

Intraservices arbete med informationssäkerhet 2023

2023-03-21 (0176/23)

Anna-Lena Björk – Informationssäkerhetschef (CISO)

Patrik Skog – Kanslichef

0176/23 Förbättra Intraservice säkerhetshållning

Stads-
revisionen
Årligen

0196/22
Stadsrevisionens granskning av
verksamhetsåret 2022

Stadsrevisionen önskar yttrande
från nämnd.

Yttrande godkänns och översänds

Stadsrevision

Regionarkivet
(ca 3-5 års
intervall)

0351/22
Regionarkivets tillsynsrapport
2022

Regionarkivet önskar nämndens
skriftliga återkoppling i ärendet
senast den 15 september 2023.

Yttrande godkänns och översänds

Regionarkivet

Dataskydds-
ombuden
Årligen

0120/22
Dataskyddsenhetens årsrapport
2022

Information

Ta fram en handlingsplan med tidplan för att omhänderta
brister i kontrollområden som framkommer i
dataskyddsenhetens årsrapport 2022.

Förvaltningen
återrporterar

Intraservice
Årligen

0124/23
Intern efterlevnadskontroll inom
Intraservice informationssäkerhet
2023

Information

Kontinuerlig information om 0176/23

Nämnd
/politisk
vilja



Göteborgs
Stad

Kommer komma

Är genomfört

Under 2023 kommer Intraservice att fokusera på informationssäkerhet

- Intraservice kommer under 2023 att arbeta med uppdrag kopplade till informationssäkerhet.



Varför ska Intraservice fokusera på informationssäkerhet under 2023?



Intraservice ska genomföra uppdrag kopplade till:

- Intraservice tjänsteleveranser
- Dataskyddsombudens rapport 2021 och 2022
- Stadsrevisionens rapport 2021 och 2022
- Tillsynsbeslut efter systemtillsyn av arkivvård
- Tekniskt arkivansvar
- Interna analyser

Intraservice uppdrag som leverantör tillhörande informationssäkerhet



Intraservice uppdrag

- Intraservice har ett särskilt ansvar som leverantör av gemensamma tjänster och tjänster tillhörande digital infrastruktur.
- Intraservice ansvarar för att det digitala informationsutbytet med omvärlden sker samordnat, med rätt säkerhet och via standardiserade funktioner och format.
- **Intraservice uppdrag innefattar ett aktivt arbete med informationssäkerhet. Övergripande innebär detta att se till att informationstillgångar tillhandahållna av Intraservices tjänster finns tillgängliga när de behövs, att de är korrekta, och att obehöriga inte får åtkomst till dem.**

Intraservice ansvarar dessutom för att:

- löpande följa upp att tillämpliga lagar, föreskrifter, styrande dokument och beslut följs samt att beslutad säkerhetsnivå uppfylls
- löpande följa upp väsentliga störningar och brister avseende säkerhet
- direkt rapportera nyupptäckta avvikelser mot säkerhetskrav till berörda verksamheter samt beredningsfunktionen för den strategiska samordningsgruppen
- årligen formellt presentera en uppföljningsrapport för berörda verksamheter och strategisk samordningsgrupp.

Vad avses med informationssäkerhet?

Informationssäkerhet

Informationssäkerhet handlar om **säker informationsförvaltning**, d.v.s. att ge informationen rätt skydd både ur ett administrativt och tekniskt perspektiv

Rätt skydd

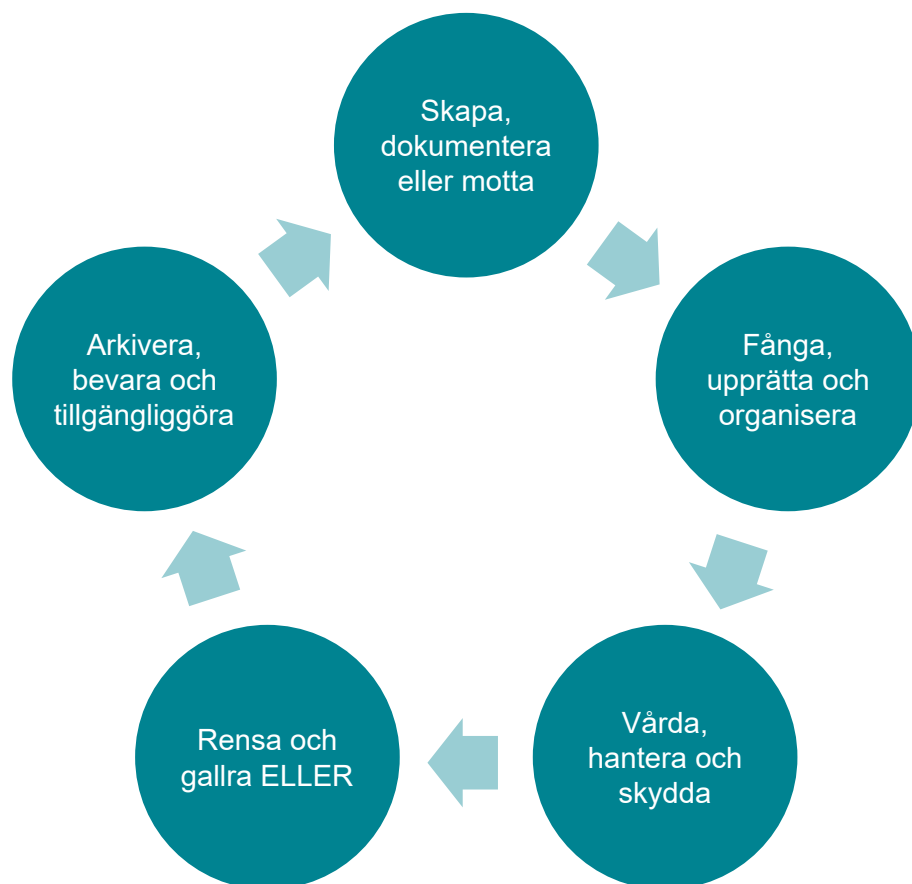
- Vad som är rätt skydd avgörs av
 - de **krav** som gäller för verksamheten
 - det **hot** och de **sårbarheter**, samt **risker**, som verksamheten behöver skydda sig mot

Informationssäkerhet



- Intraservice behöver rätt skydd utifrån
 - Lagkrav
 - Styrande dokument
 - Funktionella krav på tjänsteleveranserna
 - Rapporteringsplikt
 - Hot från olika typer av aktörer
 - Sårbarheter
 - Administrativa och tekniska risker

Kort om informationsförvaltning



Informationsförvaltning handlar om hur information:

uppstår, klassificeras, dokumenteras, registreras, hanteras, lagras, sprids, arkiveras och återanvänds.

Flera av dessa aktiviteter sker parallellt och är ömsesidigt beroende av varandra.

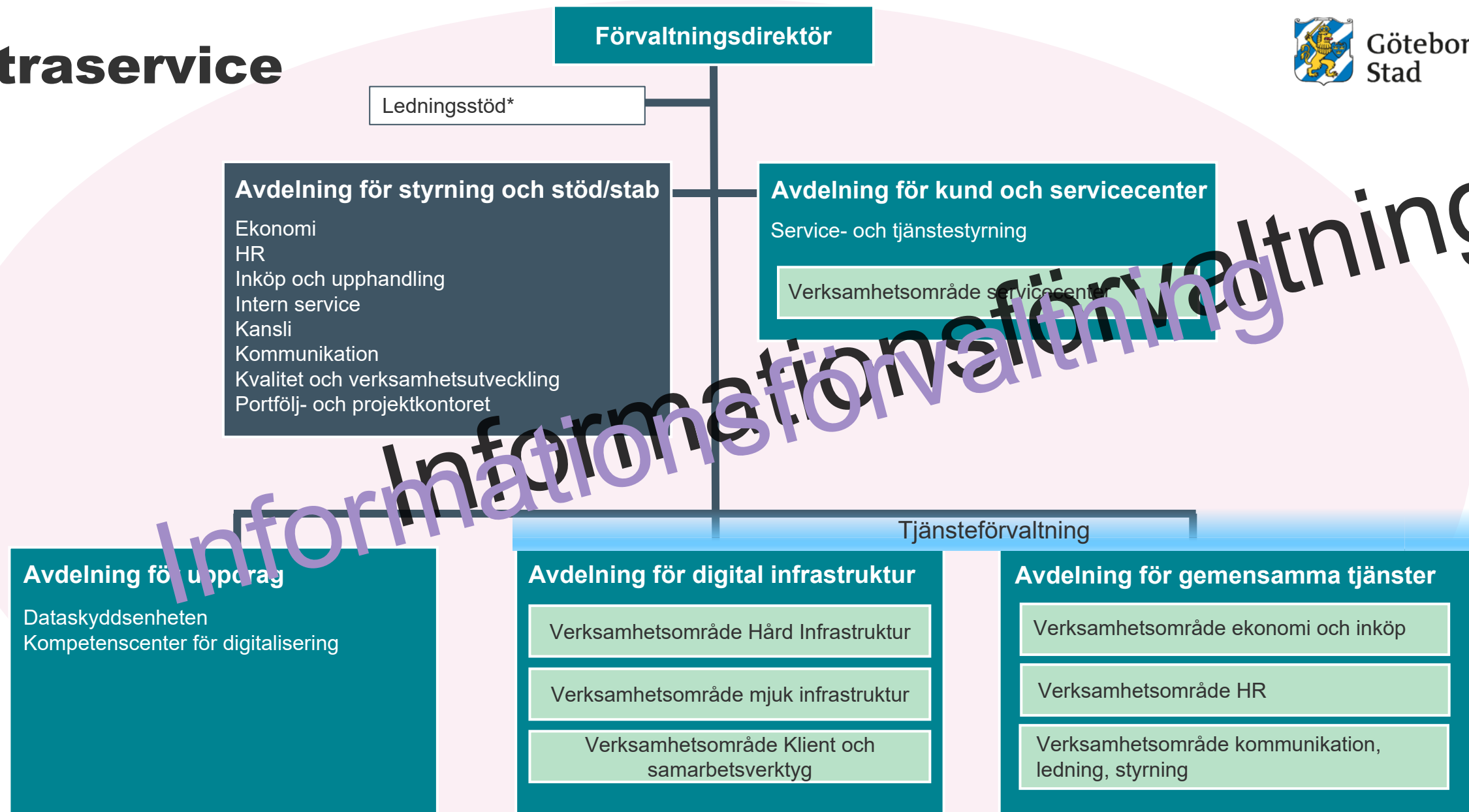
Det ska vara lätt att göra rätt utifrån gällande krav.

För att uppnå detta behöver man ha ett ordnat och strukturerat arbetssätt. Förutom strategier och dokumenterade rutiner behöver det finnas vägledande processer och arbetssätt, och lämpliga IT-stöd.

Intraservice



Göteborgs
Stad



* förvaltningscontroller och säkerhetsskyddschef

Revisioner, rapporter och interna analyser



Stadsrevisionens rapporter
2021 och 2022.



Dataskyddsbudens
årsrapporter 2021 och 2022.



Tillsynsbeslut efter
systemtillsyn av arkivvård.



Interna analyser.

Stadsrevisionens rapport 2021 och 2022

Stadsrevisionens rapport 2021

Stadsrevisionens rapport 2021

- Nämnden bör se till att det finns **dokumenterade arbetssätt, uttalade ansvar och beslutsmandat** som säkerställer den interna kontrollen när det gäller personuppgiftsansvaret och i uppdragen som stadens dataskyddsombud, tjänsteleverantör och personuppgiftsbiträde.
- Säkerställa **ansvar och roller samt utveckla uppföljning gällande efterlevnad av informationssäkerhetskrav och dataskyddsförordningen.**

Stadsrevisionens rapport 2021, forts.

- Nämnden skall hålla sig väl informerad om dataskyddsenhetens och it-säkerhetsavdelningens arbete och rapportering.
- Nämnden bör säkerställa att konstaterade brister och förbättringsförslag som framkommer i dessa rapporter omhändertas,

Stadsrevisionens rapport 2021

Stadsrevisionens rapport 2021, forts

- Nämnden bör besluta om handlingsplaner och fastställa tillfällen för återrapporeringar och uppföljningar.
- Vidare skall förvaltningen säkerställa rapportering till nämnd, prioriterings och beslutsråd för tjänsteplan och stadsdirektörens beslutsstödsfunktion.

Stadsrevisionens rapport 2021, forts.

- Komplettera med nödvändig dokumentation, dokumenterade arbetssätt, uttalade ansvar och beslutsmandat gällande
 - Intraservice som personuppgiftsansvarig
 - Intraservice som dataskyddsombud
 - Intraservice som tjänsteleverantör och personuppgiftsbiträde

Stadsrevisionens rapport 2022

Inväntar formell rapport

Dataskyddsbuds årsrapport 2021 och 2022

Dataskyddsbuds årsrapport 2021 och 2022

Dataskyddsbud fokuserar på vad dataskyddsförordningen (GDPR) anger.

Årsrapport för dataskyddsarbete 2021 och 2022 presenterar resultat av fasta kontrollpunkter för Intraservice, samt särskilda iakttagelser.

- Kontrollpunkt 1: Dataskyddsorganisation
- Kontrollpunkt 2: Personuppgiftsincidenter
- Kontrollpunkt 3: Biträdesavtal och andra överenskommelser
- Kontrollpunkt 4: Personuppgiftsregister
- Kontrollpunkt 5: Övergripande strategi för dataskydd
- Kontrollpunkt 6: Utbildning
- Kontrollpunkt 7: Integritetspolicy
- Kontrollpunkt 8: Mejl och dokumenthantering
- Kontrollpunkt 9: Konsekvensbedömning/samråd
- Kontrollpunkt 10: IT-projekt och upphandling
- Kontrollpunkt 11: IT-system och digitala verktyg
- Kontrollpunkt 12: Hantering av registrerades rättigheter

Dataskyddsombuds årsrapport 2021 och 2022

Kontrollpunkt 1: Dataskyddsorganisation

- Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

Kontrollpunkt 2: Personuppgiftsincidenter

- Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att identifiera och hantera personuppgiftsincidenter.

Kontrollpunkt 3: Biträdesavtal och andra överenskommelser

- Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd, och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i personuppgiftsregistret. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

Kontrollpunkt 4: Personuppgiftsregister

- Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande personuppgiftsregister innefattas.

Dataskyddsbuds årsrapport 2021 och 2022

Kontrollpunkt 5: Övergripande strategi för dataskydd

- Kontrollpunkten avser verksamhetens övergripande strategi för att arbeta med dataskydd.

Kontrollpunkt 7: Integritetspolicy

- Kontrollpunkten avser verksamhetens utformning samt tillhandahållande av dess integritetspolicy till registrerade (både internt och externt). Även verksamhetens rutin för att upprätthålla en aktuell integritetspolicy omfattas.

Kontrollpunkt 6: Utbildning

- Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

Kontrollpunkt 8: Mejl och dokumenthantering

- Kontrollpunkten avser verksamhetens rutiner för e-post och dokumenthantering. I detta är en aktuell och fastställd dokumenthanteringsplan med gallringsbeslut en förutsättning för att verksamheten ska kunna säkra följsamhet gentemot dataskyddsförordningen. Även verksamhetens rutin för att säkerställa att gallringsrutiner för personuppgifter följs innefattas.

Dataskyddsombuds årsrapport 2021 och 2022

Kontrollpunkt 9: Konsekvensbedömning/samråd

- Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras, samt rutiner kopplat till detta.

Kontrollpunkt 11: IT-system och digitala verktyg

- Kontrollpunkten avser verksamhetens rutiner för att säkerställa att verksamhetens personuppgiftshantering inom ramen för IT-system och digitala verktyg är förenlig med dataskyddsförordningen. Rutin för att säkerställa och kontrollera att dessa system/tjänster uppfyller kraven på dataskydd ingår.

Kontrollpunkt 10: IT-projekt och upphandling

- Kontrollpunkten avser verksamhetens organisation och rutiner för hantering av dataskyddsfrågor inom IT-projekt och upphandling. I detta ingår till exempel hur verksamheten integrerar dataskyddsfrågor i arbetet med upphandling av nya, samt utvecklingen av, befintliga system och tjänster.

Kontrollpunkt 12: Hantering av registrerades rättigheter

- Kontrollpunkten avser verksamhetens förutsättningar och rutiner för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering.

Dataskyddsbuds årsrapport 2021 och 2022

Särskilda iakttagelser 2021

- Tredjelandsoverföring och användning av sociala medier
- Intraservice ansvar som personuppgiftsbiträde

Särskilda iakttagelser 2022

- Utredning av Intraservice personuppgiftsansvar i nya styrmodellen

I årsrapport för dataskyddsarbete 2021 ges rekommendation att fokusera på kontrollpunkterna 1, 4, 5, 6, 7, 8 och 9.

Förvaltningen rekommenderas även vidta åtgärder för att hantera de rekommendationer som lämnats med anledning av förvaltningens ansvar som personuppgiftsbiträde och tjänsteleverantör åt övriga förvaltningar och bolag inom Göteborgs Stad.

I årsrapport för dataskyddsarbete 2022 ges rekommendation att fokusera på kontrollpunkterna 1, 4 och 5.

Dataskyddsombuds årsrapport 2021 och 2022

Särskilda iakttagelser 2021: Tredjelsöverföring och användning av sociala medier

- Personuppgiftsbehandlingar vid användning av sociala medier som innebär tredjelsöverföring.

Särskilda iakttagelser 2022: Utredning av Intraservice personuppgiftsansvar i nya styrmodellen

- I samverkan med parter inom Göteborgs Stad tydliggöra ansvarsförhållande för de personuppgiftsbehandlingar som ingår i tjänster/system som är gemensamma för flera förvaltningar/bolag inom Göteborgs Stad.

Särskilda iakttagelser 2021: Intraservice ansvar som personuppgiftsbiträde

- I samverkan med parter inom Göteborgs Stad tydliggöra ansvarsförhållande och Intracervice del av leverantörskedjan och roll i staden..



Arkivansvar utifrån två perspektiv

Intraservice

Patrik Skog - Kanslichef

Stadsrevisionens och Arkivnämndens rapporter 2022

- Upprätta arkivförteckning enligt styrande dokument
- Planera övergång till processorienterad arkivförteckning i samråd med Regionarkivet
- Upprätta förteckning över IT-system som innehåller elektroniska allmänna handlingar enligt styrande dokument
- Upprätta plan för bevarande av elektroniska handlingar
- Uppdatera dokumenthanteringsplan och besluta om att fastställa ändringar enligt styrande dokument
- Utreda vilka handlingar som är möjliga att gallra men inte omfattas av gallringsbeslut
- Utreda och samråda med Regionarkivet om arkivbildning

Tekniskt arkivansvar - bakgrund

- ”Arkivnämnden beslutar enligt 2 kap. 19 § *Göteborgs Stads föreskrifter och riktlinjer om arkiv- och informationshantering* att nämnden för Intraservice ska vara tekniskt arkivansvarig för information i elektroniska system som används av mer än en myndighet i Göteborgs Stad
- Det tekniska arkivansvaret omfattar enbart de elektroniska system som nämnden för Intraservice nu och i framtiden förvaltar och som används av flera kommunala förvaltningar, bolag och stiftelser.”

Samråd har genomförts med Regionarkivet på tjänstepersonsnivå för att få bild över hur arbetet skulle kunna organiseras.

Vad ingår i det tekniska arkivansvaret?

- ansvar för att bevara, verkställa gallring och leverera information som hanteras och förvaras i IT-lösningen, på uppdrag av arkivbildaren/informationsägaren
- val av lagringsmetod och skydd för lagrad information, exempelvis konvertering till arkivgodkända format
- att säkerställa att Arkivnämndens krav för arkivering följs vid upphandling eller utveckling av IT-lösningar
- samordning av leveransarbete till mellanlagringstjänster och system för bevarande
- kontakter med leverantörer när det gäller systemfunktioner som berör arkiveringen
- att upprätta den plan för bevarande av elektroniska handlingar som avses i 4 kap. 25 § Föreskrifter och riktlinjer om arkiv- och informationshantering på egen hand eller tillsammans med arkivbildaren/informationsägaren
- att lämna ut information ur IT-lösningen till den myndighet som äger informationen om den inte har direktåtkomst till informationen. I det tekniska arkivansvaret ingår inte det som varje myndighet ansvarar för

Ovanstående sammanfaller i stor utsträckning med utvecklingsarbetet avseende informationssäkerhet och dataskydd

Förvaltningens interna analyser

Interna analyser

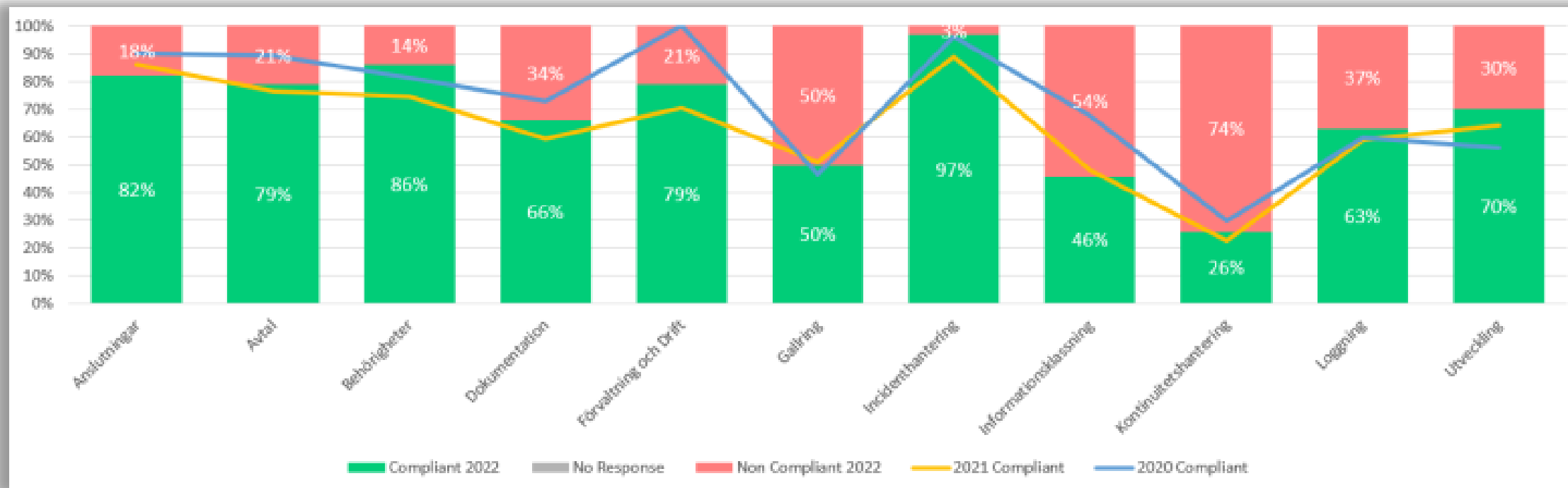
Interna analyser består av

- Årlig efterlevnadskontroll
- Oberoende granskningar av infrastrukturella lösningar och system

Kontrollpunkter

- Specifika kontroller med perspektiv på IT-säkerhet
- Avtal
- Behörigheter
- Dokumentation
- Förvaltning och drift
- Gallring
- Incidenthantering
- Informationsklassning
- Kontinuitetshantering
- Loggning
- Utveckling

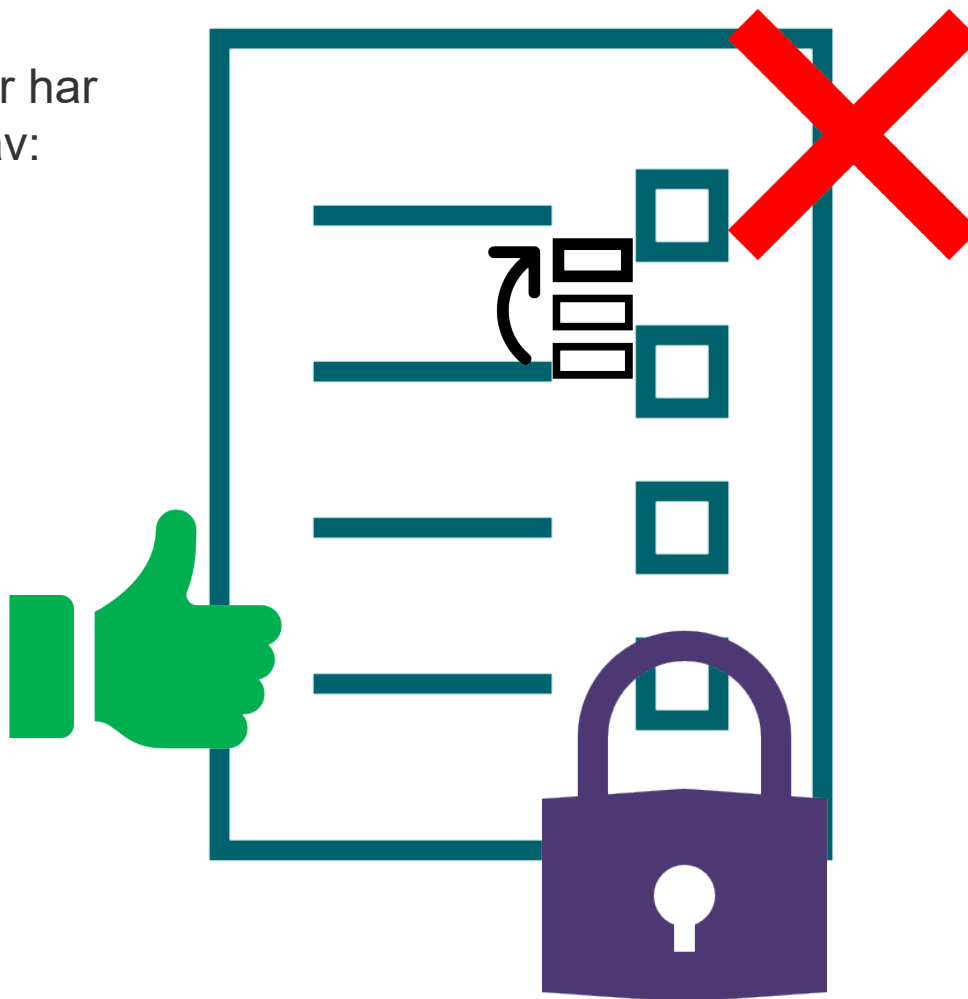
Efterlevnadskontroll 2022



Oberoende granskningar 2022 och 2023

Oberoende granskningar har genomförts/genomförs av:

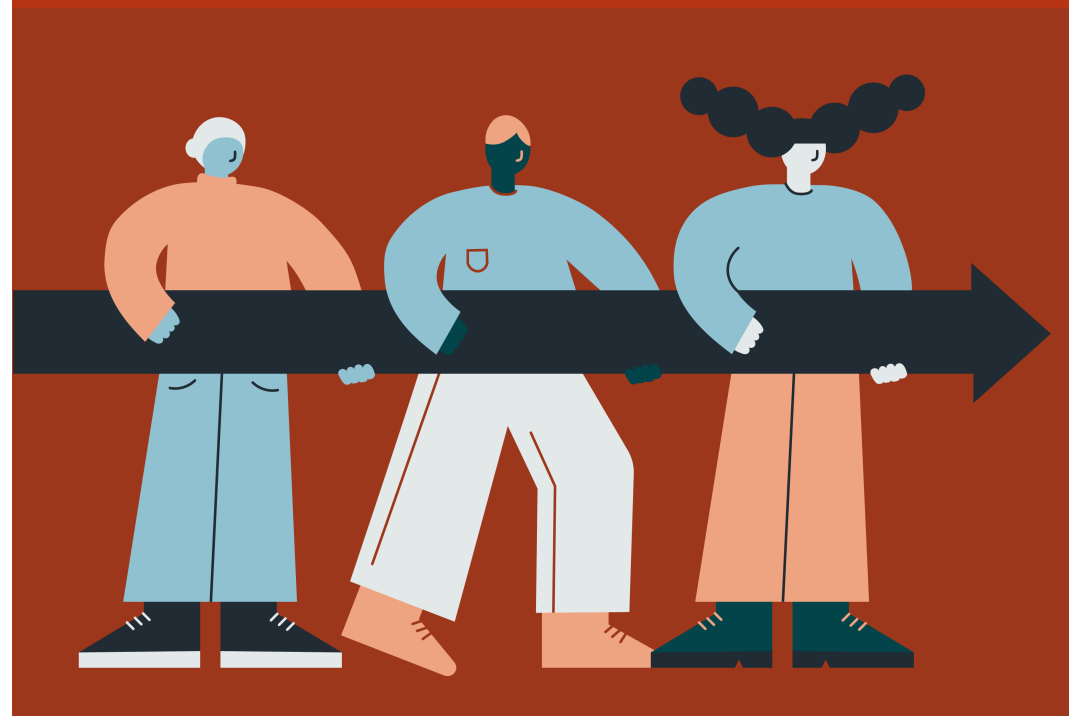
- Digital Infrastruktur
- System



Vad behöver åtgärdas?

Dokumentera rutiner, arbetssätt och roller

- Dokumenterade **rutiner** ska tas fram som **säkerställer efterlevnad** av lagar, förordningar, styrande dokument.
- Dokumenterade **arbetssätt** och **tydliggörande** av roller, **ansvar** och **mandat** ska tas fram för att
 - reglera hur styrningen av informationssäkerhetsarbetet ska ledas och återkopplas,
 - ange hur uppföljning av informationssäkerhetsarbetet ska ske samt hur efterlevnaden ska säkerställas,
 - motverka ”stuprörseffekten” och
 - säkerställa att ansvaret för informationssäkerhet är känt och accepterat, samt
 - att det tydligt framgår hur informationsspridning ska genomföras
 - vart frågor och synpunkter ska riktas för att omhändertas på bästa sätt.



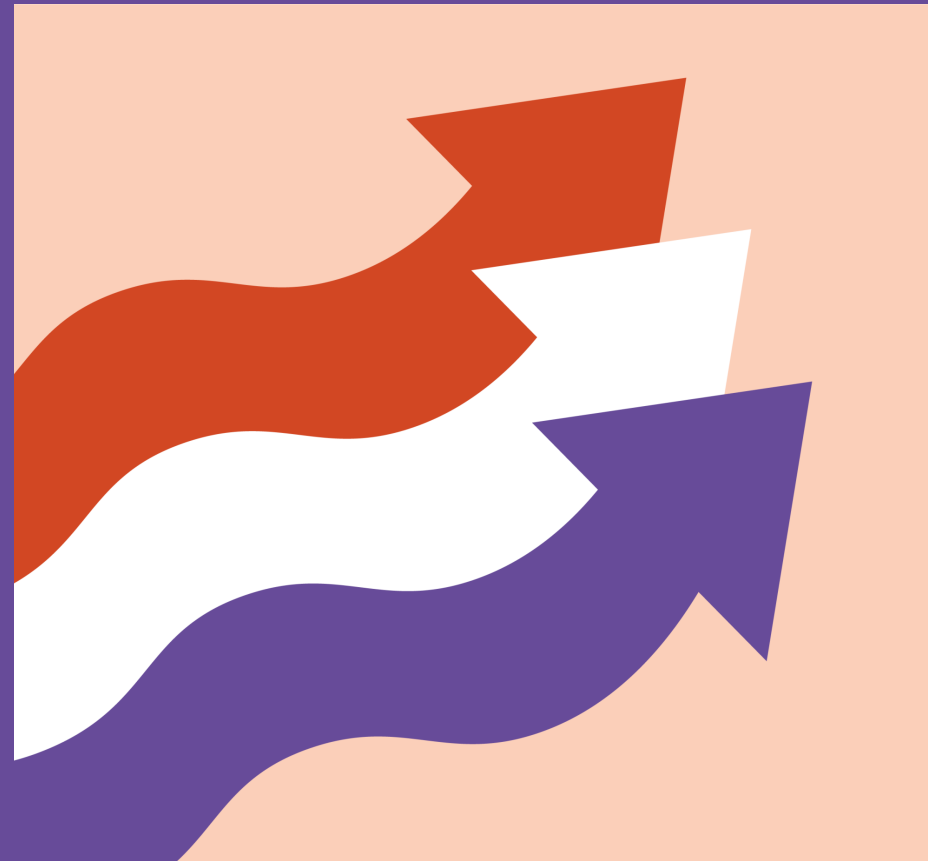
Etablera och uppdatera processer

- Processer och arbetssätt för **informationsklassning** ska etableras för att värdera förvaltningens information. Detta utifrån vilka konsekvenser otillräckligt skydd för informationens konfidentialitet, riktighet och tillgänglighet skulle kunna få.
- Intraservice ska etablera processer och arbetssätt för **riskhantering** i syfte att identifiera vilka åtgärder som behöver vidtas, för att undvika en oönskad situation. Att identifiera risker innebär även en beredskap för de åtgärder som krävs om en risk inträffar.
- Befintliga processer och arbetssätt för **incidenthantering** ska ses över och uppdateras. Bland annat med inriktning på personuppgiftsincidenter, informationssäkerhetsincidenter och det vi inom Intraservice benämner som "oegentligheter".



Etablera och uppdatera processer

- Etablering av processer och arbetssätt tillhörande **kontinuitetshantering** ska ske för att säkerställa att Intraservice, som förvaltning och leverantör av tjänster, har tillräcklig beredskap för att förhindra och hantera ett driftstopp vid händelse av en IT-incident.
- Även processer och arbetssätt tillhörande **projekt, inköpsuppdrag** och **changehantering** ska tas fram/uppdateras. Detta gäller tekniska såväl som administrativa informationssäkerhetsrelaterade aktiviteter tillhörande anskaffning, utveckling och avveckling av tjänster/system.
- Processer och arbetssätt ska tas fram som anger hur **medvetenheten och kunskap om informationssäkerhet** ska förmedlas och vidmakthållas.



Se över och uppdatera register/dokumentation

- Intraservice behöver som förvaltning och leverantör:
 - Register över personuppgiftsbehandling och säkerhetsåtgärder.
 - Register över system, systemägare, biträdesavtal och tydlig information om biträdens och underbiträdens hemvist.
 - Register över genomförda konsekvensbedömningar.
 - Teknisk beskrivning av tjänst/tjänsteerbjudande.
 - Systemdokumentation och driftsdokumentation
- Detta exempelvis för att kunna tillhandahålla information om behandlingar och leverantörer till kund (förvaltningar/bolag), så att de i sin tur kan uppfylla sina åtaganden enligt artikel 28 GDPR.



Systemstöd och dokumenthantering



- Följande behöver hanteras i någon form av **systemstöd**:
Tjänstespecifikationer, funktionsbeskrivningar, systemdokumentation, driftsdokumentation och register över exempelvis personuppgiftsbehandlingar, säkerhetsåtgärder, system och leverantörer och dess underbiträden.

Intraservice upplever idag utmaningar kring åtkomst av information, gallring, och förmåga att på ett enkelt sätt söka fram och hålla informationen uppdaterad och aktuell.
- Intraservice befintliga **dokumenthanteringsplan** ska uppdateras för att bland annat säkerställa krav på lagringsminimering och allmänhetens rätt att ta del av allmän handling.

Översyn av processer och arbetssätt

Finns men ska uppdateras

- Incidenthanteringsprocessen
- Behörighetshanteringsprocessen
- Personalsäkerhetsprocessen

Behöver tas fram

- Informationsklassningsprocess
- Riskhanteringsprocess informationssäkerhet
- Informationssäkerhetsprocess för anskaffning, utveckling och avveckling av tjänster och system.
- Kontinuitetshanteringsprocess
- Säkerhetsmedvetandeprocess
- Uppföljningsprocess informationssäkerhet
- Ledningsprocess informationssäkerhet

Handlingsplan och tidplan

Handlingsplan

- **Uppdragsdirektiv för:**
 - Personuppgiftsregister kopplat till tjänsteleverans
 - Ansvarsfrågan
 - Etablering av processer och arbetssätt tillhörande kontinuitetshantering
 - Etablering av processer och arbetssätt tillhörande styrning och uppföljning av informationssäkerhet
- **Förvaltningsövergripande prioritering och planering**
- **Uppföljning**



Tidplan



Göteborgs
Stad

- **Personuppgiftsregister kopplat till tjänsteleverans**
 - **Pågår.** Efter pilot kan tidplan tas fram till samtliga tjänster.
- **Ansvarsfrågan**
 - **Pågår.** Samverkan inom Staden.
- Etablering av processer och arbetssätt tillhörande **kontinuitetshantering** (inkl. återställning)
 - Start av förstudie Q2 2023
- Etablering av processer och arbetssätt tillhörande **styrning och uppföljning av informationssäkerhet**
 - Start av förstudie Q2/Q3 2023



Preliminär tidplan för piloten (fem tjänsteleveranser) och fastställande av ansvarsroller

Februari och framåt

För varje gemensam tjänst och tjänster tillhörande digital infrastruktur analysera och dokumentera personuppgiftsbehandlingar. Tjänsten Office 365 är en av de tjänster som vi fortsätter med inom piloten.

Januari 2023

Nämnden får information om fortsatt arbete med Digitala navet och Office 365.

Februari och framåt

Granska skyddsnivå för varje personuppgiftsbehandling och ta fram ev. plan för åtgärd.

Preliminärt juni 2023

Nämnden för Intraservice tar ställning till konsekvensbedömning Office 365 och Digitala navet

Vinter

Sommar

Februari 2023

April 2023

Juni 2023

Augusti 2023

Februari – ? 2023

Arbete med definition och fastställande av ansvarsroller kopplade till personuppgiftsbehandlingar

Preliminärt maj och framåt

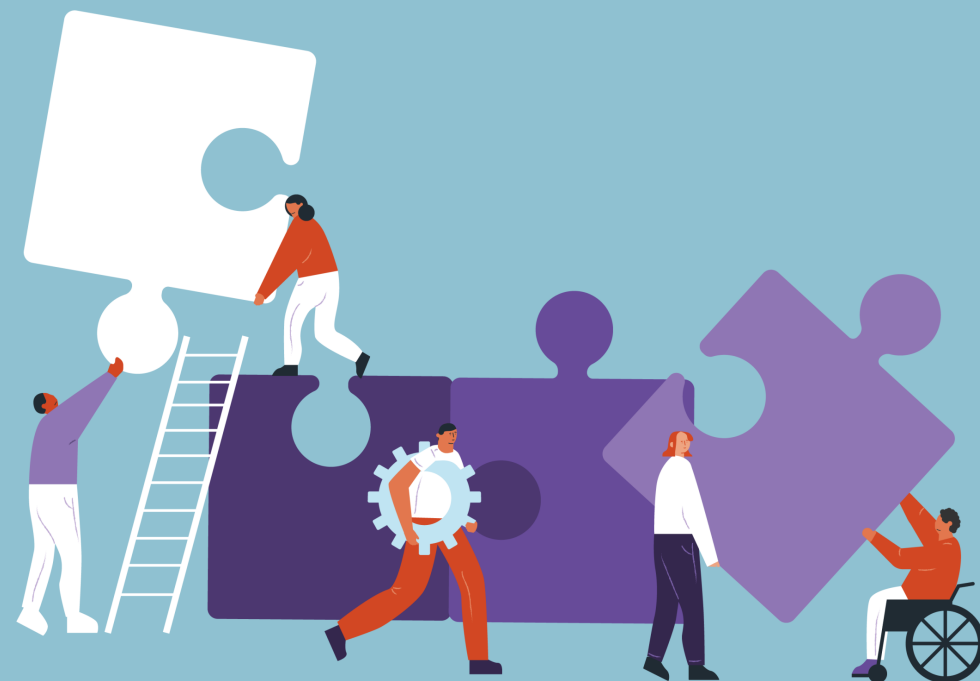
Efter fastställda ansvarsroller:

Uppdatering av riskanalyser och konsekvensbedömningar. Tjänsterna Office 365 och Digitala navet omhändertas först.

Så här går vi framåt

Intraservice fokuserar just nu på

- Framtagande av tjänstespecifikationer och funktionsbeskrivningar, där dokumentation sker av **personuppgiftsbehandlingar och säkerhetsåtgärder** (pågår sedan Q4 2022)
- Uppstart av uppdraget *Etablering av processer och arbetssätt tillhörande **kontinuitetshantering***
- Kontinuerlig förvaltningsövergripande prioritering och planering inför uppstart av **övriga uppdrag**



Omvärldsbevakning



Omvärldsbevakning

- Tredjelandspromblematiken
- NIS2 (Oktober 2024)
- Nya typer av hot och sårbarheter

NIS2

Regelverket ställer specifika krav på

- Riskhantering
- Incidenthantering (inkl. förmåga att upptäcka incidenter)
- Säkerhet i system och infrastruktur

Riskhantering betraktas enligt NIS2 som grundläggande för allt säkerhetsarbete. Kraven på incidenthantering omfattar inte bara åtgärder i samband med intrång utan även kontinuitets- och krisantering. Säkerhetskraven för system och infrastruktur påverkar nätverkssäkerhet och systemutveckling, liksom identitets- och åtkomstkontroll.



Göteborgs
Stad

Kontakt

Anna-Lena Björk

anna.bjork@intraservice.goteborg.se

Intraservice, Göteborgs Stad