



Roller och ansvar

Dataskyddsorganisation

Tekniskt arkivansvar

Informationsförvaltning

Intraservice

2024-05-23

- Bakgrund
- Tidplan
- Förslag till hur arbetet med informationssäkerhet (inkl. dataskydd och arkivansvar) kan organiseras
- Övergripande beskrivning av begreppen
 - Informationssäkerhet – Dataskydd – Informationsförvaltning - Arkivansvar - Tekniskt arkivansvar
- Systematiskt informationssäkerhetsarbete
- Roller och ansvar
 - Informationsägare, riskägare, systemägare, tekniskt arkivansvar, projektledare, processägare, processledare
- Informationsklassning
 - Utgå från ett helhetsperspektiv vid informationsklassning
- Riskhantering
- Sammanfattning

- Denna presentation ger förslag till roller, ansvar och organisation kopplade till ett systematiskt informationssäkerhetsarbetet (inkl. dataskydd och arkivansvar).
- Förslaget grundar sig på
 - 0120/22 Dataskyddsenhetens årsrapport 2022
 - 0351/22 Regionarkivets tillsynsrapport 2022
 - Intern utredning tillhörande arkivansvar och tekniskt arkivansvar
 - Befintliga roller inom förvaltningen
 - MSB:s rekommendationer kring organisation, roller, ansvar och mandat kopplat till informationssäkerhet
 - Göteborgs Stads styrande dokument
 - Information om kommande ändringar i Göteborgs Stads regel för IT-användare

- Under perioden för projektet *Etablera systematiskt informationssäkerhetsarbete* kommer flera förslag att presenteras tillhörande ansvar och mandat för befintliga roller inom Intraservice kopplat till informationssäkerhet (inkl. dataskydd och arkivansvar).
- I denna presentation fokuserar vi på
 - informationsägare, riskägare, systemägare, tekniskt arkivansvar, projektledare, processägare och processledare
 - Förhållningssättet när ansvar tagits fram har varit att
 - **en roll ska ha vissa ansvar**
 - **dess ansvar ska inte kunna innehas av annan roll**

Tidplan

Tidplan

- ✓ 2023 Dialog arkivnämnden
- ✓ Oktober-december 2023 information och dialog avdelningschefer och Intraservice ledningsgrupp
- ✓ 20 december 2023 Information ILG

- **2024-03-19** Information FSG
- **2024-03-20** ILG
- **April** Intern förankring
- **2024-05-02** Riskanalys ur ett arbetsmiljömässigt perspektiv
- **2024-05-08** ILG
- **2024-05-23** Samverkan FSG
- **2024-06-13** Presidiemöte
- **2024-06-19** Informationsmöte Intraservice nämnd
- **2024-06-27** Beslut Intraservice nämnd

- 5 juni anmälan av ärende till nämndmöte
- 12 juni inlämning av tjänsteutlåtande och övrigt material

Förslag till hur arbetet med informationssäkerhet (inkl. dataskydd och arkivansvar) kan organiseras

Vilken påverkan får föreslagen förändring?

- Samtliga medarbetare (inkl. chefer) påverkas.
 - Alla roller får utökat och nya ansvar.
- Befintliga processer behöver kompletteras.
- Nya processer behöver skapas.
- Befintliga styrande dokument behöver uppdateras.
- Nya styrande dokument behöver tas fram
- Utbildningsmaterial behöver tas fram.
- Samtliga medarbetare (inkl. chefer) behöver utbildas.



Strategiskt – Taktisk – Operativ nivå



Göteborgs
Stad



Informationssäkerhets-/dataskyddsorganisation

- **Förslag till organisation kring informationssäkerhet/dataskydd**
- Biträdande direktör/Stabschef får i uppdrag att genomföra förändringen.
- Förvaltningsdirektören får i uppdrag att fatta delegationsbeslut utifrån att:
 - Medarbetare tilldelas ansvar som informationsägare med utgångspunkt från den informationsmängd som denne hanterar
 - Medarbetare tilldelas ansvar som systemägare

- **Förslag till organisation kring tekniskt arkivansvar**
 - Biträdande direktör/stabschef får i uppdrag att genomföra förändringen.
 - Förvaltningsdirektören får i uppdrag att fatta delegationsbeslut enligt följande:
 - Stina Hall Hellqvist utses till arkivansvarig med huvudansvar
 - Anna-Lena Björk utses till Tekniskt arkivansvarig
 - Patrik Skog utses till Arkivansvarig för Intraservice som egen myndighet
 - En expertgrupp för arkiv- och informationsförvaltning ska etableras inom förvaltningen.

Informationsägare - Systemägare

Informationsägare

Intraservice nämnd

Text från Göteborgs Stads riktlinje för informationssäkerhet

”Ansvar och roller i informationssäkerhet 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.

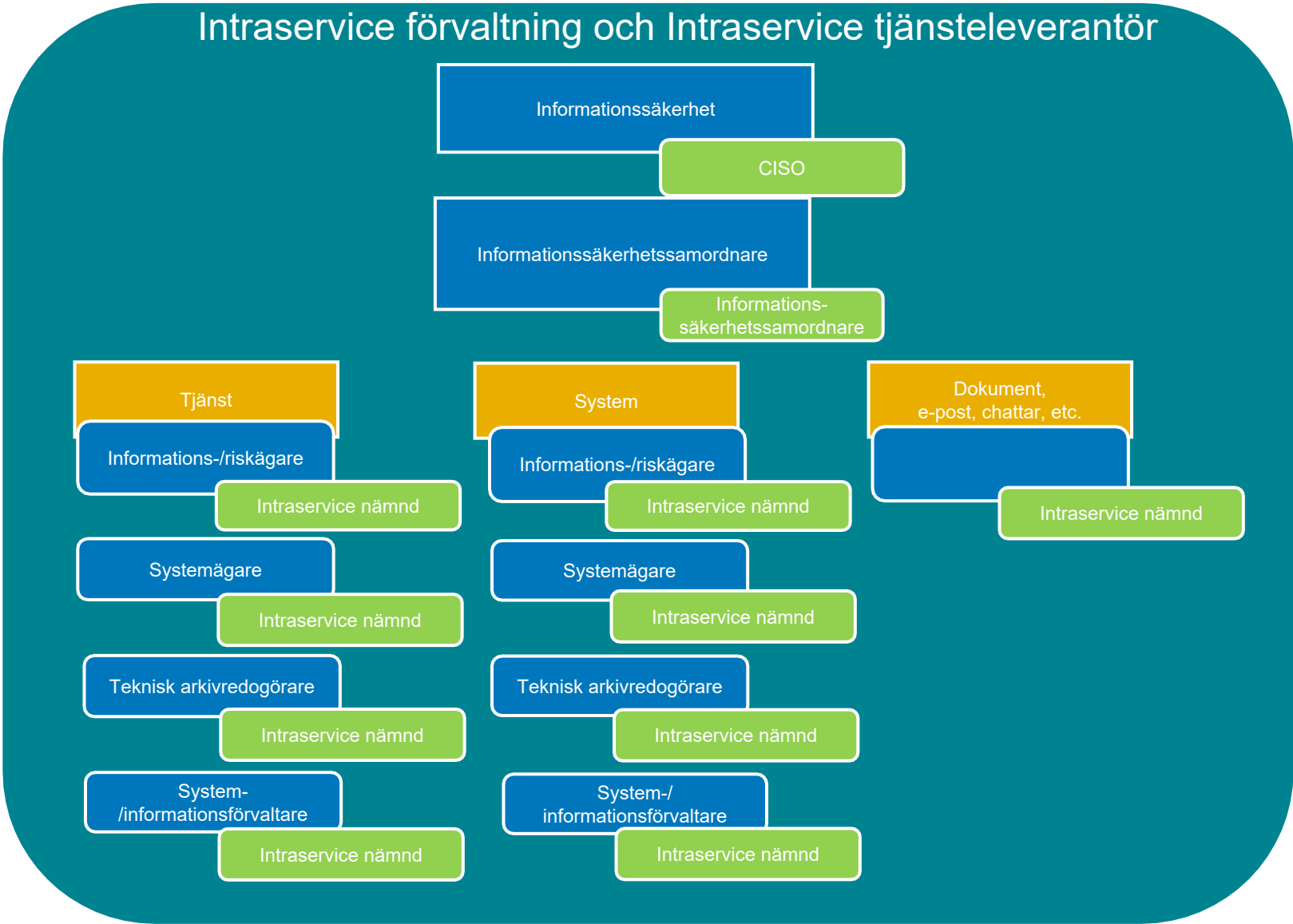
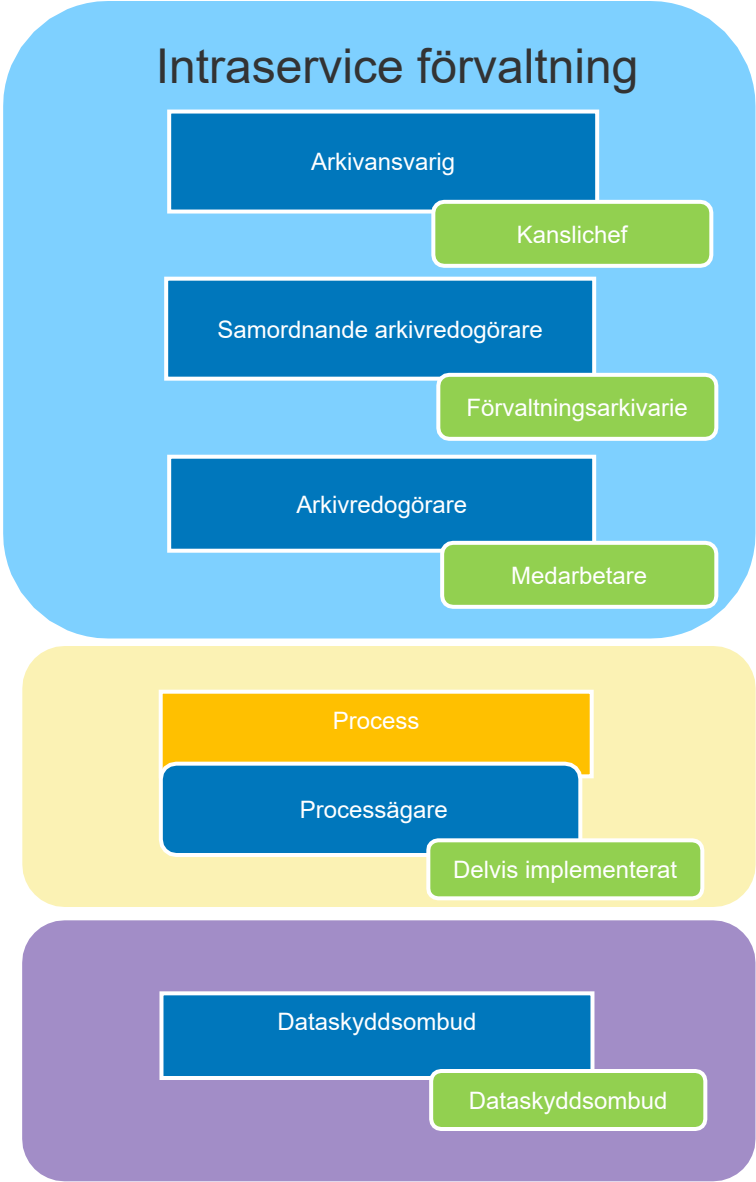
Informationsägare är den nämnd/styrelse som ansvarar för den information som skapas och hanteras. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten.

Informationssägaren klassificerar och beslutar om informationshantering inom ramen för befintlig lagstiftning och verksamhetskrav.

Systemägare är den som har ett överordnat ansvar för administration, drift och säkerhet för ett system. Ett system kan innehålla information som tillhör en eller flera informationsägare.

Systemägaren ansvarar för att system uppfyller lagkrav och verksamhetskrav som fastställts av informationsägare.”

Organisation 2024-04-19



Organisation Förslag



Göteborgs
Stad

Intraservice förvaltning

Arkivansvarig

Kanslichef

Samordnande arkivredogörare

Förvaltningsarkivarie

Arkivredogörare

Medarbetare

Process

Processägare

Verksamhetschef

Dataskyddsombud

Dataskyddsombud

Intraservice förvaltning och Intraservice tjänsteleverantör

Informationssäkerhet

CISO

Informationssäkerhetssamordnare
Teknisk arkivsamordnare

Informations-
säkerhetssamordnare

Tjänst

Informations-/riskägare

Verksamhetschef

Systemägare

Enhetschef

Teknisk arkivredogörare

Förvaltningsledare

System-
/informationsförvaltare

Medarbetare

System

Informations-/riskägare

Verksamhetschef

Systemägare

Enhetschef

Teknisk arkivredogörare

Förvaltningsledare

System-/
informationsförvaltare

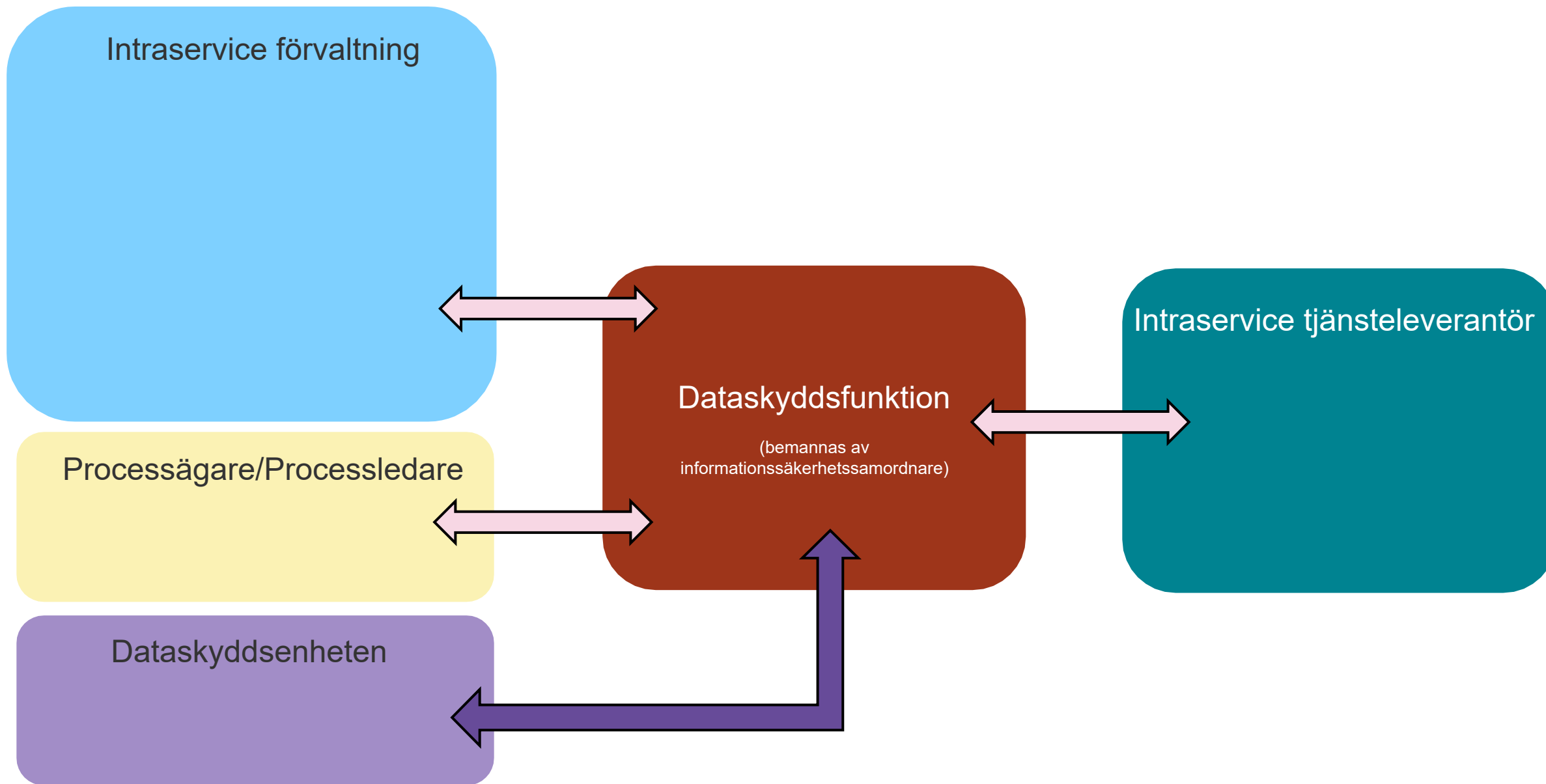
Medarbetare

Dokument,
e-post, chattar, etc.

Ansvarig IT-användare

IT-användare

Dataskyddsfunktion



Organisation Förslag



Göteborgs
Stad

Intraservice förvaltning

Arkivansvarig

Kanslichef

Samordnande arkivredogörare

Förvaltningsarkivarie

Arkivredogörare

Medarbetare

Process

Processägare

Verksamhetschef

Dataskyddsombud

Dataskyddsombud

Intraservice förvaltning och Intraservice tjänsteleverantör

Informationssäkerhet

CISO

Dataskyddsfunktion

Informationssäkerhetssamordnare
Teknisk arkivsamordnare

Informations-
säkerhetssamordnare

Tjänst

Informations-/riskägare

Verksamhetschef

Systemägare

Enhetschef

Teknisk arkivredogörare

Förvaltningsledare

System-
/informationsförvaltare

Medarbetare

System

Informations-/riskägare

Verksamhetschef

Systemägare

Enhetschef

Teknisk arkivredogörare

Förvaltningsledare

System-
/informationsförvaltare

Medarbetare

Dokument,
e-post, chattar, etc.

Ansvarig IT-användare

IT-användare

Dataskyddsfunktion - Dataskyddskontakt

- Varje personuppgiftsansvarig organisation i Göteborg Stad ska ha minst en dataskyddskontakt.
- Förslag om etablering av en funktion med medarbetare som agerar som dataskyddskontakter. Funktionen bemannas av informationssäkerhetssamordnare.
- Dataskyddskontakt ska vara en kontaktperson till dataskyddsombudet och har som uppgift att kanalisera frågor från verksamheten till dataskyddsombudet.
- Dataskyddskontakten är den som kontaktar dataskyddsombud när deras roll bör/behöver involveras.
- Funktionen ska vara en central funktion som har en etablerad kommunikation (ex. kontinuerligt återkommande möten) med roller som operativt utför aktiviteter kopplade till dataskydd.
- Funktionen ska ge stöd och råd, och kontrollera efterlevnad.

Dataskyddsfunktion - Dataskydd



Dataskyddsförordningen
(GDPR)

- Dataskydd handlar om att skydda personuppgifter.
- Dataskydd är en del av vad som inkluderas i begreppet informationssäkerhet.
- Medarbetare inom Intraservice behöver agera utifrån vad Dataskyddsförordningen anger, men även utifrån den lagstiftning som i övrigt gäller för Intraservice som förvaltning och tjänsteleverantör (krav på leveransen).
- **Dataskyddsfunktionen ska medverka till att det blir lätt att göra rätt.**

Övergripande beskrivning av begreppen

**Informationssäkerhet
Dataskydd
Informationsförvaltning
Arkivansvar
Tekniskt arkivansvar**

Informationssäkerhet

Dokumentnamn: Göteborgs Stads riktlinje för informationssäkerhet

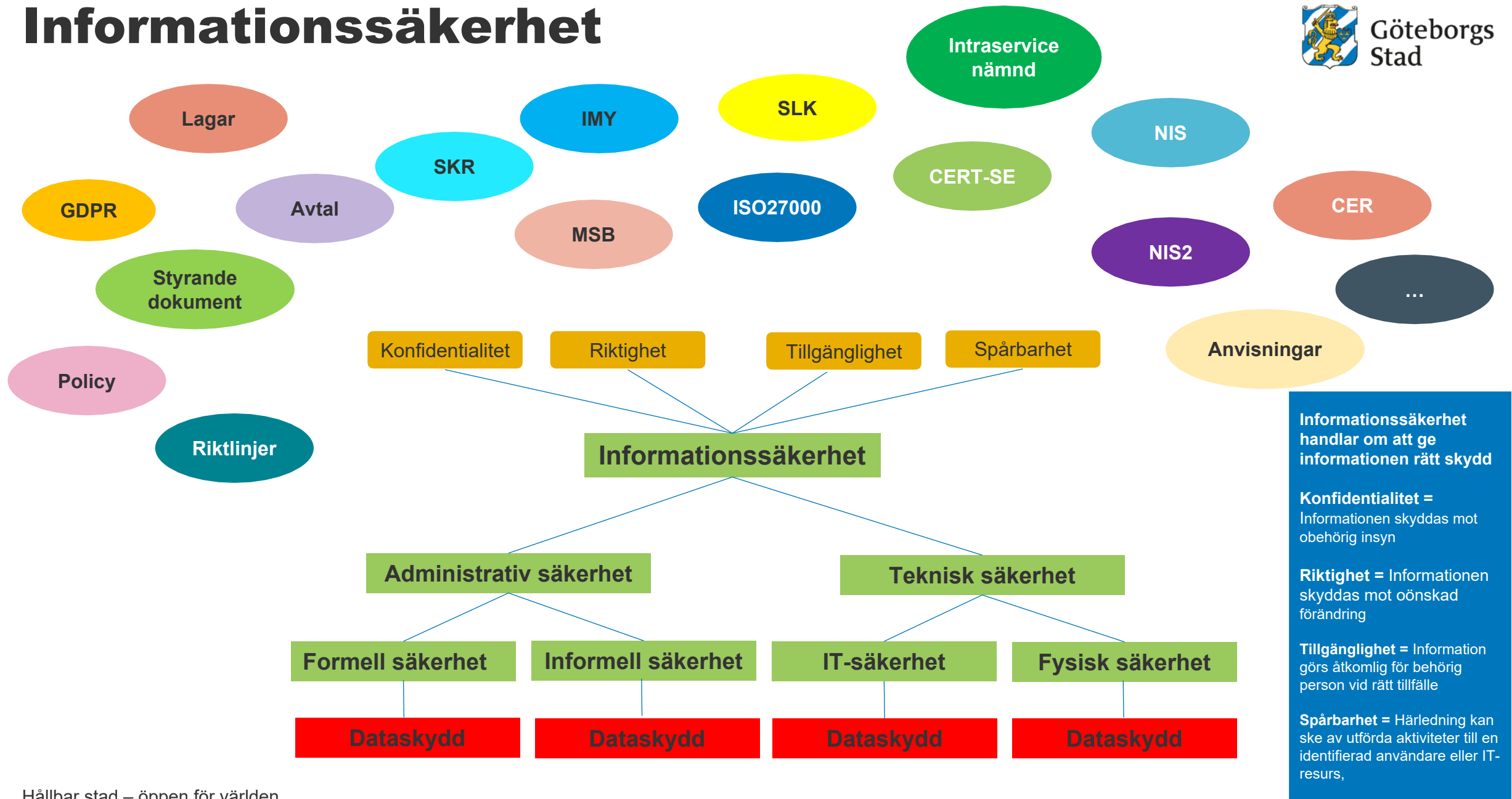
Beslutad av: Kommunfullmäktige	Gäller för: Stadens nämnder och styrelser	Diarienummer: 0160/23	Datum och paragraf för beslutet: 2023-05-25, § 7
--	---	---------------------------------	--

Dokumentsort: Riktlinje	Giltighetstid: Tills vidare	Senast reviderad: 2023-05-25	Dokumentansvarig: Säkerhetschef
-----------------------------------	---------------------------------------	--	---

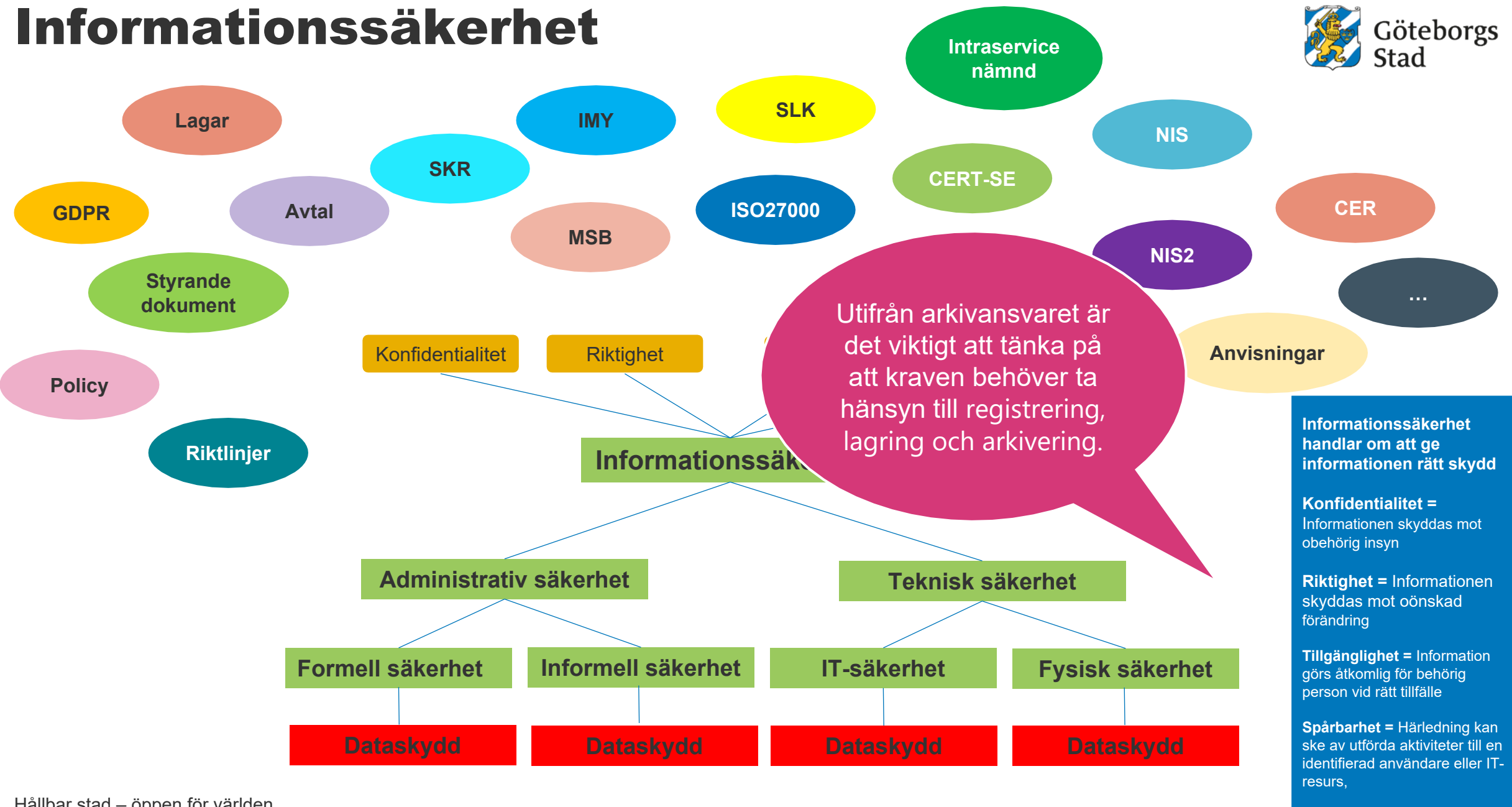
Bilagor:
Göteborgs Stads klassificeringsmodell
Göteborgs Stads klassificeringsmodell - beskrivning av konsekvensnivåer
Begreppsdefinition

- Informationssäkerhet handlar om att skydda all typ av information så att
 - endast behöriga personer får ta del av den (konfidentialitet)
 - vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet)
 - den alltid finns när vi behöver den (tillgänglighet)

Informationssäkerhet



Informationssäkerhet



Administrativ säkerhet

- **Formell säkerhet:** Styrande dokument, anvisningar rutiner och instruktioner som beskriver hur information ska hanteras, till exempel hur anställda ska hantera information, men även hur man hanterar behörigheter till olika IT-system, med mera.
- **Informell säkerhet:** Kultur, dvs. hur organisationen ser på informationssäkerhet och hur man agerar.

Teknisk säkerhet

- **IT-säkerhet:** Tekniska skyddsåtgärder för att skydda informationen såsom exempelvis åtkomstkontroll, brandväggar, kryptering, övervakning/loggning och virus/malwareskydd.
- **Fysisk säkerhet:** Tekniska skyddsåtgärder för att skydda informationen genom att förhindra att obehöriga får tillträde till lokaler och/eller objekt. Exempel på tekniska säkerhetsåtgärder är inpasseringssystem, avlyssningsskyddade rum och övervakning/loggning.

Dataskydd



Dataskyddsförordningen
(GDPR)

- Dataskydd handlar om att skydda personuppgifter

Informationsförvaltning



- Informationsförvaltning handlar om hur information
 - skapas
 - hanteras
 - distribueras och till slut bevaras eller gallras

Riksarkivets författningssamling

ISSN 0283-2941



Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar (upptagningar för automatiserad behandling);

beslutade den 30 april 2009.

Riksarkivet föreskriver med stöd av 2, 3, 4, 11 och 12 §§ arkivförordningen (1991:446) följande föreskrifter och allmänna råd om elektroniska handlingar.

RA-FS 2009:1

Utkom från trycket
den 1 juli 2009

- Arkivansvar handlar om att skydda all typ av information så att
 - den skyddas mot avsiktlig och oavsiktlig förändring eller förlust, skada, manipulation och obehörig åtkomst (RA-FS 2009:1, 6 kap. 2 §), samt att åtgärder finns för att förhindra informationsförluster (RA-FS 2009:1, 4 kap. 13 §).

Tekniskt arkivansvar

- *"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.

Systematiskt informationssäkerhetsarbete

Systematiskt informationssäkerhetsarbete

- Ett systematiskt informationssäkerhetsarbete börjar med att vi vet vilken information som ska skyddas.
- Vi måste ha kunskap om
 - vilka informationsbärare som finns
 - vilken informationsklassning som gäller för processen som informationsbärare ingår i
 - vilka säkerhetskrav som gäller utifrån aktuell informationsklassning
 - vilka krav som finns för gallring och arkivering
 - vilka risker som kan identifieras och därutifrån
 - vilka säkerhetsåtgärder som finns och vilka säkerhetsåtgärder som behöver implementeras.
- Därtill behövs processer och styrande dokument som stödjer arbetet med att kontinuerligt arbeta med förvaltningen av informationen.

Processer i flera lager – flera processägare – HR-processerna ett exempel

- Det finns idag processer som är kan sägas vara "staden-övergripande", bland annat HR-processerna.
- HR-processerna kompletteras med det som benämns som arbetsformer.
- Ett exempel är arbetsformen för löneadministration och löneskuld.
- Denna arbetsform har ett beroende till process/er inom Intraservice tjänsteleverans/er.
- Exempelvis processen som bl.a. fyller Intraservice tjänst, *Stöd i arbete med löneadministration för förvaltningar och bolag*, med personuppgifter.
- De för Göteborgs Stad gemensamma processerna har processägare.
- Den process som bl.a. fyller tjänsten *Stöd i arbete med löneadministration för förvaltningar och bolag* med personuppgifter har en processägare som har sin hemvist inom Intraservice. Denne processägare är informationsägare för den information som processen skapar, nyttjar eller bearbetar. Som informationsägare är denne därtill riskägare.

Roller och ansvar

Informationsägare Riskägare Systemägare

Informations- och systemägare

Dokumentnamn: Göteborgs Stads riktlinje för informationssäkerhet

Beslutad av: Kommunfullmäktige	Gäller för: Stadens nämnder och styrelser	Diarienummer: 0160/23	Datum och paragraf för beslutet: 2023-05-25, § 7
--	---	---------------------------------	--

Dokumentsort: Riktlinje	Giltighetstid: Tills vidare	Senast reviderad: 2023-05-25	Dokumentansvarig: Säkerhetschef
-----------------------------------	---------------------------------------	--	---

Bilagor:
Göteborgs Stads klassificeringsmodell
Göteborgs Stads klassificeringsmodell - beskrivning av konsekvensnivåer
Begräppsförklaring

Text från Göteborgs Stads riktlinje för informationssäkerhet

”Ansvar och roller i informationssäkerhet 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.

Informationsägare är den nämnd/styrelse som ansvarar för den information som skapas och hanteras. Ansvaret för informationen och dess säkerhet följer med ansvaret för verksamheten.

Informationssägaren klassificerar och beslutar om informationshantering inom ramen för befintlig lagstiftning och verksamhetskrav.

Systemägare är den som har ett överordnat ansvar för administration, drift och säkerhet för ett system. Ett system kan innehålla information som tillhör en eller flera informationsägare.

Systemägaren ansvarar för att system uppfyller lagkrav och verksamhetskrav som fastställts av informationsägare.”

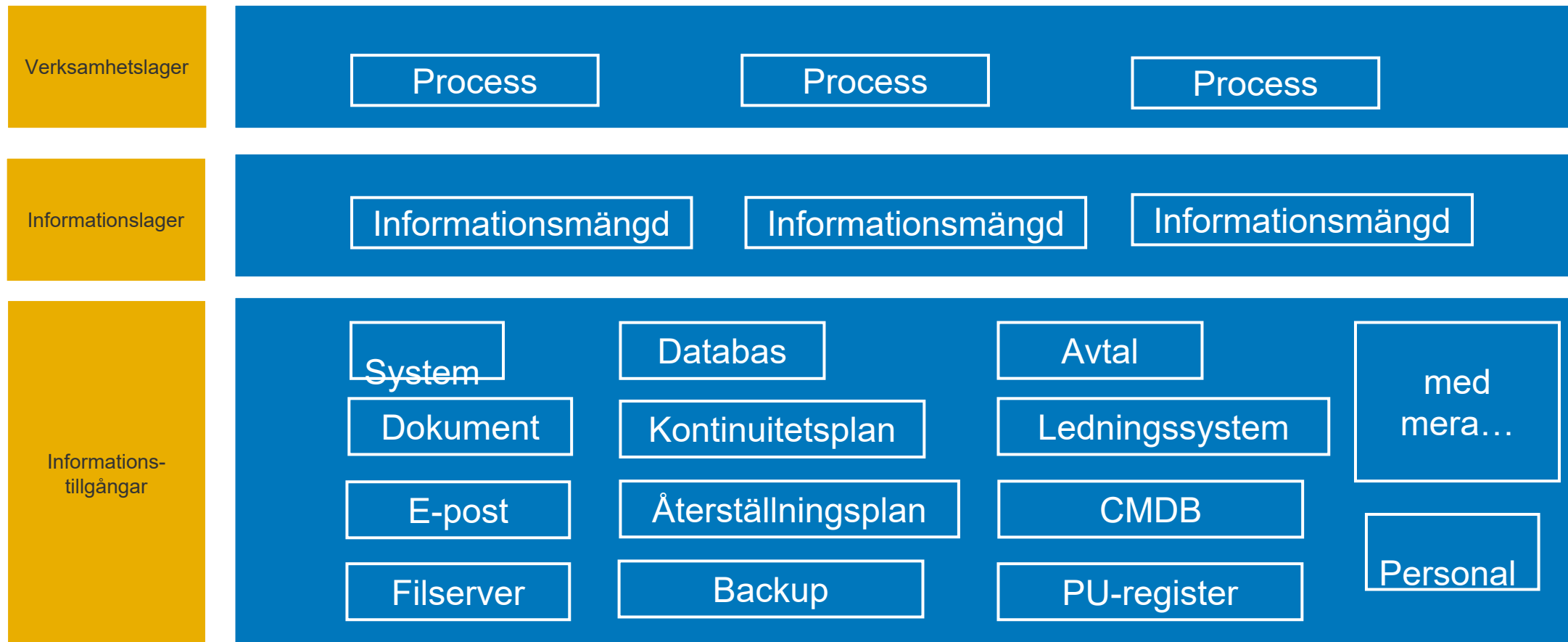
Informationsägare

- Informationsägare har ett ansvar för informationen som hanteras inom en informationsmängd.
- Med informationsmängd avses den information som en process skapar, nyttjar eller bearbetar.
- En informationsmängd utgörs av information som är avgränsad för ett visst ändamål.
- Inom en informationsmängd kan det finnas en eller flera informationstillgångar.

Informationshantering



Göteborgs
Stad



Riskägare

- Riskägaren ansvarar för att risker identifieras och accepteras eller hanteras, exempelvis med säkerhetsåtgärder.
- **I och med att ett riskägaransvar ofta berör tillgång till resurser, beslutsmandat och delaktighet i centrala beslut ska riskägaransvaret innehas av en chef.**

Intraservices förvaltningsorganisation

Verksamhetschef

- **Verksamhetschef**

- **Ledningsansvar** gällande utveckling, underhåll, användning och säkerhet kopplat till process/system och dess informationstillgångar.
- **Ledningsansvar** gällande förutsättningar för att medarbetare ska kunna ta sitt ansvar, bland annat inkluderande att som informationsägare ansvara för att ställa krav på tjänst och/eller system som nyttjas av medarbetare (IT-användare).
- **Informationsägare process**
- **Riskägare**
- **Återrapporterar till avdelningschef**

Exempel på vad som inkluderas i informationsägaransvar

Ansvar för

- uppföljning av att hanteringen av informationen följer styrande dokument, anvisningar, rutiner och instruktioner, bland annat inkluderande att ansvara för att
 - informationsklassning genomförs och fastställande av denna
 - riskanalyser genomförs och att risker identifieras
 - risker accepteras eller säkerställande av att risker hanteras, exempelvis med säkerhetsåtgärder
 - risker och säkerhetsåtgärder följs upp och att aktuell status är dokumenterad
 - informationsklassning, risker och säkerhetsåtgärder delges berörda
- att enhetschef uppdaterar register över tillgångar (inkl. bland annat utrustning, system/applikationer, verktyg, leverantörer, underleverantörer)
- att enhetschef vid upprättande av förvaltningsplan säkerställer att åtgärder vidtas utifrån resultat från aktuell riskanalys och bevakar uppfyllnad
- att säkra finansieringen av förvaltningsplan
- att bevaka och följa upp nyttoppfyllnaden av processens system/applikation/verktyg/informationen
- att enhetschef upprättar, följer upp och uppdaterar kontinuitets- och återställningsplan, och bevakar uppfyllnad *)
- avtalsskrivande med leverantör (*I de fall personuppgifter hanteras på uppdrag utanför den egna organisationen ska avtal om personuppgiftsbiträde upprättas i enlighet med dataskyddsförordningen.*)
- att bevaka och följa upp avtal med leverantörer

*) Kravställning tillhörande kontinuitets- och återställning återspeglas av vad verksamheten ska leverera (ansvarig: *ska fastställas under 2024*)

- **Enhetschef**

- **Verkställande ansvar** gällande utveckling, underhåll, användning och säkerhet kopplat till process/system och dess informationstillgångar. Ansvaret innebär att tillse att processen/systemet och informationen har rätt kvalitet för sitt ändamål, finns tillgänglig när den behövs och att information som skapas i eller kommuniceras till eller från den egna verksamheten skyddas.
- **Verkställande ansvar** gällande förutsättningar för att medarbetare ska kunna ta sitt ansvar.
- **Systemägare**
- **Återrapporterar till verksamhetschef**

Exempel på vad som inkluderas i enhetschefs/systemägares ansvar

Ansvar för

- att hanteringen av information i process och/eller system följer styrande dokument, anvisningar, rutiner och instruktioner och samråder med informationssäkerhetssamordnare
- genomförande av informationssäkerhetsklassning
- genomförande av riskanalyser och samordnar riskanalyser med andra systemägare
- att säkerhetsåtgärder implementeras
- att säkerställa att förvaltningsplan/er innehåller åtgärder utifrån resultat från aktuell riskanalys och ansvarar för att bevaka uppfyllnad
- att kontinuitets- och återställningsplan upprättas, följs upp och uppdateras
- och beslutar om användares åtkomsträttigheter och att dessa överensstämmer med deras faktiska behörigheter
- att tillse att arkivredogörare (förvaltningsledare) tillsätts och att gallring och arkivering utförs enligt arkivreglementet
- att tillse att förvaltningsledare tar fram och underhåller bevarandeplan för system
- att register över tillgångar (inkl. bland annat utrustning, system/applikationer, verktyg, leverantörer, underleverantörer) hålls uppdaterade

- **Förvaltningsledare**

- **Operativt ansvar** gällande utveckling, underhåll, användning och säkerhet kopplat till process/system och dess informationstillgångar. Ansvaret innebär att tillse att processen/systemet och informationen har rätt kvalitet för sitt ändamål, finns tillgänglig när den behövs och att information som skapas i eller kommuniceras till eller från den egna verksamheten skyddas
- **Arkivredogörare**
- **Återrapporterar till närmaste chef**

Exempel på vad som inkluderas i förvaltningsledarens Ansvar för

- att ta kontakt med dataskyddskontakt vid nyutveckling, förändring och incidenter om informationen inkluderar personuppgifter
- att samordna arbete med incident, problem, change, request, test och release
- att hanteringen av information i process och/eller system följer styrande dokument, anvisningar, rutiner och instruktioner och samråder med informationssäkerhetssamordnare
- implementering av säkerhetsåtgärder
- upprättande av förvaltningsplan/er och att åtgärder vidtas utifrån resultat från aktuell riskanalys
- uppföljning av förvaltningsplan/er och återrapportering till enhetschef/informations-/risk-ägare
- att följa upprättad kontinuitets- och återställningsplan, samt med regelbundenhet (enligt anvisning) utvärdera och praktiskt testa dessa, samt rapportera uppfyllnad
- agera som teknisk arkivredogörare och att samråda med arkivarie/teknisk arkivsamordnare i frågor som rör gallring enligt 9 § arkivreglementet och arkivering
- framtagande och underhåll av systems bevarandeplan

Intraservices tjänsteorganisation

Verksamhetschef

- **Verksamhetschef**

- **Ledningsansvar** gällande utveckling, underhåll, användning och säkerhet kopplat till tjänst/system och dess informationstillgångar.
- **Ledningsansvar** gällande förutsättningar för att medarbetare ska kunna ta sitt ansvar, bland annat inkluderande att som informationsägare ansvara för att ställa krav på tjänst och/eller system som nyttjas av medarbetare (IT-användare).
- **Tjänsteägare**
- **Informationsägare process**
- **Riskägare**
- **Återrapporterar till avdelningschef**

Exempel på vad som inkluderas i informationsägaransvar

Ansvar för

- uppföljning av att hanteringen av informationen följer styrande dokument, anvisningar, rutiner och instruktioner, bland annat inkluderande att ansvara för att
 - informationsklassning genomförs och fastställande av denna
 - riskanalyser genomförs och att risker identifieras
 - risker accepteras eller säkerställande av att risker hanteras, exempelvis med säkerhetsåtgärder
 - risker och säkerhetsåtgärder följs upp och att aktuell status är dokumenterad
 - informationsklassning, risker och säkerhetsåtgärder delges berörda
- att tjänste-/system-/informationsförvaltare är utsedda och för avtal (OLA) med tjänste-/system-/informationsförvaltare som vill nyttja tjänsten/systemet/informationen (integration till andra tjänster/system/objekt)
- att enhetschef uppdaterar register över tillgångar (inkl. bland annat utrustning, system/applikationer, verktyg, leverantörer, underleverantörer)
- att enhetschef vid upprättande av förvaltningsplan säkerställer att åtgärder vidtas utifrån resultat från aktuell riskanalys och bevakar uppfyllnad
- att bevaka och följa upp nyttoppfyllnaden av tjänstens/processens system/applikation/verktyg/informationen
- att enhetschef upprättar, följer upp och uppdaterar kontinuitets- och återställningsplan, och bevakar uppfyllnad *)
- avtalsskrivande med leverantör (*I de fall personuppgifter hanteras på uppdrag utanför den egna organisationen ska avtal om personuppgiftsbiträde upprättas i enlighet med dataskyddsförordningen.*)
- att bevaka och följa upp avtal med leverantörer

*) Kravställning tillhörande kontinuitets- och återställning återspeglas av vad tjänst ska leverera (ansvarig: ska fastställas under 2024)

- **Enhetschef**

- **Verkställande ansvar** gällande utveckling, underhåll, användning och säkerhet kopplat till tjänst/system och dess informationstillgångar. Ansvaret innebär att tillse att tjänsten/systemet och informationen har rätt kvalitet för sitt ändamål, finns tillgänglig när den behövs och att information som skapas i eller kommuniceras till eller från den egna verksamheten skyddas.
- **Verkställande ansvar** gällande förutsättningar för att medarbetare ska kunna ta sitt ansvar.
- **Systemägare**
- **Återrapporterar till verksamhetschef**

Exempel på vad som inkluderas i enhetschefs/systemägares ansvar

Ansvar för

- att hanteringen av information i tjänst och/eller system följer styrande dokument, anvisningar, rutiner och instruktioner och samråder med informationssäkerhetssamordnare
- genomförande av informationssäkerhetsklassning
- genomförande av riskanalyser och samordnar riskanalyser med andra systemägare
- att säkerhetsåtgärder implementeras
- att säkerställa att förvaltningsplan/er innehåller åtgärder utifrån resultat från aktuell riskanalys och ansvarar för att bevaka uppfyllnad
- att kontinuitets- och återställningsplan upprättas, följs upp och uppdateras
- och beslutar om användares åtkomsträttigheter och att dessa överensstämmer med deras faktiska behörigheter
- att tillse att arkivredogörare (förvaltningsledare) tillsätts och att gallring och arkivering utförs enligt arkivreglementet
- att tillse att förvaltningsledare tar fram och underhåller bevarandeplan för tjänsten
- att register över tillgångar (inkl. bland annat utrustning, system/applikationer, verktyg, leverantörer, underleverantörer) hålls uppdaterade

- **Förvaltningsledare**

- **Operativt ansvar** gällande utveckling, underhåll, användning och säkerhet kopplat till tjänst/system och dess informationstillgångar. Ansvaret innebär att tillse att tjänsten/systemet och informationen har rätt kvalitet för sitt ändamål, finns tillgänglig när den behövs och att information som skapas i eller kommuniceras till eller från den egna verksamheten skyddas
- **Teknisk arkivredogörare**
- **Återrapporterar till närmaste chef**

Exempel på vad som inkluderas i förvaltningsledarens Ansvar för

- att ta kontakt med dataskyddskontakt vid nyutveckling, förändring och incidenter om informationen inkluderar personuppgifter
- att samordna arbete med incident, problem, change, request, test och release
- att hanteringen av information i tjänst och/eller system följer styrande dokument, anvisningar, rutiner och instruktioner och samråder med informationssäkerhetssamordnare
- implementering av säkerhetsåtgärder
- upprättande av förvaltningsplan/er och att åtgärder vidtas utifrån resultat från aktuell riskanalys
- uppföljning av förvaltningsplan/er och återrapportering till enhetschef/informations-/risk-ägare
- att följa upprättad kontinuitets- och återställningsplan, samt med regelbundenhet (enligt anvisning) utvärdera och praktiskt testa dessa, samt rapportera uppfyllnad
- agera som teknisk arkivredogörare och att samråda med arkivarie/teknisk arkivsamordnare i frågor som rör gallring enligt 9 § arkivreglementet och arkivering
- framtagande och underhåll av tjänstens bevarandeplan

Personuppgiftsbehandling Tjänst

Personuppgiftsbehandlingar - Tjänst

- Samverkan pågår kring frågan om för vilka personuppgiftsbehandlingar olika parter ska vara personuppgiftsansvarig respektive personuppgiftsbiträde.
- I dialogerna har Intraservice framfört att Intraservice bör vara personuppgiftsansvarig för vissa behandlingar. Exempelvis behandlingar av personuppgifter som utförs inom tjänsterna kopplade till vissa kvalitets- och säkerhetsåtgärder.
- Om samverkan leder fram till att Intraservice är personuppgiftsansvarig för vissa personuppgiftsbehandlingar behöver det även verifieras att Intraservice är att anse som informationsägare av denna information.
- Detta synsätt kan matchas mot vad som bl.a. tas upp i Göteborgs Stads riktlinje för styrning, samordning och finansiering av digital utveckling och förvaltning, där det anges att Intraservice har ett speciellt ansvar när det gäller säkerheten i tjänster.
- Om samverkan kommer fram till att Intraservice som tjänsteleverantör är personuppgiftsansvarig för vissa typer av personuppgiftsbehandlingar behöver Intraservices organisation utbildas i vad detta innebär och vilket ansvar som följer med detta.
- I möte 23 april framkom att representanter från Stadsledningskontoret, Intraservice och dataskyddsombud har en gemensam syn på att Intraservice bör vara personuppgiftsansvarig för vissa typer av personuppgiftsbehandlingar. Nästa steg är att utreda hur samverkan ska ske framöver när det gäller övriga personuppgiftsbehandlingar och för att erhålla en samsyn generellt inom Göteborgs Stad. **Vem som är att anse som ansvarig part för fortsatt arbete och hur detta ska hanteras är inte fastställt. Intraservice CISO har dialog med Stadsledningskontoret i frågan om ansvarig part.**

Ett exempel

Informationsägare

Ett ärende till Intraservice nämnd

Exempel

Fråga:

- Vem är informationsägare om en medarbetare skapar ett dokument som hör till ett ärende som ska behandlas av nämnden för Intraservice? Är det medarbetaren? Är det processägaren för processen ärende till nämnd eller är det Verksamhetschefen för tjänsten med systemet som dokumentet lagras i (LIS)?

Svar:

- Medarbetare som skapar dokumentet ansvarar för att dokumentet klassificeras utifrån den klassificeringsmodell som anges i Göteborgs Stads riktlinje för informationssäkerhet och för att dokumentet hanteras utifrån den klassificering av informationen som gjorts. Detta innebär att medarbetaren behöver säkerställa att process för ärende till nämnd når upp till de administrativa och tekniska säkerhetsåtgärder som klassificeringen ger svar om. När inte processen upp till kraven kan den inte användas, alternativt behöver informationen i dokumentet anpassas utifrån vad som processen kan erbjuda i form av säkerhetsåtgärder.
- Processägaren (processägaren för processen för ärenden till nämnd) ansvarar för att processens aktiviteter har de säkerhetsåtgärder som beslutats om. Dvs att processen har nödvändiga administrativa och tekniska säkerhetsåtgärder för att skydda informationen som hanteras inom processen.
- Tjänsteägaren (verksamhetschefen), som också är informationsägare för tjänsten som tillhandahåller systemstöd (LIS) ansvarar för att tjänsten har de säkerhetsåtgärder som beslutats om. Dvs att tjänsten har nödvändiga administrativa och tekniska säkerhetsåtgärder för att skydda informationen som hanteras inom tjänsten.
- Medarbetarens närmaste verksamhetschef har ansvar som informationsägare utifrån verksamhetens användningen av tjänst och/eller system. Denne är kravställare på tjänst och/eller system-som verksamheten använder sig av.

Medarbetare

System-/informationsförvaltare

- **Medarbetare**

- **Operativt ansvar** för system som berörs.
- Rollen samverkar med berörda systemägare och förvaltningsledare för att säkerställa att systemet hanteras/förvaltas i enlighet med styrande dokument, anvisningar, rutiner och instruktioner.
- **Återrapporterar till närmaste chef**

Exempel på vad som inkluderas i system-/informationsförvaltares ansvar

Ansvar för att

- utföra informationssäkerhetsåtgärder enligt förvaltningsplan
- hantera ärende (incident, problem, change, request)
- hanteringen av information i tjänst och/eller system följer styrande dokument, anvisningar, rutiner och instruktioner och samråder med systemägare och förvaltningsledare
- eskalera till systemägare och förvaltningsledare

IT-användare dokument, e-post, chattar, etc.

- **Samtliga IT-användare**

- Med IT-användare avses i enlighet med gällande styrande dokument "Göteborgs Stads regel för IT-användare" (0347/08 (0110/20) anställda, entreprenörer, inhyrd personal, konsulter och leverantörer som arbetar i eller med stadens IT-resurser.
- **Återrapporterar till närmaste chef**

Exempel på vad som inkluderas i IT-användares ansvar

- Informera sig om de regelverk, rutiner och det ansvar som är tillämpliga. Med detta avses att IT-användare behöver ha kunskap och kompetens att avgöra utifrån innehåll i dokument, e-post, chattar, etc. hur informationen ska utformas och hanteras när det gäller spridning, gallring och lagring.
- IT-användare som skapar dokumentet ansvarar för att dokumentet klassificeras utifrån den klassificeringsmodell som anges i Göteborgs Stads riktlinje för informationssäkerhet och för att dokumentet hanteras utifrån den klassificering av informationen som gjorts. Detta innebär att IT-användare behöver säkerställa att process för ärende till nämnd når upp till de administrativa och tekniska säkerhetsåtgärder som klassificeringen ger svar om. När inte processen når upp till kraven kan den inte användas, alternativt behöver informationen i dokumentet anpassas utifrån vad som processen kan erbjuda i form av säkerhetsåtgärder.
- IT-användare ansvarar för att kontakta närmaste chef vid frågor eller då det är tveksamt eller konstaterat att process/tjänst/system inte når upp till de administrativa och tekniska säkerhetsåtgärder som klassificeringen ger svar om.

Tekniskt arkivansvar

Tekniskt arkivansvar

Det tekniska arkivansvaret ingår i det ansvar som åligger Intraservice som informationsägare, systemägare och tjänsteleverantör.

Det tekniska arkivansvaret ska ses som ett komplement till ordinarie förvaltningsansvar.

Tekniskt arkivansvarig

Om flera tjänstepersoner utses till tekniskt arkivansvarig ska en av dessa utses till huvudansvarig. Huvudansvarig för det tekniska arkivansvaret ska ha möjlighet att påverka och belysa arkivfrågor så att myndigheten avsätter pengar ur budgeten för arkivarbete.

Teknisk arkivsamordnare

Utöver arkivansvarig ska myndigheten utse tjänstepersoner/arkivredogörare som svarar för det praktiska arbetet med frågor rörande det tekniska arkivansvaret. Arkivredogörarna leds och stöds i detta arbete av en samordnande funktion. Då funktionen är bemannad av specialister inom informationsförvaltning säkerställs den kompetens som krävs för att uppnå kvalitet och lagefterlevnad i arbetet.

Arkivredogörare tekniskt arkivansvar

För etablerade tjänster sammanfaller ansvaret som arkivredogörare för tekniskt arkivansvar med förvaltningsledarens ansvar. Vid nyetablering eller omfattande förändring/utveckling av tjänst åligger det projektledare att ansvara för det tekniska arkivansvaret hanteras inom projekt.

Projekt

Projekt

- Projektledare
- Ansvarar för att samverka med projektägare och dataskyddskontakt
- Vid nyetablering eller omfattande förändring/utveckling av tjänst åligger det projektledare att ansvara för det tekniska arkivansvaret hanteras inom projekt.

Processer

Processer

- Det finns olika typer av processer
 - Ledningsprocesser (styr verksamheten)
 - Stödprocesser (stödjer leveransen)
 - Huvudprocesser (skapar resultat – operativt arbete)
- Exempel på processer som ingår i Ledningssystem för informationssäkerhet
 - Informationsklassning
 - Riskhantering
 - Kontinuitetshantering
 - Sårbarhetshantering
 - Behörighetshantering
 - Patch-hantering
 - Undantagshantering
 - etc.

Processägare - Intraservice

- **Verksamhetschef**

- **Ledningsansvar** gällande styrning, samordning och uppföljning av process som tas fram och leds från strategisk och taktisk nivå och som är gemensam för organisationen, exempelvis processer som rör organisationens enhetliga arbete med ekonomi, personal, arkiv, informationssäkerhet, tjänsteleverans, etc.
- **Informationsägare process**

Klassificeringsstruktur = en struktur som ska användas vid upprättande av arkivförteckning och vid registrering av ärenden.

[Klassificeringsstruktur - Regionarkivet - Göteborgs Stad \(goteborg.se\)](#)

Exempel på vad som inkluderas i processägaransvar

- Ansvarig för viss process
- Ansvarar för att
 - processens mål överensstämmer med vad som anges i styrande dokument
 - processens aktiviteter skapar ett stöd och underlättar dagligt arbete i processen
 - vid behov komplettera processen med systemstöd
 - styra, samordna och följa upp utvecklings- och underhållsarbete av processen
 - följa upp processens effektivitet och kvalitet
 - följa upp processens efterlevnad
 - samråda med arkivfunktionen (förändring av verksamhetsprocess kan påverka beslutad klassificeringsstruktur)

Processledare - Intraservice

- **Medarbetare**

- **Ledningsansvar** för viss process gällande utveckling och underhåll samt kunskapsspridning

Exempel på vad som inkluderas i processledaransvar

- Ansvarig för att på uppdrag av processägare
 - planera och leda arbetet med utvecklings- och underhållsarbete av processen
 - sprida kunskap om processen
 - Ta fram anvisningar, rutiner och instruktioner
 - Utbilda
 - ge operativt råd och stöd i hur processen ska användas/följas
 - samverka med förvaltningsarkivarie och arkivredogörare när det gäller ändringar som påverkar beslutad klassificeringsstruktur
- Ansvarar för att samverka med förvaltningsledare och systemägare, samt datakyddskontakt

Informationsklassning

Informationsklassning initieras av *informationsägare*.

Informationsklassning ska utföras i samband med:

- Förändrad användning av information i en process eller förändringar av en process. Även förändringar i lagar, styrande dokument eller avtal som har påverkan på information i en process motiverar förnyad informationsklassning.
- Införskaffning av ny informationsbärare i form av exempelvis nytt system/ny applikation, övergång till molndrift eller annan form av utkontraktering. Informationsklassningen bör i dessa fall vara ett förberedande arbete inför ett upphandlingsprojekt eller liknande.
- Förändring av tjänst eller IT-lösning som påverkar informationsmängderna i en process.
- Periodicitet. Om informationsklassning inte har genomförts av någon annan anledning inom en period av fyra år ska en förnyad informationsklassning genomföras.

Utgå från ett helhetsperspektiv vid informationsklassning

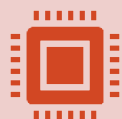
Informationsklassning utifrån ett helhetsperspektiv



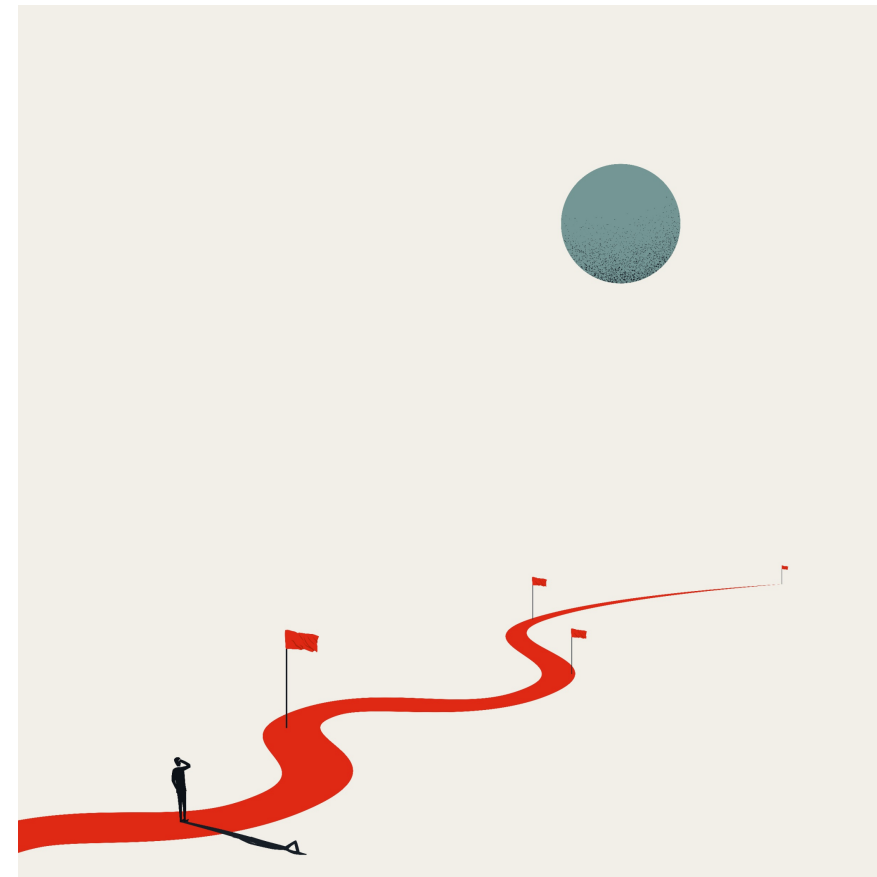
Behov finns av att implementera och verifiera säkerheten i Intraservice förvaltningsarbete och tjänsteleveranser ut ett helhetsperspektiv – “från A till Ö”



Det räcker inte att se till enskilda system eller funktioner



Säkerheten måste verifieras från det att exempelvis ett system med automatik fylls på med information till dess att tjänstens produkt används i det dagliga arbetet



Informationsklassning av en process

- När vi arbetar med informationsklassning utgår vi från att informationen hanteras i någon form av process. Detta gäller oavsett om vi ser till verksamhetsprocesser, tjänst eller enskild medarbetares hantering av exempelvis dokument. Därav anges att en informationsklassning sker av en process.

Riskhantering

Förutom vad som tas upp i [Anvisning för styrning, uppföljning och kontroll \(goteborg.se\)](https://www.goteborg.se/Anvisning_för_styrning_oppfolljning_och_kontroll) ska riskhantering ske i samband med arbete kopplat till:

- Ärendehantering; Incident, problem, change, request
- Projekt och uppdrag
 - Exempelvis nyutveckling, inköp, etc.
- Förändringar av verksamhet, tjänsteleveranser eller annat som inte hanteras via ärendehantering, projekt eller uppdrag
- Årlig riskanalys av tjänst, tjänsteerbjudande och dess beståndsdelar
- Notera att bevarandeplan ska uppdateras utifrån genomförd riskanalys

Olika typer av risker

- Strategiska risker
- Finansiella risker
- Risker kopplade till efterlevnad av lagar/regelverk/styrande dokument
- Operativa risker

Olika roller hanterar olika typer av risker

Olika roller hanterar olika risknivåer (hög, medel, låg)

Befogenhet att hantera vissa risker styrs av verksamhetsansvaret

- Ex.:
 - Verksamhetschef för område A har befogenhet att hantera risker för område A, men saknar befogenhet att hantera risker för område B – D.
 - Avdelningschef för verksamhetsområdena A – D har befogenhet att hantera risker för område A - D.
 - Avdelningschef för verksamhetsområdena E – H har befogenhet att hantera risker för område E – H, men saknar befogenhet att hantera risker för område A – D.

Riskhantering

- Riskbehandling
 - Risker kan
 - Accepteras
 - Reduceras med hjälp av åtgärder som minskar effekten
 - Undvikas med hjälp av åtgärder som eliminerar risken
 - Överförs

Riskhantering

- **Hot**
 - Önskad händelse som kan ge negativa konsekvenser
- **Konsekvens**
 - Resultat av en händelse
- **Sårbarhet**
 - Bristande förmåga
- **Sannolikhet**
 - Hur troligt det är att ett hot realiseras
- **Risk**
 - Möjligheten att ett givet hot nyttjar sårbarheten

Sammanfattning

Sammanfattning

- Det som presenteras i detta bildspel är ett förslag till vilka roller som får ett utpekat ansvar för arbetsuppgifter som är kopplade till informationssäkerhet (inkl. dataskydd och tekniskt arkivansvar).
- Vad som är föreslaget ger svar om att nuvarande delegationsordning behöver justeras.

Fortsatt arbete 2024 - 2026

- I det fortsatta arbetet inom projektet Etablera systematiskt informationssäkerhetsarbete kommer ytterligare ansvar att föreslås för roller inom förvaltningen
- Fortsatt arbete kommer att ske med riskanalyser ur ett arbetsmiljöperspektiv

Kontakt

Anna (Anna-Lena) Björk

Chief Information Security Officer (CISO)

Enhetschef Styrning och uppföljning av informationssäkerhet

GÖTEBORGS STAD Intraservice

Telefon: 031 367 00 00 | Mobil: 079 060 61 83

E-post: anna.bjork@intraservice.goteborg.se