel att bedriva näringsverksamhet eller har ideella uppdrag och använder stadens mobila enheter även för dessa ändamål skulle det ses som privat användning utifrån regeln men däremot inte nödvändigtvis omfattas av hushållsundantaget i dataskyddsförordningen.

En medarbetade som behandlar personuppgifter inom ramen för arbetsgivarens verksamhet ska normalt inte ses som personuppgiftsansvarig. I den mån medarbetaren behandlar personuppgifter för sina egna ändamål, som skiljer sig från arbetsgivarens, kommer han eller hon emellertid att kunna betraktas som personuppgiftsansvarig. En medarbetare som utför behandling av personuppgifter som inte är anställningsrelaterad med hjälp av sina mobila enheter kan alltså komma att ses som personuppgiftsansvarig för dessa behandlingar. Om en behandling som medarbetaren gör faller under hushållsundantaget blir dataskyddsförordningen dock inte tillämplig och något personuppgiftsansvar uppstår inte.

Sammanfattningsvis kan medarbetaren bli personuppgiftsansvarig när det gäller behandling av personuppgifter som inte omfattas av hushållsundantaget och inte heller är anställningsrelaterad. Motsvarande resonemang gäller för andra IT-användare än medarbetare. Det bör framhållas att det kommer kunna uppstå svårigheter att bedöma vad som är relaterat till tjänsten/uppdraget och inte, vilket kan leda till gränsdragningsfrågor kopplat till personuppgiftsansvaret. En följdfråga som kommer behöva utredas är också i vilken mån en nämnd/styrelse kan komma att ses som personuppgiftsbiträde.

Att en arbetsgivare tar del av en medarbetares privata e-post eller privata filer i arbetsgivarens datanätverk har ansetts innebära en sådan behandling av personuppgifter som arbetsgivaren är personuppgiftsansvarig för enligt den tidigare personuppgiftslagen. Om arbetsgivaren av något skäl behöver bereda sig tillgång till uppgifter som finns på

medarbetarens mobila enheter innebär det att nämnden/styrelsen kan komma att behandla även sådana personuppgifter som medarbetaren har i sina mobila enheter och som inte är tjänsterelaterade. Ett exempel på en sådan situation är om nämnden/styrelsen får en begäran om att ta del av allmänna handlingar som omfattar information på en medarbetarens mobila enheter eller i olika loggar som skapas vid användningen av dessa. Nämnden/styrelsen kommer då vara personuppgiftsansvarig för de behandlingar som hanteringen av begäran medför. En annan sådan situation är att arbetsgivaren behöver bereda sig tillgång till medarbetarens mobila enheter för att genomföra kontroller vid misstanke om och utredning av oegentligheter.

En slutsats är att nämnden/styrelsen i olika situationer kan komma att behandla privata uppgifter om en IT-användare eller uppgifter om andra externa personer och då få ett personuppgiftsansvar för dessa behandlingar. Eftersom nämnden/styrelsen inte kommer ha kontroll över vilken slags uppgifter IT-användaren hanterar på sina mobila enheter kan detta även vara känsliga personuppgifter.

Det kan konstateras att ökad privat användning också kan öka risken för personuppgiftsincidenter som rör nämndens/styrelsens ordinarie verksamhet. Om medarbetare till exempel laddar ner och använder appar eller slår på olika funktioner för sin privata användning kan detta resultera i att medarbetaren omedvetet delar information från organisationen till leverantören av de privata apparna. Även privat användning genom att till exempel besöka hemsidor, klicka på länkar, skicka och ta emot e-post och att spara ner filer kan leda till ökad risk för skadlig kod, vilket kan leda till personuppgiftsincidenter som drabbar de personuppgifter som organisationen ansvarar för i sin ordinarie verksamhet.

Intraservice har i sin utredning framhållit att ett antal säkerhetsåtgärder skulle behöva införas för att uppnå tillräcklig teknisk säkerhet om obegränsad privat användning ska tillåtas. Dessa åtgärder kan enligt Intraservice i vissa fall komma att beröra personuppgifter eller annan privat information och innefatta både insyn i och påverkan på personuppgifterna och informationen. Beroende på var ansvaret att bestämma över åtgärderna läggs kan den nuvarande uppdelningen av personuppgiftsansvaret påverkas.

Vidare visar den utredning som Intraservice genomfört om möjligheterna att tillåta av privat användning att det kommer krävas säkerhetsåtgärder som innebär en mer omfattande övervakning av stadens mobila enheter. Eftersom det ur det här perspektivet inte går att skilja på privata aktiviteter och aktiviteter som sker inom ramen för tjänsten eller uppdraget medför säkerhetsåtgärderna även att det kan uppstå risker med hänsyn till den personliga integriteten.

Om stadens regel för IT-användare ska ändras på så sätt att privat användning av mobila enheter tillåts fullt ut kommer nämnder/styrelser behöva vidta olika åtgärder för att minimera de risker som finns. Även om riskerna i viss utsträckning kan motverkas av till exempel tekniska säkerhetsåtgärder, rutiner och utbildning i säker hantering av de mobila enheterna så kommer privat användning öka befintliga risker. Ur den enskilde IT-användarens perspektiv blir en konsekvens av detta att ett stort ansvar läggs på den enskilde individen att inte, medvetet och omedvetet, hantera sina mobila enheter på ett sätt som innebär att det uppstår risker som påverkar staden.

Förmånsbeskattning

Om en arbetsgivare tillhandahåller en medarbetare en förmån som innebär en inbesparing av privata levnadskostnader uppkommer normalt en skattepliktig förmån. Ytterligare en aspekt av privat användning av de IT-resurser som arbetsgivaren tillhandahåller är därför frågan om förmånsbeskattning.

Bestämmelserna om förmånsbeskattning finns i 11 kap. inkomstskattelagen (1999:1229). Av 11 kap. 8 § inkomstskattelagen, som gäller alla sorters varor och tjänster som arbetsgivaren tillhandahåller medarbetaren som arbetsredskap, framgår att förmån av en vara eller tjänst som en anställd får av arbetsgivaren inte ska tas upp om:

1. varan eller tjänsten är av väsentlig betydelse för att den skattskyldige ska kunna utföra sina arbetsuppgifter,
2. förmånen är av begränsat värde för den anställde, och
3. förmånen för den anställde inte utan svårighet kan särskiljas från nyttan i anställningen.

Skatteverket har publicerat ett vägledande ställningstagande som gäller ”Förmånsbeskattning av elektronisk utrustning eller abonnemang mot fast avgift” (dnr 202 233742-18/111) där frågan om skattemässiga konsekvenser när arbetsgivaren tillhandahåller elektronisk utrustning eller abonnemang mot fast avgift som en medarbetare använder även för privat bruk behandlas.

Av Skatteverkets ställningstagande framgår bland annat följande. Med elektronisk utrustning avses mobiltelefon, dator, läsplatta och router. Med abonnemang mot fast avgift avses tjänster som tillhandahålls via den elektroniska utrustningen mot fast avgift utan möjlighet att särskilja användandet. Med ordinarie arbetsplats avses de platser där den anställde normalt utför sina arbetsuppgifter.

Privat användning av elektronisk utrustning eller abonnemang på den ordinarie arbetsplatsen är inte skattepliktig. Att på arbetstid använda arbetsgivarens elektroniska utrustning för att utföra privata ärenden förmånsbeskattas därför inte. I de fall en anställd kan använda elektronisk utrustning eller abonnemang mot fast avgift på ordinarie arbetsplats som inte är i arbetsgivarens lokaler ska en separat bedömning göras för varje ordinarie arbetsplats och varje teknisk utrustning med tillhörande abonnemang mot fast avgift för sig.

När arbetsgivarens elektroniska utrustning med abonnemang mot fast avgift finns utanför ordinarie arbetsplats ska en medarbetare i regel förmånsbeskattas för möjligheten att använda dessa för privat bruk. Om det är av väsentlig betydelse för arbetsuppgifternas utförande att en anställd har tillgång till både den elektroniska utrustningen och abonnemanget mot fast avgift utanför ordinarie arbetsplats ska en anställd dock inte beskattas för förmånen att använda utrustningen privat eftersom Skatteverket gör bedömningen att det i sådana fall är svårt att särskilja det privata användandet från nyttan i anställningen. Det privata användandet blir i dessa fall en närmast ofrånkomlig biförmån.

Om arbetsgivaren tillhandahåller elektronisk utrustning med abonnemang mot fast avgift utanför ordinarie arbetsplats utan att utrustningen eller abonnemanget är av väsentlig betydelse för att den anställde ska kunna utföra sina arbetsuppgifter uppkommer det en

skattepliktig förmån. Varje elektronisk enhet (mobiltelefon, dator, läsplatta, router) bedöms separat för väsentlighet i arbetet.

Sammanfattningsvis kan konstateras att det kommer behöva skapas rutiner för hanteringen av frågan om förmånsbeskattning. Medarbetare som har tillgång till elektronisk utrustning kommer få ta ställning till om han eller hon önskar använda utrustningen även privat. Om medarbetaren väljer att inte använda utrustningen privat utanför den ordinarie arbetsplatsen behöver detta dokumenteras i en överenskommelse. För medarbetare som väljer att använda utrustningen privat utanför den ordinarie arbetsplatsen behöver i stället ansvarig chef gör en bedömning av om förutsättningarna för skattefrihet är uppfyllda eller inte.

I ställningstagandet ger Skatteverket även vägledning genom ett antal exempel som illustrerar de bedömningar som behöver göras.

- **Exempel 1: Tillgång till elektronisk utrustning eller abonnemang mot fast avgift behövs utanför arbetsplatsen**

Arbetsgivaren tillhandahåller Lisa, som arbetar som projektledare, en mobiltelefon med abonnemang mot fast avgift för att hon ska kunna komma i kontakt med sina kollegor under ordinarie arbetstid och för att hon ska vara nåbar när hon inte är på sin ordinarie arbetsplats. Lisa arbetar på kontoret men utför också en hel del arbete i hemmet och på de olika platser som hon besöker som ett led i sitt arbete som projektledare. Arbetsgivaren tillåter att Lisa använder mobiltelefonen för privat bruk även när hon inte är på sin ordinarie arbetsplats, vilket Lisa också gör. Eftersom mobiltelefonen med tillhörande abonnemang mot fast avgift är av väsentlig betydelse för att Lisa ska kunna utföra sina arbetsuppgifter även utanför den ordinarie arbetsplatsen ska inte Lisa beskattas för den eventuella förmån som kan uppkomma när hon använder mobiltelefonen privat.

- **Exempel 2: Den anställda får möjlighet att använda elektronisk utrustning eller abonnemang mot fast avgift för privat bruk trots att det inte är nödvändigt för tjänstens utförande**

Arbetsgivaren tillhandahåller Adam, som arbetar som lagerarbetare, en mobiltelefon med abonnemang mot fast avgift för att han ska kunna komma i kontakt med sina kollegor när han arbetar. Arbetsgivaren tillåter att Adam använder mobiltelefonen för privat bruk när han inte är på arbetet, vilket Adam också gör. Förvisso har Adam behov av mobiltelefonen när han är på sin arbetsplats men när han lämnar arbetsplatsen är telefonen inte nödvändig för att han ska kunna fullgöra sina arbetsuppgifter. Eftersom mobiltelefonen och abonnemanget inte är av väsentlig betydelse när Adam befinner sig utanför ordinarie arbetsplats ska Adam beskattas för förmånen att privat använda en mobiltelefon och abonnemang mot fast avgift som arbetsgivaren betalar. Värdet på förmånen är vad det skulle ha kostat honom att inneha motsvarande mobil och abonnemang. Förmånsvärdet ska beräknas löpande varje månad.

- **Exempel 3: Den anställde avstår från möjligheten att använda elektronisk utrustning eller abonnemang mot fast avgift för privat bruk**

Arbetsgivaren tillhandahåller Lena, som arbetar som lagerarbetare tillsammans med Adam, en mobiltelefon med abonnemang mot fast avgift för att hon ska kunna komma i kontakt med sina kollegor när hon arbetar. Till skillnad från Adam vill Lena inte använda

arbetsgivarens mobiltelefon på sin fritid och meddelar arbetsgivaren detta. Tillsammans kommer arbetsgivaren och Lena skriftligt överens om att Lena inte ska använda mobiltelefonen privat utanför den ordinarie arbetsplatsen. Eftersom Lena inte har tillåtelse att använda den elektroniska utrusningen för privat bruk utanför den ordinarie arbetsplatsen uppkommer inte någon skattepliktig förmån.

- **Exempel 4: Den anställda får möjlighet att för privat bruk använda abonnemang som innehåller fler funktioner än vad som krävs för att utföra arbetet**

Arbetsgivaren tillhandahåller Per, som arbetar som löneassistent, en mobiltelefon med abonnemang mot fast avgift. Abonnemanget ger Per tillgång till telefoni och surf. Båda tjänsterna är nödvändiga för att han ska kunna sköta sitt arbete som löneadministratör. Per utför allt sitt arbete på kontoret. Arbetsgivaren kräver att Per ska vara tillgänglig på telefon efter kontorstid och Per får därför ta med sig sin mobiltelefon hem. Arbetsgivaren tillåter att Per får använda mobiltelefonen för privat bruk även när han inte är på sin ordinarie arbetsplats (kontoret), vilket Per också gör. Mobiltelefonen med tillhörande abonnemang mot fast avgift är nödvändig för att Per ska kunna utföra sina arbetsuppgifter utanför den ordinarie arbetsplatsen. Förmånen att få använda mobiltelefonen privat är av begränsat värde och det är svårt att särskilja det privata användandet från användandet i tjänsten. Abonnemang mot fast avgift ska i detta sammanhang betraktas som en tjänst oavsett om abonnemanget innehåller flera olika funktioner såsom mobil telefoni, sms, mms och surf eller datatrafik. Per ska därför inte beskattas för den eventuella förmån som kan uppkomma när han använder någon av abonnemangets funktioner privat.

Göteborgs Stad
Stadsledningskontoret

Central Samverkansgrupp
(Ordinarie CSG)

Protokoll 7/2024
Sammanträdesdatum
2024-04-18

Ärendenr:SLK-2024-00058

Utdrag ur protokoll

§ 5 Samverkan före beslut

b) Regel för IT-användare (slk-2024-00392) Tjänsteutlåtande och regel är utsänt 2024-04-11

Helena Österlind, Linda Larsson och Sara Linderup föredrar ärendet.

CSG har dialog i ärendet

Sveriges Lärare vill ha fört till protokollet att frågan gällande fackliga förtroendevaldas e-postadresser är viktigt och måste lösas.

Akademikerförbundet SSR framför att det skulle behövas läggas till en menig i regeln att fackliga förtroendevaldas e-postadresser har en särskild ordning. Förbundet framför att också att det är viktigt att regeln behöver kommuniceras ut och bli känd för medarbetare i staden.

Vision framför att det har varit ett bra arbete i referensgruppen. Förbundet ser att det är viktigt att det framgår i regeln vad som gäller för fackliga organisationers e-post och att den ska hanteras i en särskild ordning. Det måste också vara tydligt för chefen vad denne har för ansvar i frågan.

Sacorådet ser inte så mycket avtryck i regeln från dialogen i den fackliga referensgruppen, exempelvis gällande misstanke om brott eller illojalt beteende. De fackliga organisationerna vill ha ett förtydligande i regeln angående rekvisit för att gå in och titta på medarbetares mail

En reviderad regel skickas ut till CSG och samverkan sker genom mail 2024-04-23

Akademikerförbundet SSR anger att förbundet ser samverkan som fullgjord, och antecknar till protokollet att förbundet ser det som högst angeläget att komma i gång med arbetet kring vad som ska gälla för fackligt förtroendevalda.

Sacorådet förklarar sig oenig i samverkan då förbundet vill att meningen ”för facklig förtroendevalda **kan** frågan om fullmakt behöva hanteras i särskild ordning”, ändras till ”för facklig förtroendevalda **ska** frågan om fullmakt hanteras i särskild ordning.

Övriga förbund anmäler inga ytterligare kommentarer antecknas till protokollet.

Sacorådet förklarar sig därmed oeniga.

Samverkan förklaras fullgjord via mail 2024-04-23.

Vid protokollet

……..
Anna Wilsson

Protokollet justeras

……..... …….....
Eva Hessman, Arbetsgivare Johanna Morgensterns, Akademikerförbundet SSR

……..... ……..…….
Martha Zoura, Kommunal Anette Sernlo Larsen, Vision

Göteborgs Stadshus AB

Göteborgs Stad

Dag och tid: 2024-04-24, kl 15:00-16:30
Plats: Gustav Adolfs Torg, lokal Riksbankssalen

Protokoll från Koncernfackligt råd 3/2024

Protokollsutdrag: **§ 9**

§ 9 Göteborg Stads regel för IT-användare

Linda Larsson och Sara Linderup redovisar, i enlighet med till Koncernfackliga rådet tillställt underlag, stadsledningskontorets arbete med revidering av Göteborg Stads regel för IT-användare. Bakgrunden till arbetet är bland annat omvärldsförändringar, nya regler på säkerhetsområdet samt uppdrag enligt stadens handlingsplan för digitalisering syftande till att tydliggöra styrningen. Genom det pågående arbetet föreslås två befintliga regler, regeln för IT-användare respektive regeln för e-post, slås samman till en. Den nya regeln föreslås träda i kraft för nämnder och styrelser per 1 januari 2025.

Fackliga företrädare i Koncernfackliga rådet ställer frågor kring arbetet och innehållet som besvaras, samt lämnar synpunkter på förslaget enligt följande.

Vårt medskick är att det ska stå att det måste vara Lätt att göra rätt! Mycket ansvar läggs på användaren - men då måste man ha rätt förutsättningar att göra rätt. Viktigt med infomaterial, utbildning, uppföljning, tid, nanolearning, guider mm.

När det gäller texten: ”Kontrollera sin e-post, eller säkerställa att annan medarbetare gör det, minst en gång per dag, varje helgfri måndag till fredag.” Om detta är ett lagkrav bör detta tydliggöras. Annars verkar det helt orimligt att alla ska göra detta oberoende av vilket arbete man har. Hur förenkla detta?

När det gäller texten:”Misstanke om/utredning av oegentligheter, såsom brott, allvarliga avvikelser mot interna regler och riktlinjer i tjänsten, brott mot anställningsavtalet eller annat illojalt beteende. Tydliggör vad som krävs för att det ska vara misstänkt?”

Det kan bli en risk att man får svårare att få tag i personal då man förmodligen lägger mobilen på jobbet (viktigt på ett samhällsnyttigt företag där man ibland behöver ringa in personal snabbt). Mobilen anses som en förmån så dessutom ytterligare något som tas bort.

Bilaga 8

Göteborgs Stad
Stadsledningskontoret

Central Samverkansgrupp **(Ordinarie CSG)**	Protokoll 6/2025 Sammanträdesdatum **2025-04-10**	Ärendenr:SLK-2025-00057

Utdrag ur protokoll

§ 5 Samverkan före beslut

a) Samverkan av revidering av IT-regel.
Helena Österlind, Linda Larsson och Sara Linderup deltar. TU, regel samt rättsligt underlag utsänt inför mötet. Dialog genomfördes på CSG den 27 mars.

De fackliga organisationerna anser att det behövs förtydliganden runt vad som avses med att läsa sin e-post, telefonmeddelande samt sms varje dag. Det finns medarbetare som går på schema och många medarbetare som inte har en tillgång till dator eller telefon i sitt arbete där ett sådant krav kan få stora konsekvenser för både medarbetare och chefer. Det verkar som om regeln utgår från att alla har arbeten där man sitter vid datorn hela tiden. De fackliga värnar om alla medarbetares rätt till ett privatliv och att den personliga integriteten är skyddad.

De Fackliga organisationer anser att det är för många saker som är otydliga i regeln och ser en risk att det vänds mot medarbetare som inte har uppfattat vad som gäller. Vidare lyfts att den föreslagna IT-regeln innebär stora förändringar och de fackliga upplever inte att de har fått tillräckligt stor möjlighet att vara med i framtagandet. Det är också svårt att se hur regeln kommer att kunna hanteras praktiskt.

Arbetsgivaren lyfter IT-regeln kommer att påverka olika yrkesgrupper på olika sätt. Varje arbetsgrupp behöver prata om frågorna för att se hur det påverkar dem och ta fram arbetssätt. Redan idag finns det en risk man som medarbetare utsätter organisationen för risker utifrån hur IT-verktygen används. Tanken är att IT-regeln ska minska den risken.

De fackliga förbunden vill vara med och förtydliga tolkning och tillämpning och ser även behov av dialog och förtydliganden om IT-regelns praktiska effekter för fackliga företrädare. Arbetsgivaren föreslår inrättande av en facklig referensgrupp. Frågan om facklig referensgrupp hanteras på nästa CSG-möte.

Utifrån ovanstående resonemang förklarar sig samtliga fackliga oeniga till förslaget till reviderad IT-regel.

Det antecknas att partssamverkan har fullgjorts i oenighet.

Punkten förklaras omedelbart justerad

Vid protokollet

……..
Anna Wilsson

Protokollet justeras

…….....	…….....
Eva Hessman, Arbetsgivare	Johanna Morgensterns, Akademikerförbundet SSR
…….....	……..…….
Marie Lökkeberg, Kommunal	Elin Pellegrino, Vision

Göteborgs Stadshus AB

Göteborgs Stad

Dag och tid: 2025-03-19, kl 15:00-16:30
Plats: Stadshus AB, lokal Riksbankssalen samt Teams

Protokoll från Koncernfackligt råd 1/2025

Protokollsutdrag: **§ 8**

§ 8 Göteborgs Stads regel för IT-användare

Helena Österlind och Linda Larsson (stadsledningskontoret) presenterar, i enlighet med till Koncernfackliga rådet tillställt underlag, nuläget i rubricerat ärende. Bakgrunden till att revidering av regeln initierats är: ändrad och tillkommen lagstiftning inom cyber- och informationssäkerhetsområdet, förändrat omvärldsläge som kräver tydligare styrning samt att digitalisering både privat och i tjänsten har utvecklat en praxis av befintlig regel som inte överensstämmer med tolkning och nuvarande behov. Stadsledningskontorets förslag har en del innehållsmässiga förändringar med tydligare reglering men det finns också ett behov av att säkerställa implementering och efterlevnad, bland annat genom kommunikation och kompetenshöjande insatser.

Stadsledningskontorets ursprungliga förslag återremitterades av KS 2024-06-12 för utredning av konsekvenser av privat användning av Göteborgs Stads digitala arbetsverktyg med hänsyn till säkerhet, ekonomi och juridik. Den fördjupade utredning som skett (av Intraservice avseende tekniska frågor), visar att det går att vidta åtgärder för att förbättra den tekniska säkerheten och att det ur det perspektivet finns förutsättningar för att tillåta privat användning. Stadsledningskontoret bedömer dock att förslaget till regel fortfarande är gällande då åtgärderna: ökar riskerna för säkerhetsincidenter, inte beaktar administrativa, organisatoriska eller fysiska aspekter av informationssäkerhet, är förknippat med ytterligare administration och kostnader, riskerar medarbetarnas integritet samt kan innebära att nämnder och styrelser blir personuppgiftsansvariga för privata uppgifter. Det konstateras även att regeln kan behöva kompletteras med information om att inte ladda ner jobbrelaterade appar på privata enheter.

Koncernfackliga rådet tackar för bra information och bekräftar behoven av förändring. Det framhålls dock som viktigt att det ges tid och stöd för implementering och att det informeras väl då förändringarna skulle kunna ge upphov till besvikelse. Det betonas att rutiner för kommunikation inom arbetsledning kan behöva ses över liksom vissa arbetsmiljöaspekter. Även användande av privat bank-id i arbetsgivarens utrustning behöver utredas och hanteras.