Lokal anvisning för informationssäkerhet

Idrottsförvaltningen

Beslutad 2023-12-28
Reviderad [datum]

Lokal anvisning för informationssäkerhet

Dnr: 1.1.3/2023/3002

Kontaktperson: Johan Malmström

1 Bakgrund

Denna lokala anvisning beskriver roller och organisation för Idrottsförvaltningens informationssäkerhetsarbete. Dokumentet fastställdes av Marina Högland för idrottsnämndens räkning den 2023-12-28.

Den lokala anvisningen kompletterar stadens centrala riktlinje och tillämpningsanvisning för informationssäkerhet. Anvisningen förklarar hur idrottsförvaltningen lokalt tillämpar och arbetar med informationssäkerheten. Den förtydligar hur ansvarsfördelning och roller har anpassats för idrottsförvaltningen – vem som ansvarar, vilka stöd- och kontrollfunktioner samt övriga roller som i sitt uppdrag arbetar med skydd av informationstillgångar.

Den lokala tillämpningsanvisningen beskriver också hur idrottsförvaltningen systematiskt arbetar med samt följer upp informationssäkerheten.

Innehållsförteckning

1 Bakgrund ... 2
2 Organisation och roller ... 4
2.1 Ledning ... 4
2.1.1 Idrottsnämnden ... 4
2.1.2 Förvaltningschef ... 5
2.1.3 Chef ... 5
2.1.4 Systemförvaltare ... 6
2.2 Stödjande och uppföljande roller ... 6
2.2.1 Informationssäkerhetssamordnare (ISAM) ... 6
2.2.2 Dataskyddsombud (DSO) ... 7
2.2.3 Dataskyddssamordnare ... 8
2.2.4 Registrator ... 9
2.2.5 Systemadministratör säkerhet ... 9
2.2.6 ILS-samordnare ... 9
2.2.7 Arkivansvarig och arkivsamordnare ... 9
2.2.8 Säkerhetssamordnare ... 10
2.2.9 Kommunikatör ... 10
2.3 Övriga funktioner ... 10
2.3.1 Medarbetare ... 10
2.3.2 IT-funktioner ... 10
2.3.3 Verksamhetsspecialist ... 11
3 Nätverk och grupper ... 11
3.1 Informationssäkerhet och dataskydds-grupp ... 11
3.2 Nätverk för stadens informationssäkerhetssamordnare ... 11
3.3 Samverkan gemensam DSO ... 12
4 Årshjul ... 12
5 Rutiner och praktiskt arbete ... 12

2 Organisation och roller

Idrottsförvaltningens organisation för informationssäkerhet är indelad i tre olika nivåer. Den **styrande** omfattar strategiskt och operativt beslutande roller och funktioner.

De **stödjande** och **granskande** funktionerna är specialistfunktioner som stödjer förvaltningen i dess informationssäkerhetsarbete. De granskande funktionerna, utöver stadens egna revisorer, följer även upp att riktlinjer och lagstiftning följs.

2.1 Ledning

2.1.1 Idrottsnämnden

Idrottsnämnden är ytterst ansvarig för informationen och formellt informationsägare och personuppgiftsansvarig för idrottsförvaltningen. Idrottsnämnden ansvarar för att det finns ett ändamålsenligt och effektivt informationssäkerhetsarbete inom förvaltningen samt att stadsövergripande riktlinjer och vägledande dokument för informationssäkerhet följs.

Idrottsnämnden ansvarar för att en ändamålsenlig organisation finns på plats och för att nödvändiga resurser tilldelas samtliga funktioner för att kunna genomföra ett effektivt informationssäkerhetsarbete. I denna lokala anvisning beskrivs hur denna organisation fungerar i praktiken.

Idrottsnämnden har delegerat till förvaltningschef att utse dataskyddsombud enligt delegationsordning 1.2.1 samt anmäla till idrottsnämnden.

Idrottsnämnden delges årligen en så kallad GDPR årsrapport från dataskyddsombudet. Syftet är att idrottsnämnden med hjälp av rapporten ska kunna utöva sin lagstadgade skyldighet att informera sig om dataskyddsrisker för verksamheten.
Denna rapport delgavs senast idrottsnämnden i ärendet verksamhetsberättelse för år 2022 och godkändes av idrottsnämnden.

I idrottsnämndens ansvar ligger även att delegera uppgiften att besluta om informationshantering och regler för detta. Denna uppgift beskrivs i rubrik 2.1.2 samt 2.1.3 i detta dokument.

2.1.2 Förvaltningschef

Förvaltningschefen är nämndens delegat när det gäller de övergripande lednings- och styrningsfrågorna.

Förvaltningschef ansvarar för:

- Att fastställa de lokala tillämpningsanvisningarna och andra övergripande styrdokument för idrottsförvaltningen.
- Att utse en informationssäkerhetssamordnare och ansvara för att stödfunktioner för informationssäkerhet tilldelas de resurser som krävs.
- Att hålla sig underrättad om informationssäkerheten i idrottsförvaltningen, minst genom att inhämta den årliga rapporten ”Ledningens genomgång” från informations-säkerhetssamordnaren.
- Att se till att klassificeringsstruktur och hanterings-anvisningar och dokumenthanteringsplan har fastställts för verksamhetens informationshantering.

2.1.3 Chef

Ansvaret för att skydda informationen som hanteras inom verksamheten följer linjeansvaret. Varje chef har inom sin verksamhet ett särskilt ansvar för att informationen hanteras på ett korrekt sätt enligt gällande lagstiftning och riktlinjer. Ansvaret för informationshanteringen ska ligga så verksamhetsnära som möjligt, och inom idrottsförvaltningen innebär det som lägst enhets-chefsnivå. Chefen kan delegera och fördela ansvaret inom sin verksamhet på det sätt som bedöms lämpligt, men har fortsatt kvar det formella ansvaret.

Chefer inom idrottsförvaltningen ansvarar för:

- Att se till att samtliga medarbetare och konsulter som hanterar stadens information genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd årligen.
- Att följa upp och utreda de incidenter som verksamheten anmäler i stadens incidentrapporteringssystem (IA), samt att kontakta informationssäkerhetssamordnare eller dataskyddsombud vid incidenter som rör personuppgifter eller andra informationssäkerhetsfrågor.

- Att säkerställa att registervård genomförs inom chefens ansvarsområde och att meddela uppdatering till förvaltningens informationssäkerhetssamordnare.
- Att de inköp/upphandlingar som chef beslutar om följer gällande lagar vad gäller informationshantering, samt stadens och förvaltningens styrdokument.
- Att informationsinventering är gjord av den egna verksamheten med stöd från informations-säkerhetssamordnare och arkivfunktioner.

2.1.4 Systemförvaltare

En systemförvaltare[1] (objektledare) ansvarar för drift och förvaltning av en IT-tjänst. En systemförvaltare är utsedd för samtliga digitala tjänster hos idrottsförvaltningen.

Vilka som tilldelats rollen systemförvaltare inom idrotts-förvaltningen framgår i förteckningen över verksamhetens informationstillgångar som upprättas av informations-säkerhetssamordnaren.

När det gäller de IT-tjänster där drift sköts av extern leverantör eller på annan förvaltning, är verksamhetens (personuppgiftsansvarig) systemförvaltare ansvarig för tjänsten i relation till den beställda (personuppgiftsbiträde) tjänsten och fungerar då som lokalt ansvarig för hur systemet används i verksamheten. I de fall både drift och verksamhet finns inom idrottsförvaltningen förekommer rollen systemförvaltare specifikt för tjänstens drift.

Systemförvaltarens ansvar är:

- att tillse att informationstillgången är klassad och att handlingsplaner från klassning tas om hand för systemet
- att se till att förvaltningsplan och andra nödvändiga rutiner finns på plats och följs upp
- att tillse att stadens riktlinjer och tillämpningsanvisningar följs vad gäller informationssäkerhet för IT-tjänster
- att besluta om regler för tillgång till systemet och se till att dessa är kända av medarbetarna

2.2 Stödjande och uppföljande roller

2.2.1 Informationssäkerhetssamordnare (ISAM)

[1] För rollbeskrivning se stadens metodstöd för Pm3

Idrottsförvaltningens ISAM är utsedd av förvaltningschefen. Nu tjänstgörande ISAM utsågs 2019-01-19.

ISAM ansvarar för att samordna och följa upp det operativa informationssäkerhetsarbetet och att stötta samt vägleda idrottsförvaltningens verksamhet. ISAM ska arbeta utifrån styrning av vilka verksamhetsrisker och åtgärder som ska prioriteras.

ISAM ansvarar för:

- anmäla personuppgiftsincidenter till tillsynsmyndigheten inom 72 timmar i samråd med dataskyddssamordnare och dataskyddsombud
- att vara kontaktperson för stadens centralt informationssäkerhetsansvariga (CISO) samt rapportera allvarliga incidenter till denna
- att fungera rådgivande gentemot förvaltningens systemförvaltare, i projekt samt till ansvariga för upphandling
- att samverka med andra närliggande ansvarsområden och roller
- delta i förvaltningens informationssäkerhets- och dataskyddsgrupp
- att stödja verksamheterna i det strategiska arbetet, kartlägga information, informationsklassificera den, hantera incidenter samt att utbilda medarbetare och sprida kunskap om lokala rutiner
- att bevaka förändringar i lagstiftningen och händelser i omvärlden
- att genomföra uppföljning av det lokala informations-säkerhetsarbetet.
- följa upp idrottsförvaltningens register över hantering av personuppgifter (registerförteckningen)

2.2.2 Dataskyddsombud (DSO)

Nu tjänstgörande dataskyddsombud anmäldes till idrottsnämnden 2022-05-24. Förvaltningens dataskyddsombud utgörs av en konsult som delas av flera förvaltningar inom staden.

Dataskyddsombudets övergripande och viktigaste uppgift är att kontrollera att dataskyddsförordningen (GDPR) följs av verksamheten. Uppföljningen består bland annat i att utföra kontroller och informationsinsatser.

Dataskyddsombudet ska kunna agera självständigt och oberoende i sitt uppdrag och ska därför inte utföra det operativa arbetet. DSO har ett nära samarbete och kontakt med ISAM, vilket är nödvändigt för att arbetet ska bedrivas effektivt och leda till största möjliga nytta.

Dataskyddsombudet har dessutom i uppgift att:

- adjungeras till förvaltningens grupp för informations-säkerhet- och dataskydd
- vägleda, informera och ge råd om hur relevanta skyddsåtgärder ska väljas och implementeras för att person- och integritetsskyddet ska upprätthållas
- ge råd vid personuppgiftsincidenter, i enlighet med verksamhetens incidentrutin
- ska alltid involveras i samband med konsekvens-bedömningar och ges möjlighet att övervaka genomförandet
- vara en kontaktpunkt för tillsynsmyndigheten IMY
- ge stöd i arbetet med framtagande av styrdokument, riktlinjer, rutiner och mallar i syfte att förvaltningen ska behandla personuppgifter lagligt och korrekt
- ge stöd till dataskyddssamordnare och informationssäkerhetssamordnare i arbetet med att säkerställa förvaltningens hantering av personuppgifter

2.2.3 Dataskyddssamordnare

Dataskyddssamordnare utgör informationssäkerhetssamordnarens och dataskyddsombudets länk till chefer och medarbetare i verksamheterna.

- delta i förvaltningens informationssäkerhets- och dataskyddsgrupp.
- delta i arbetet med den centrala förteckningen över de behandlingar av personuppgifter som verksamheterna hanterar
- ge råd och stöd gällande hantering av personuppgifter
- vid behov anmäla eventuella brister till dataskyddsombudet
- vara kontaktperson gentemot dataskyddsombudet
- tillsammans med informationssäkerhetssamordnaren ta fram styrdokument, rutiner, riktlinjer och mallar gällande hantering av personuppgifter
- tillsammans med informationssäkerhetssamordnaren informera och utbilda gällande hantering av personuppgifter

2.2.4 Registrator

- delta i förvaltningens informationssäkerhets- och dataskyddsgrupp
- är stödfunktion i framtagandet av dokumenthantering och arkivering
- hålla sig informerad om lagar och författningar som styr hanteringen av allmänna handlingar och diarieföring
- hålla diariets handlingar tillgängliga enligt offentlighets- och sekretesslagstiftningen och ser till att handlingarna registreras i förvaltningens ärendediarium
- samordna begäran utifrån den registrerades rättigheter (registerutdrag, rättelse, radering etc.)

2.2.5 Systemadministratör säkerhet

- delta i förvaltningens informationssäkerhets- och dataskyddsgrupp
- stödja informationssäkerhetssamordnaren
- följa upp och kontrollera avvikelser i passagesystemet- och inbrottslarmsystem
- tillsammans med informationssäkerhetssamordnaren utveckla och säkerställa informationssäkerhetsarbetet så att förvaltningens IT-verksamhet bedrivs med rätt krav på informationssäkerhet
- delta i uppföljning, analys och utredning av inträffade oönskade händelser inom informationssäkerhetsområdet
- delta i förvaltningens risk- och sårbarhetsanalyser (RSA)

2.2.6 ILS-samordnare

- samordnar uppföljningen och beredningen av nämndens ILS-arbete
- aktivt arbeta för att informationssäkerhet är med och följs upp i förvaltningens väsentlighets- och riskanalys samt införliva informationssäkerheten i verksamhetsplanen med stöd från informationssäkerhetssamordnaren

2.2.7 Arkivansvarig och arkivsamordnare

- arkivansvarig är administrativ avdelningschef
- arkivsamordnaren arbetar operativt tillsammans med arkivkonsult från stadsarkivet med arkivfrågor
- arkivsamordnaren deltar i förvaltningens informationssäkerhetsarbete och i dess inventeringar av informationstillgångar – både digitala och fysiska

- är stödfunktion i framtagandet av dokumenthantering och arkivering

2.2.8 Säkerhetssamordnare

- deltar i förvaltningens informationssäkerhets- och dataskyddsgrupp
- säkerställa helhetsperspektiv och samverkan i förvaltningens säkerhetsarbete

2.2.9 Kommunikatör

- deltar i förvaltningens informationssäkerhets- och dataskyddsgrupp
- deltar i kommunikationsfrågor och kommunikation via idrottsförvaltningens kanaler

2.3 Övriga funktioner

2.3.1 Medarbetare

Medarbetare inom idrottsförvaltningen ska:

- följa stadens riktlinjer och regelverk, både centrala och lokala
- ta del av informationen som finns om informationssäkerhet
- genomföra de obligatoriska utbildningarna inom informationssäkerhet och dataskydd
- nyanställda medarbetare godkänner stadens generella användarkontrakt i samband med sin första inloggning i stadens IT-miljö

2.3.2 IT-funktioner

IT-funktioner innebär i förvaltningens verksamhet rollerna IT-chef, systemförvaltare, IT-samordnare, IT-tekniker och systemadministratörer IT.

Dessa roller deltar aktivt i det operativa arbetet genom att t.ex. delge sin kunskap vid upphandlingar, införande av system, informationsklassningar och drift.

2.3.3 Verksamhetsspecialist

Inom idrottsförvaltningen finns även verksamhetsspecialister som förvaltar system i verksamheten. Hanteringen för varje system sätts för varje enskilt objekt och det finns minst en kontaktperson.

3 Nätverk och grupper

3.1 Informationssäkerhet och dataskydds-grupp

För att säkerställa en effektiv och ändamålsenlig organisation utvecklar förvaltningen fortlöpande arbetet inom informations-säkerhet och dataskydd. Det är ett komplext område som inbegriper ett flertal olika funktioner inom förvaltningen.

Det operativa och strategiska arbetet bedrivs av förvaltningens arbetsgrupp för informationssäkerhet och dataskydd. Arbetsgruppen hanterar strategiska och operativa informationssäkerhets- och dataskyddsfrågor. Gruppen ansvarar vidare för att informera och tillse att förvaltningens medarbetare utbildas i relevanta områden.
Deltagare:

- IT-chef, ordförande och sammankallande
- Informationssäkerhetssamordnare
- Systemadministratör säkerhet
- Registrator
- Dataskyddssamordnare
- Kommunikatör
- Säkerhetssamordnare
- Dataskyddsombud (särskild inbjudan)

Övriga adjungeras utifrån behov, till exempel arkiv-samordnare, systemförvaltare eller andra sakkunniga.

3.2 Nätverk för stadens informationssäkerhetssamordnare

Informationssäkerhetssamordnaren (ISAM) deltar i stadens nätverk för informationssäkerhet och dataskydd. Stadens informationssäkerhetsansvarig (CISO) ansvarar och bjuder in till mötena.

3.3 Samverkan gemensam DSO

Tillsammans med fem andra förvaltningar, (serviceförvaltningen, arbetsmarknadsförvaltningen, kulturförvaltningen, stadsarkivet och kyrkogårdsförvaltningen) delar förvaltningen på ett gemensamt upphandlat dataskyddsombud. Syftet är att säkerställa en oberoende och opartisk resurs med en granskande och rådgivande roll.

Samverkan sker genom en gemensam styrgrupp för administrativa chefer samt en operativ grupp där gemensamma frågor hanteras. Dataskyddsombudet deltar i båda grupperna.

4 Årshjul

Ett årshjul håller på att tas fram inom samverkan gemensam DSO. Där ska det årliga arbetet framgå.

5 Rutiner och praktiskt arbete

Baserat på kommande årshjul kommer rutiner och det praktiska arbetet att beskrivas under 2024.

.