Lokal anvisning för informationssäkerhet

SGA Fastigheter AB

Beslutad 2023-02-22

Lokal anvisning för informationssäkerhet

Dnr: SGAF 2022/72

Kontaktperson: Sara Feinberg

1 Bakgrund

Denna lokala anvisning beskriver roller och organisation för SGA Fastigheters AB:s (SGAF) informationssäkerhetsarbete. Dokumentet fastställdes av VD Mats Viker för styrelsens räkning den 2023-02-22.

Den lokala anvisningen uppdateras årligen enligt årshjulet.

Den lokala anvisningen kompletterar stadens centrala riktlinje och tillämpningsanvisning för informationssäkerhet och dokumenterar hur SGAF lokalt och praktiskt tillämpar och arbetar med informationssäkerheten. Den förtydligar hur ansvarsfördelning och roller har anpassats för SGAF – vem som ansvarar, vilka stödfunktioner och kontrollfunktioner som finns, och vilka övriga roller som i sitt uppdrag arbetar med skydd av informationstillgångar.

Den lokala tillämpningsanvisningen beskriver också hur SGAF systematiskt arbetar med, och följer upp, informationssäkerheten.

Innehållsförteckning

2 Organisation och roller

SGAF är ett litet bolag med 19 anställda. Merparten arbetar med att förvalta fastigheterna. Inom bolaget finns tre arbetsområden – fastighetsförvaltning, ekonomi och utveckling. Informationssäkerhet ligger hos utveckling.

2.1 Ledning (styrande)

2.1.1 SGA Fastigheters styrelse

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

Styrelsen ansvarar för att en ändamålsenlig organisation finns på plats och kan genomföra ett effektivt informationssäkerhetsarbete. I denna lokala anvisning beskrivs hur denna organisation fungerar i praktiken, under de förutsättningar som finns i ett litet bolag.

Styrelsen har ansvar att utse ett dataskyddsombud. Styrelse kan även delegera uppgiften till bolagschef, som då ska anmäla sitt beslut till styrelse.

Styrelsen inhämtar årligen en så kallad GDPR årsrapport från dataskyddsombudet. Syftet är att styrelse med hjälp av rapporten ska kunna utöva sin lagstadgade skyldighet att informera sig om dataskyddsrisker för verksamheten. Denna rapport har senast inhämtats för år 2021 och godkänts av styrelsen.

I styrelsens 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 Bolagschef

Bolagschefen är styrelsens representant (delegat) när det gäller de övergripande lednings- och styrningsfrågorna.

Bolagschef ansvarar för:

- Att fastställa de lokala tillämpningsanvisningarna och andra övergripande styrdokument för SGAF.
- Att utse en informationssäkerhetssamordnare och ansvara för att stödfunktioner för informationssäkerhet tilldelas de resurser som krävs.
- Att verksamheten tilldelas de resurser som behövs för att kunna upprätthålla god informationssäkerhet.
- Att hålla sig underrättad om informationssäkerheten i bolaget, minst genom att inhämta den årliga rapporten ”VP-anvisning: Ledningens genomgång” från informationssäkerhetssamordnaren.
- Att se till att klassificeringsstruktur och hanteringsanvisningar har fastställts för verksamhetens informationshantering.

2.1.3 Chef tillika processägare

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 ligger på bolagets fyra chefer, inkl. bolagschef. De är även processägare och tillser att processer finns där så behöver. Dessa ska även följa bolagets klassificeringsstruktur. Chefen kan delegera och fördela ansvaret inom sin verksamhet på det sätt som bedöms lämpligt, men har fortsatt kvar det formella ansvaret.

Chefer inom SGAF 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 IA, samt att kontakta dataskyddsombud och/eller informationssäkerhetssamordnare vid incidenter som rör personuppgifter eller andra informationssäkerhetsfrågor.

- Att säkerställa att registervård genomförs inom chefens verksamhet och att uppdatera och följa upp bolagets register över hantering av personuppgifter (det vill säga registerförteckningen).
- Att de inköp/upphandlingar som chef beslutar om följer gällande lagar vad gäller informationshantering, samt stadens och bolagets styrdokument.
- Att informationsinventering är gjord av den egna verksamheten med stöd från informations-säkerhetssamordnare och arkivfunktioner. Att se till att viktigare informationstillgångar är klassade och att verksamhetens it-tillgångar har en utsedd objektledare.
- Att vid behov ta fram lokala rutiner för den egna verksamheten vid behov.

2.1.4 Objektledare

En objektledare[1] ansvarar för drift och förvaltning av en it-tjänst. Objektledare är utsedda för samtliga it-tjänster hos SGAF.

Vilka som tilldelats rollen objektledare inom SGAF framgår i den förteckning över verksamhetens informationstillgångar som upprättas av informationssäkerhetssamordnaren.

När det gäller de it-tjänster där drift sköts på entreprenad eller på annan förvaltning, är verksamhetens (personuppgiftsansvarig) objektledare 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 bolaget förekommer ibland rollen objektledare specifikt för tjänstens drift.

Objektledarens ansvar är:

- Att tillse att informationstillgången är klassad och att handlingsplaner från klassning tas om hand för systemet.
- Att se till att objektplan 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.

[1] För rollbeskrivning se stadens metodstöd för Pm3

- Att utse övriga nödvändiga funktioner inom it (t.ex. objektspecialist).

2.2 Stödjande och uppföljande

2.2.1 Informationssäkerhetssamordnare (ISAM)

Bolagets ISAM är utsedd av bolagschefen. Nu tjänstgörande ISAM utsågs datum 2020-05-26.

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

ISAM ansvarar för:

- Att vara kontaktpunkt för stadens centralt informationssäkerhetsansvariga (CISO) samt rapportera allvarliga incidenter till denna.
- Att fungera rådgivande gentemot bolagets objektledare, i projekt samt till ansvariga för upphandling.
- Att samverka med andra närliggande ansvarsområden och roller.
- Att stödja linjeverksamheten när det gäller 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/revision av det lokala informationssäkerhetsarbetet.

2.2.2 Dataskyddsombud (DSO)

Nu tjänstgörande dataskyddsombud utsågs i september 2019 och anmäldes till dåvarande Datainspektionen, nu Integritetsskyddsmyndigheten (IMY). I samband med denna anvisning anmäls även DSO, Sara Wallin, till styrelsen. 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, vilket är komplext i en liten organisation. 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:

- Vägleda, informera och ge råd till verksamheten om hur relevanta skyddsåtgärder ska väljas och implementeras för att person- och integritetsskyddet ska upprätthållas.
- Ge råd vid personuppgiftsincidenter, i enlighet med verksamhetens incidentrutin. Dataskyddsombudet ska alltid involveras i samband med konsekvensbedömningar och ges möjlighet att övervaka genomförandet av dem.

2.2.3 ILS-samordnare

Verksamhetens ekonomichef samordnar uppföljningen och beredningen av bolagets ILS-arbete.
ILS-samordnaren ska aktivt arbeta för att informationssäkerhet är med och följs upp i bolagets väsentlighets- och riskanalys samt införliva informationssäkerheten i verksamhetsplanen med stöd från informationssäkerhetssamordnaren.

2.2.4 Arkivansvarig

Övergripande arkivfunktioner har en viktig funktion i stadens informationssäkerhetsarbete. Bolagets ISAM är även arkivansvarig. Därutöver finns arkivhandläggare (tillika DSO) samt arkivkonsult från Stockholms stadsarkiv. Bolagets informationssäkerhetsarbete och dess inventeringar av informationstillgångar – både digitala och fysiska täcks på så sätt in.

Arkivkonsult är stödfunktion i framtagandet av de dokument där hantering och arkivering av styrelsens samtliga informationstillgångar beskrivs, dvs bolagets hanteringsanvisningar/dokumenthanteringsplan och övrig arkivdokumentation.

Arkivfunktionernas roller beskrivs i bolagets arkivinstruktion.

2.3 Övriga funktioner

2.3.1 Medarbetare

Medarbetare inom SGAF ska följa stadens riktlinjer och regelverk (både centrala och lokala), ta del av den information som finns om informationssäkerhet och genomföra de obligatoriska utbildningarna inom informationssäkerhet och dataskydd. Nyanställda medarbetare godkänner stadens generella användarkontrakt i samband med sin första inloggning i stadens it-miljö, och ska därefter påminnas om kontraktets innehåll enligt en rutin som styrelsen beslutar om. SGAF har även lokala kontrakt och användarregler.

2.3.2 It-funktioner

Roller med denna expertfunktion deltar aktivt i det operativa arbetet genom att till exempel delge sin expertkunskap vid upphandlingar, införande av system/produkt, informationsklassningar och drift. It-funktioner innebär i bolagets verksamhet rollerna it-chef samt it-stöd. It-stödet är konsult via ett systerbolag.

2.3.3 Objektspecialist

Inom SGAF finns även de som genom administratörsbehörigheter på olika sätt förvaltar it-objekt i verksamheten. Strukturen/hanteringen för varje it-objekt sätts för varje enskilt objekt, men det finns alltid minst en kontaktperson. Objektledaren ansvarar för att utse den organisationen.

3 Nätverk och grupper

Exempel på nätverk och grupper som bolaget deltar inom ramen för denna anvisning är stadens nätverk för informationssäkerhetssamordnare (ISAM deltar) och dataskyddsombudsnätverket (DSO deltar).

4 Årshjul

Uppföljningar av informationssäkerhet i samtliga system sker löpande och vid behov, men minst i samband med det årliga arbetet med internkontrollplanen och RSA.
Uppföljningar av registret över personuppgiftsbehandlingar sker löpande och vid behov samt årligen i samband med årsrapporten.
Uppföljning av annan rutindokumentation sker löpande och vid behov.

5 Rutiner och praktiskt arbete

SGAF har samlat såväl stadens som bolagets egna policys och riktlinjer i två guider- en medarbetarguide och en guide för bolagets ledningsgrupp. Dessa finns på länkade på bolagets intranät. I samband med att bolagets alla medarbetare samlas på månadsmöten lyfts gemensamma frågor inom ramen för denna anvisning, till exempel aktuell information gällande informationssäkerhet.

Underskriftens äkthet valideras här: https://underskriftpas.stockholm.se/validera

Undertecknad av
Mats Viker

Datum
2023-02-22 15:20:05

Elektronisk underskrift

underskrift.stockholm.se