Göteborgs Stad

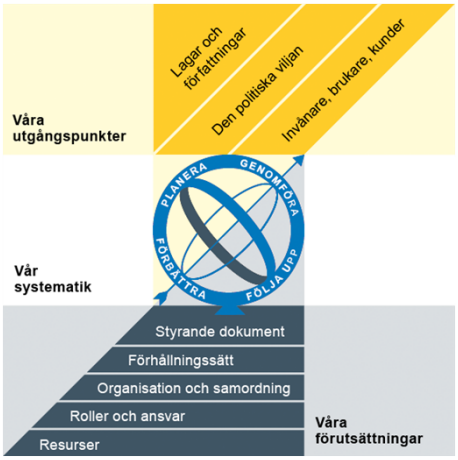
Nämnden för Intraservices anvisning för autentisering och åtkomst

IIFS 4

Reglerande styrande dokument

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

Göteborgs Stads styrsystem



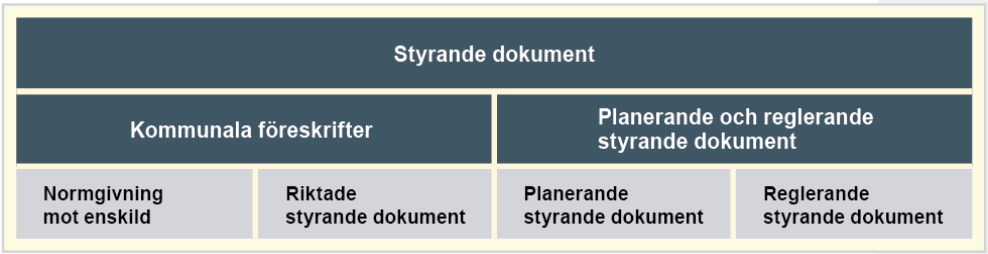
Utgångspunkterna för styrningen av Göteborgs Stad är lagar och författningar, den politiska viljan och stadens invånare, brukare och kunder. För att förverkliga utgångspunkterna behövs förutsättningar av olika slag. Stadens politiker har möjlighet att genom styrande dokument beskriva hur de vill realisera 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:**
Nämnden för Intraservice	Nämnden för Intraservice CISO, Användare, Systemägare, Tjänsteägare	0193/24	[Text]
Dokumentsort:	**Giltighetstid:**	**Senast reviderad:**	**Dokumentansvarig:**
Anvisning	**2024-09-02 och tills vidare**	2024-06-03	Intraservices CISO

Bilagor:

Innehåll

Inledning

Syftet med denna anvisning

Anvisningen ska utifrån Göteborgs Stads riktlinje för informationssäkerhet ange hur Intraservice ska autentisera identiteter och fastställa åtkomst till informationstillgångar eller informationsbärare. Anvisningen ska säkerställa att autentiseringsnivåer är i proportion till skyddsvärdet på informationsmängderna användaren begär åtkomst till.

Vem omfattas av anvisningen

Denna anvisning påverkar användare som behöver åtkomst till informationstillgångar, tjänster eller informationsbärare som kan innehålla informationstillgångar; samt för de som ansvarar för att applicerbara säkerhetsåtgärder kring autentisering är implementerade på de system och tjänster som kräver det baserat på skyddsvärdet hos informationstillgångarna.

Med användare menas anställda, konsulter, politiker och leverantörer.

Med externa användare menas elever, medborgare och andra icke-anställda som har behov av åtkomst till informationstillgångar som förvaltas av Intraservice.

Bakgrund

Göteborgs Stads riktlinje för informationssäkerhet framgår bland annat att nämnder och styrelser ska säkerställa att åtkomst och behörighet till information ges restriktivt utifrån arbetsuppgifter och organisatorisk tillhörighet, samt att åtkomst till information bygger på personliga användaridentiteter och är spårbar till en fysisk person. Vidare ska nämnder och styrelser säkerställa att autentisering och åtkomstkontroll till administratörs- och systemkonton sker med unika lösenord och baseras på flerfaktorsautentisering.

Den nya cybersäkerhetslagen, baserad på NIS2-direktivet, kräver också strategier för åtkomstkontroll och tillgångsförvaltning, säkrade lösningar för kommunikation, och lösningar för autentisering, där autentisering syftar till användning av multifaktorautentisering eller kontinuerlig autentisering som en del av riskhanteringsåtgärder.

Koppling till andra styrande dokument

Styrande dokument	Koppling till denna anvisning
Göteborgs stads riktlinje för informationssäkerhet	Fördelar ansvar och ställer krav. Ställer krav på att autentisering och åtkomstkontroll till administratörs- och systemkonton sker med unika lösenord och baseras på flerfaktorsautentisering. Anvisningen utökar kravet till att även omfatta informationstillgångar.
Nämnden för Intraservices anvisning för informationssäkerhet	Grundläggande bestämmelser för informationssäkerhetsarbete
Cybersäkerhetslagen 3Kap	Krav på lösningar för autentisering

Stödjande dokument

Stödjande dokument i form av rutiner och instruktioner tas fram och godkänns av Nämnden för Intraservices CISO.

Anvisning

Princip

Åtkomst beviljas enligt principen om minsta möjliga tillgång. Konton tilldelas endast åtkomst till den information de behöver för att utföra sina uppgifter och roller.

Sekretessavtal

Samtliga användare som ges åtkomst till konfidentiell information ska underteckna sekretessavtal eller annan överenskommelse innan de ges åtkomst till information eller informationsbärare.

Rollbaserad åtkomst

Åtkomst till system baseras på roller. Åtkomst beviljas av informationsägare eller systemägare och ska godkännas formellt.

Unik identifierare

Användare tilldelas en unik identifierare för att säkerställa individuell ansvarsskyldighet. Användarnamn och identifierare ska inte delas.

Lösenord

Där åtkomst till system och information verifieras med lösenord gäller följande:

- En ny användare tilldelas lösenord som måste ändras vid första inloggningen.
- Standardlösenord som levereras med system ska ändras omedelbart efter installation.
- Lösenord ska inte vara generiska, delade eller satta på gruppnivå.
- Lösenord ska hållas konfidentiella och inte skrivas ner analogt. Lösenord ska inte visas när de skrivs in.
- Lösenord ska inte inkluderas i skript, kod eller makron.
- Lösenord ska krypteras vid överföring över nätverk.
- Lösenord ska ha en minimilängd och format, vilka ska specificeras i stödjande dokument till denna anvisning
- Systemsessioner som är inaktiva i en viss period ska kräva lösenord för att återfå åtkomst.
- Tidigare lösenord ska inte kunna återanvändas under ett antal cykler.

Åtkomsthantering

Systems åtkomsthantering:

- Visar inte system- eller applikationsidentifierare förrän inloggningsprocessen har slutförts
- Visar en allmän varning om att klienten eller systemet endast ska användas av auktoriserade användare, vid åtkomst till administrativa eller priviligierade system
- Visar inte hjälpmeddelanden under inloggningsproceduren som skulle hjälpa en obehörig användare ta reda på inloggningskrav
- Validerar inloggningsinformationen endast efter att all indata har matats in. Om ett fel uppstår ska systemet inte ange vilken del av data som är korrekt eller inkorrekt
- Skyddar mot forcerade inloggningsförsök
- Loggar misslyckade och lyckade inloggningsförsök
- System ska låsa ut användare efter ett antal misslyckade inloggningsförsök.
- Genererar en säkerhetshändelse vid potentiellt försök till eller genomförd deaktivering av inloggningsskydd
- Visar inte ett lösenord i klartext som standard när det skrivs in
- Skickar inte lösenord i klartext över nätverk
- Avslutar inaktiva sessioner efter en definierad inaktivitetsperiod, särskilt på offentliga platser, utanför Stadens nätverk eller på mobila enheter och beroende på informationens skyddsvärde
- Begränsar anslutningstider för att ge ytterligare säkerhet för högriskapplikationer

Autentisering

Användare ska identifieras och autentiseras innan de får åtkomst till system, tjänster eller information.

Styrkan på autentiseringen (tillitsnivåer) ska motsvara klassningsnivån för den information som användaren ska ha tillgång till. Autentiseringstekniken ska anpassas efter nationella och internationella regelverk och tillitsramverk samt beskrivas i underliggande instruktioner för autentisering och åtkomst.

- Externa användare från europeiska länder (svenska och europeiska medborgare) ska kunna använda sina nationella e-legitimationer vid inloggning till offentliga tjänster enligt eIDAS-förordningen
- Användare inom Staden ska autentisera sig med någon av de e-legitimationer som godkänts och säkerställts av DIGG, myndigheten för digital förvaltning i sitt tillitsramverk

Kommentar [EÖ1]: Sista-minuten kommentar här: politiker måste också ingå.

Granskning av åtkomsträttigheter

Endast behörig personal får skapa, modifiera, avsluta eller radera användarkonton, vilket även ska dokumenteras. Individuella linjechefer godkänner skapande, modifiering, avslut

och radering av konton. Verksamhets-, system- eller informationsägare godkänner åtkomst till system och information.

Det ska finnas en process för att tydligt ange åtkomstbehovet och godkännande ska ske via e-post, digital signatur eller i ett ärende. Alla användare som begär lösenordsåterställningar eller ändringar av autentiseringsuppgifter ska verifiera sin identitet.

Användares åtkomst till system ska granskas minst årligen för att säkerställa att det fortfarande finns åtkomstbehov. Inaktiva och vilande konton ska undersökas, och lämpliga åtgärder ska vidtas, inklusive borttagning av konton och uppdatering av relevant dokumentation kring konton och användare. Huvudsystemet för användaråtkomst ska granskas för att säkerställa dess lämplighet.

Ansvariga chefer eller HR ska informera om det datum då en användare slutar sin anställning eller tjänst. När en användare lämnar sin anställning eller tjänst återkallas all åtkomst till alla system och data som registrerats i listan över rollbaserad åtkomst. Användar-ID, lösenord och autentiseringsuppgifter för avslutade användare ska inte återanvändas för en ny användare.

Privilegierade- och administratörskonton

Administratörsbehörigheter tillhandahålls inte till användare, inklusive men inte begränsat till bärbara datorer och mobila enheter. Där det är möjligt ska administratörer tilldelas särskilda privilegie- eller administratörskonton utöver det normala användarkontot för specifik användning vid utförande av privilegiebaserade eller administratörsbaserade uppgifter.

Privilegie- och administratörskonton ska inte delas eller vara generiska, och dom ska ha unika lösenord. Privilegie- och administratörskonton ska vara möjliga att identifiera på ett tydligt sätt. Det ska finnas ett uppdaterat register över privilegie- och administratörskonton som visar på giltighetstid och vem som godkänt kontot. Privilegie- och administratörskonton ska loggas och övervakas. Privilegie- och administratörskonton tillhandahålls under en bestämd tidsperiod, därefter uppdateras dom eller tas bort.

Fjärråtkomst

Klienter hanterade av Intraservice

Fjärråtkomst till Stadens nätverk och molnbaserade tjänster via utrustning hanterad av Intraservice följer samma regler som täckts av denna anvisning med tillägget av kravet på flerfaktorsautentisering. Fjärranslutningar ska initieras med flerfaktorsautentisering och ska kopplas ner efter en bestämd tidsperiod.
Det ska finnas en uppdaterad lista över användare med fjärråtkomst till interna nätverkssystem.
Det ska finnas avtal som reglerar arbete som ska utföras och ett tillämpligt sekretessavtal för externa parter.

Klienter som inte hanteras av Intraservice

Åtkomst beviljas endast förutsatt att det finns ett avtal som reglerar arbete som ska utföras och ett tillämpligt sekretessavtal. Åtkomst beviljas för en specifik tid, till specifika system eller tjänster, för en specifik individ och tillhandahålls med en formell, giltig och auktoriserad åtkomstbegäran.
Åtkomst tas bort omedelbart efter att arbetet är utfört. Det ska finnas en uppdaterad lista över alla parter med åtkomst, samt vad de har åtkomst till och hur länge.

Anslutning från annat land

Anslutningar från annat land än Sverige ska godkännas av chef och genomgå en extra autentisering (tre faktorer).

Övervakning och Rapportering

Åtkomst till system ska övervakas och rapporteras. Åtgärder som direkt eller indirekt påverkar eller kan påverka konfidentialitet, riktighet eller tillgänglighet hos information hanteras via incidenthanteringsprocessen.

Efterlevnad

Åtgärder för efterlevnad

Intraservice Enhet för Informationssäkerhet ska verifiera efterlevnaden av denna anvisning genom olika metoder, inklusive men inte begränsat till rapporter, interna och externa revisioner samt återkoppling till ägare av anvisningen.

Undantag

Alla undantag från anvisningen måste följa undantagsprocessen och rapporteras till Ledningen för Intraservice.

Icke-Efterlevnad

En anställd som bryter mot denna anvisning kan vara föremål för disciplinära åtgärder.

Kontinuerlig Förbättring

Anvisningen ska uppdateras och granskas som en del av den kontinuerliga förbättringsprocessen.

Applicerbara säkerhetskontroller

Denna anvisning svarar upp mot åtgärder ställda i ISO/EIC 27001:2022 enligt nedan.

ISO/EIC 27001:2022	
ISO27002:2022 A.5.1 Riktlinje för informationssäkerhet ISO27002:2022 A.5.3 Uppdelning av arbetsuppgifter och ansvar ISO27002:2022 A.5.4 Ledningens ansvar ISO27002:2022 A.5.10 Tillåten användning av information och andra relaterade tillgångar ISO27002:2022 A.5.12 Informationsklassning ISO27002:2022 A.5.15 Åtkomstkontroll ISO27002:2022 A.5.16 Identitetshantering ISO27002:2022 A.5.17 Autentiseringsinformation ISO27002:2022 A.5.18 Åtkomsträttigheter	ISO27002:2022 A.5.19 Informationssäkerhet i leverantörsrelationer ISO27002:2022 A.5.36 Efterlevnad av policyer, regler och standarder för informationssäkerhet ISO27002:2022 A.8.2 Privilegierade åtkomsträttigheter ISO27002:2022 A.8.3 Begränsning av åtkomst till information ISO27002:2022 A.8.4 Tillgång till källkod ISO27002:2022 A.8.5 Säker autentisering ISO27002:2022 A.8.11 Datamaskning