Tjänsteutlåtande
Utfärdat 2024-04-11
Ärendenummer SLK-2024-00392

Handläggare
Linda Larsson
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 1 till stadsledningskontorets tjänsteutlåtande och gäller från och med 2025-01-01.
2. Göteborgs Stads regel för användande av e-post, beslutad i kommunfullmäktige 2011-06-09 § 13, upphör att gälla från och med 2025-01-01.
3. Göteborgs Stads regel för IT-användare, beslutad i kommunfullmäktige 2009-09-10 § 17, upphör att gälla från och med 2025-01-01.

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 informationssäkerhetsområdet. 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 informationssäkerhetsincidenter 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.

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 för att reglera användandet har att göra med säkerhetsperspektivet. Där kopplas kostnaderna 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, viket 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.

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 ekonomisk fördelaktigt att ett övergripande staden gemensamt 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 2024.

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.

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.

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 arbete med informationssäkerhet. Ett systematiskt informationssäkerhetsarbete bygger på ett samspel mellan teknik, människa 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.

Samverkan

Ärendet har samverkats i Central samverkansgrupp 2024-04-18.

Information har lämnats till Koncernfackliga rådet 2024-04-24.

Bilagor

1. Förslag till Göteborgs Stads regel för IT-användare
2. Göteborgs Stads regel för IT-användare, beslutad 2009-09-10, § 17
3. Göteborgs Stads regler för användande av e-post, beslutad 2011-06-09, § 13
4. Protokollsutdrag Central samverkansgrupp, CSG, 2024-04-18, § 5 b
5. Protokollsutdrag, Koncernfackliga rådet, KFR, 2024-04-24, § 9

Ärendet

Stadsledningskontoret har reviderat Göteborgs Stads regel för IT-användare utifrån ett förändrat omvärldsläge och den 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.

Beskrivning av ärendet

Göteborgs Stads uppdrag innebär ett ansvar att upprätthålla flera viktiga samhällsfunktioner. Detta ställer höga krav på informationssäkerhet. 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 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 privat. 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 2024 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

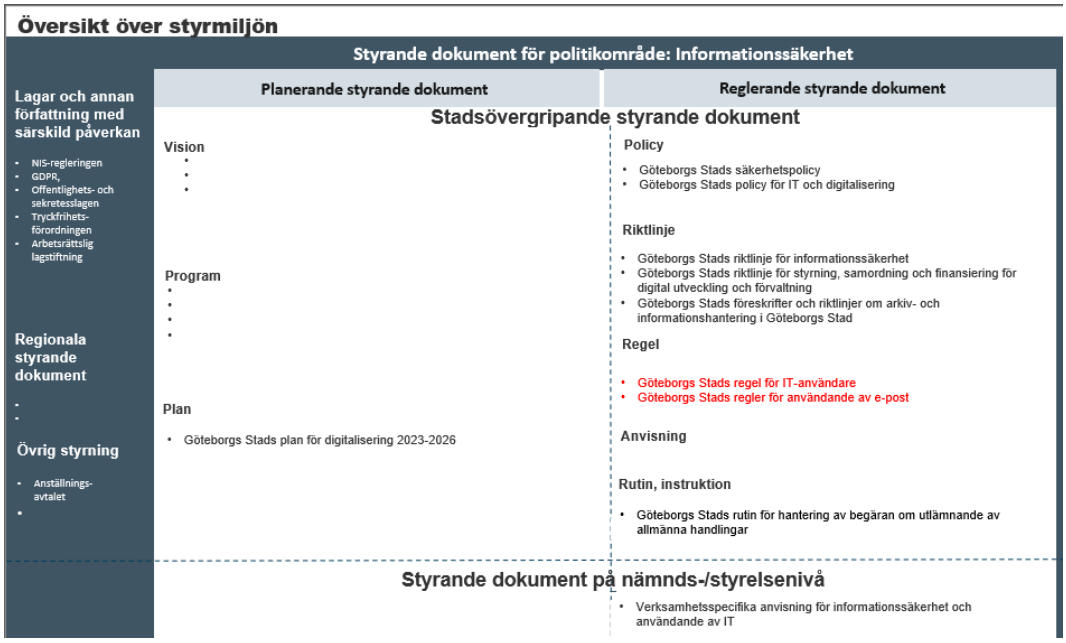
motiverade aktörer, såsom hacktivister. Hotet från främmande makt är högt, vilket återkommer bland annat i Säkerhetspolisens årsrapport från 2022/2023 där de ser en förändrad hotbild där Sverige är en arena för en större konflikt med olika former av cyberattacker och hot mot informationssäkerheten i 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.

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 10 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.

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. Göteborgs Stad är remissinstans och en sammanfattning av förslagen samt stadens synpunkter redovisas för kommunstyrelsen den 15 maj 2024 (SLK-2024-00295).

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 med 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.

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.

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 ökande kostnader för Göteborgs Stad. Stadsledningskontorets bedömning är att det inte är möjligt att helt begränsa det privata nyttjandet. 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.

Regeln har även skärpts vad gäller användning utomlands. Att ta med Göteborgs Stads IT-resurser utomlands innebär större säkerhetsrisk eftersom offentliga nätverk kan vara avlyssnade på exempelvis hotell, restauranger och flygplatser. IT-resurser ska därför inte kopplas upp på offentliga nätverk. Inom EU innebär det oftast inga ökade kostnader, men utanför EU kan det bli mycket kostsamt för staden varför regeln tydliggör att detta enbart ska ske 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.

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.

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.

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 så 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.

Stadsledningskontorets bedömning

Göteborgs Stad är en stor stad med många IT-användare och flera samhällsviktiga verksamheter. Detta innebär stora risker 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 så 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 2025-01-01, 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.

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 2024 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 åtaganden 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.

Christina Eide	Eva Hessman
Direktör Utveckling och hållbarhet	Stadsdirektör

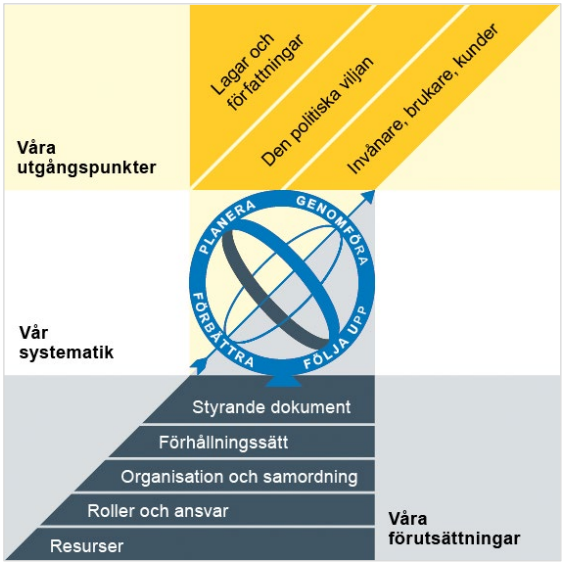
Göteborgs Stad

Göteborgs Stads regel för IT-användare

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



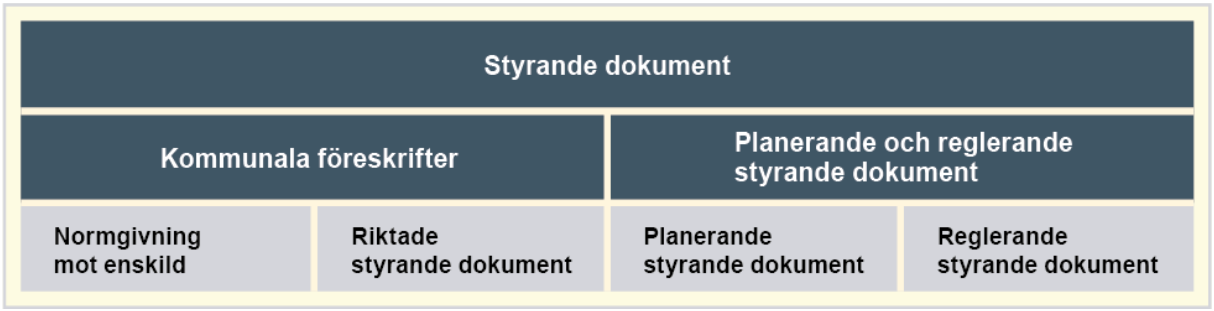
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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

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 Stads regel för IT-användare

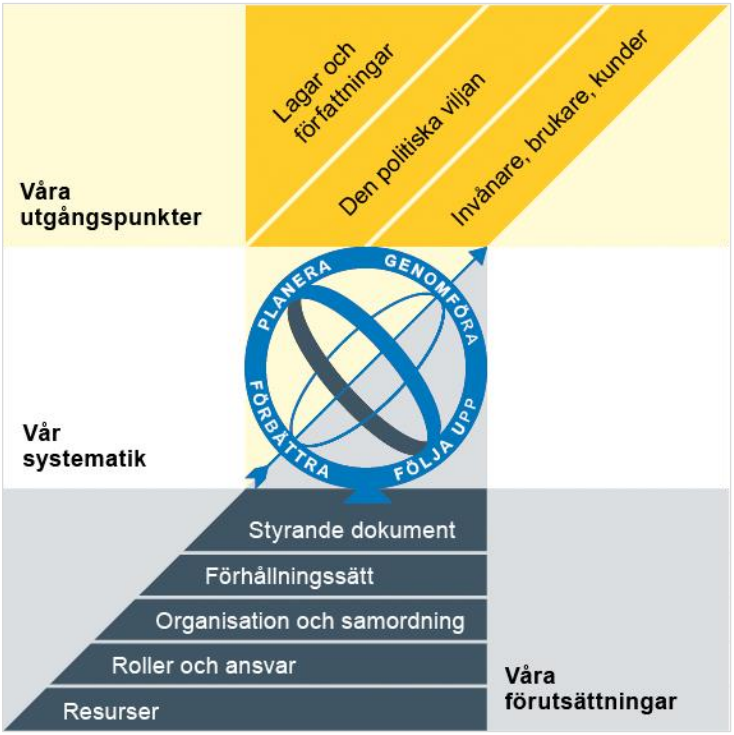
Reglerande styrande dokument

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

Grundläggande skyddsnivå - Klass 1

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.

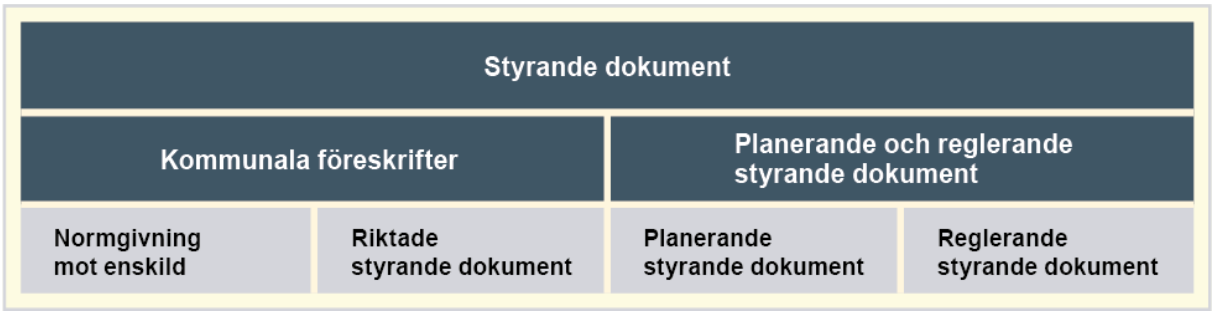


Om Göteborgs Stads styrande dokument

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: Kommunfullmäktige	Gäller för: Stadens nämnder och styrelser	Diarienummer: [Nummer]	Datum och paragraf för beslutet: [Text]
Dokumentsort: Regel	Giltighetstid: Tillsvidare	Senast reviderad: [Datum]	Dokumentansvarig: Informationssäkerhetschef
Bilagor: [Bilagor]			

Innehåll

Inledning

Syftet med dessa regler

Dessa regler fastställer ansvar och åtagande för IT-användare i Göteborgs Stad samt hur dessa får använda stadens IT-resurser såsom persondator, nätverk, servrar, mobil telefoni, programvaror, Internet etc.

Med IT-användare i Göteborgs Stad avses i dessa regler anställda, entreprenörer, inhyrd personal, konsulter och leverantörer som arbetar i eller med stadens IT-resurser.

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

Med hänsyn till att det i samhället förekommer att IT-resurser används för illegala ändamål eller ändamål som kan betraktas som stötande etcetera så loggas de så kallade elektroniska spår som IT-användaren lämnar vid användandet. Dessa loggar kan komma att användas vid utredningar av säkerhetsbrott eller misstanke om oegentlighet.

Vem omfattas av dessa regler

Reglerna gäller tillsvidare för Stadens nämnder och styrelser.

Koppling till andra styrande dokument

Dessa regler konkretiserar Stadens säkerhetspolicy samt riktlinjen för informationssäkerhet.

Regler

Som IT-användare i Göteborgs Stad har man ett personligt ansvar att

- Informera sig om de regelverk, rutiner och det ansvar som är tillämpliga. Kontakta ansvarig[1] om du behöver förtydliganden.
- Efterleva tillämpliga säkerhetsrutiner och regelverk
- Skydda de lösenord, pinkoder etcetera som man erhållit för åtkomst. 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
- Informera ansvarig vid behov av förändring och borttag av behörigheter
- Till ansvarig eller enligt formell beslutad rutin direkt rapportera störningar eller avvikelser i säkerheten eller om man fått meddelande till exempel epost eller sms som strider mot lagar och förordningar
- Inte kopiera copyrightförsedd information utan godkännande eller använda den på sådant sätt att en annan organisation otillåtet kan nyttja Göteborgs Stads information eller programkod
- Använda Göteborgs Stads IT-resurser och behörigheter endast 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 etcetera
- Inte använda Göteborgs Stads IT-resurser för ändamål som kan uppfattas som oetiskt eller stötande till exempel hantering av information och material som är pornografiskt, diskriminerande eller har anknytning till kriminell verksamhet. Undantag från detta kan göras i de fall sådan information/material behövs för tjänstebruk, vilket skriftligen ska godkännas av ansvarig
- Informationsspridning med hjälp av IT (såsom epost, webbsidor, bloggar etcetera) som inte ingår i ordinarie arbetsuppgifter från Göteborgs Stad ska inte formuleras så att de som läser får uppfattningen att informationsspridningen sker på uppdrag av Göteborgs Stad
- Förhindra att obehöriga kan använda IT-resurser och information samt att hantera anförtrodd IT-utrustning på ett sådant sätt att stöld och obehörig åtkomst förhindras

[1] Med ansvarig avses här den närmast verksamhetsansvariga personen för respektive IT-användare såsom närmaste chef, uppdragsgivare etc

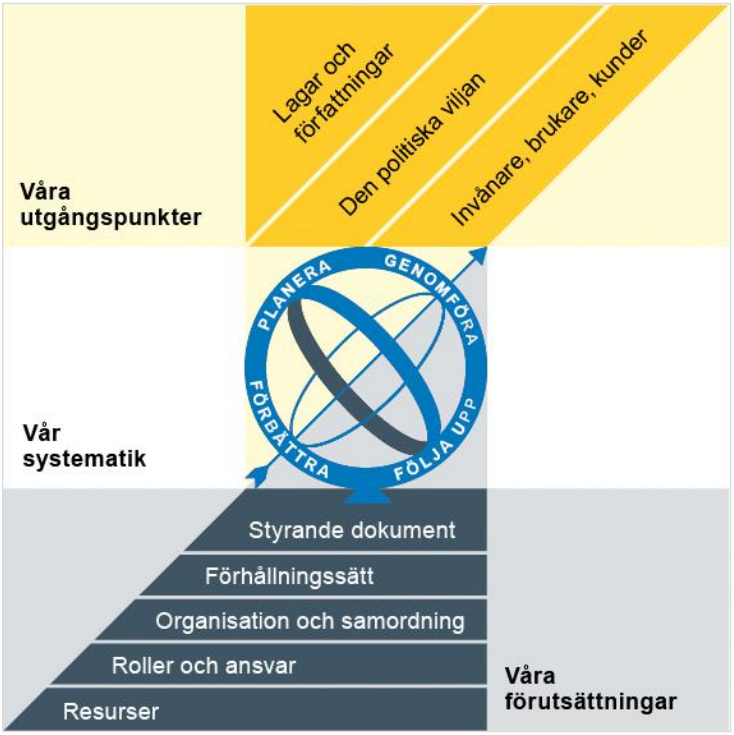
Göteborgs Stads regler för användande av e-post

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.

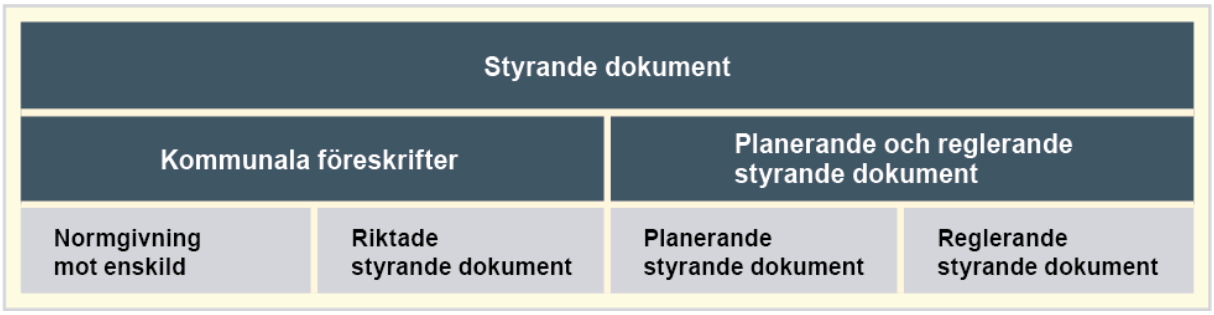


Om Göteborgs Stads styrande dokument

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

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.

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

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.