Verksamhetsutveckling

Styrelsen för Stockholm Vatten och Avfall AB

Anmälan av lokal anvisning för informationssäkerhet

FÖRSLAG TILL BESLUT

Styrelsen föreslås besluta

att godkänna anmälan

Christian Rockberger
Verkställande direktör

Anders Mohlin
TF Avdelningschef
Verksamhetsutveckling

Sammanfattning

Utifrån stadens riktlinje för informationssäkerhet i Stockholms stad har bolaget tagit fram en lokal anvisning för informationssäkerhet.

SLUT

Bilaga: Lokal anvisning för informationssäkerhet

STOCKHOLM VATTEN OCH AVFALL

Dokumentnamn: Lokal anvisning för informationssäkerhet		Fastställt datum:
Process: Hantera säkerhetsfrågor	Klassificeringsnummer: 2.6.1	Diarienummer: 24SVOA921
Processägare/processansvarig: Johanna Munther/Jonas Thorby	Processledare (dokumentansvarig): Jonas Thorby	

1 Bakgrund

Denna lokala anvisning beskriver roller och organisation för Stockholm Vatten och Avfalls (Bolaget) informationssäkerhetsarbete.

Den lokala anvisningen uppdateras årligen enligt årshjulet.

Den lokala anvisningen kompletterar stadens centrala riktlinje och tillämpningsanvisning för informationssäkerhet och dokumenterar hur bolaget lokalt och praktiskt tillämpar och arbetar med informationssäkerheten. Den förtydligar hur ansvarsfördelning och roller har anpassats för bolaget – 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 bolaget systematiskt arbetar med, och följer upp, informationssäkerheten.

Innehållsförteckning

2 Organisation och roller

Bolagets organisation för informationssäkerhet är indelad i tre olika nivåer. Den **styrande** omfattar operativt beslutande roller och funktioner i verksamheten. Dessa har på olika nivåer en budget och ett personalansvar, vilket även innefattar operativt ansvar för informationshanteringen inom den delen av verksamheten.

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

2.1 Ledning (styrande)

2.1.1 Styrelse

Styrelsen är ytterst ansvarig för informationen och formellt informationsägare och personuppgiftsansvarig för bolaget. 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 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.

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

Styrelsen inhämtar årligen en så kallad GDPR årsrapport från dataskyddsombudet. Syftet är att Styrelsen med hjälp av rapporten ska kunna utöva sin lagstadgade skyldighet att informera sig om dataskyddsrisker för verksamheten. Denna rapport har senast inhämtats för år 2023 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 bolaget.
- 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 Ledningens genomgång från informationssäkerhetssamordnaren.
- Att tillse att klassificeringsstruktur och informationshanteringsplan 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 bolaget innebär det som lägst på enhetschefsnivå. Chefen kan delegera och fördela ansvaret inom sin verksamhet på det sätt som bedöms lämpligt, men har fortsatt kvar det formella ansvaret.

Chefer inom bolaget 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 Incidentrapporteringssystemet 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 som hanteras av dataskyddsombudet, DSO.
- 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 ta fram lokala rutiner för den egna verksamheten vid behov.

2.1.4 Ägarskap generellt

Bolagets ledningsgrupp är ägare. Det betyder att enbart avdelningschefer är process-, informations-, system- och anläggningsägare och har ett ansvar att se till helheten utifrån bolagets bästa. Chefer i övrigt har ett delegerat anläggnings-, process-, system- och informationsansvar utifrån verksamhetsansvar och roll.

2.1.5 Processägare

All informationshantering i bolaget har en ansvarig chef. En ansvarig chef har utsetts för respektive process med särskilt uppdrag att se till att rutiner och instruktioner finns på plats för informationshanteringen inom processområdet. Dessa ska även stämma överens med bolagets klassificeringsstruktur. Den chef som ansvarar för en specifik process har benämningen processansvarig. Processansvarig kravställer på IT-verktyg som får användas i processen och hur information ska hanteras inom processen.

Principer för processägare och processansvarig

- Processägare är den som har det övergripande ansvaret över en av bolaget identifierad huvudprocess. Denna person är avdelningschef.
- Processansvarig har ansvar över en delprocess. Denna person är enhetschef, gruppchef eller team/arbetsledare.

Processägarens ansvar

- Utser processansvariga och processamordnare och ansvarar för att ge processorganisationen rätt förutsättningar för att utföra sitt uppdrag.
- Ansvarar för att processen som helhet lever upp till ställda krav och att dess ingående delar hålls aktuella och uppdaterade (inklusive styrande och stödjande dokument).
- Agerar ambassadör för bolagets processarbete och att bolagets processer tas fram i samverkan samt på ett enhetligt sätt
- Vid behov informera och eskalera till VD och bolagsledning för beslut.

Nedan kan delegeras

- Sätter upp processmål och följer upp.

Processägaren ska också följa upp processen genom att tillse att denna är effektiv och ändamålsenlig.

2.1.6 Informationsägare

Principer kring ägarskap och ansvar.

- Informationsägare är den som har det övergripande ansvaret för de informationstillgångar som skapas och används inom en verksamhet. "Ägare" innebär inte att personen/funktionen har äganderätt till tillgången, utan avser

ett ledningsansvar för underhåll, användning och säkerhet avseende den specifika informationstillgången.
- Informationsägare är en avdelningschef.

Informationsägarens ansvar
- Utser informationsansvarig för olika informationstillgångar och ansvarar för att ge informationsorganisationen rätt förutsättningar för att utföra sitt uppdrag. Så långt det är möjligt är det en fördel om informationsansvarig är processansvarig.
- Agerar ambassadör för bolagets informationshanteringsarbete
- Vid behov informera och eskalera till VD och bolagsledning för beslut

Nedan kan delegeras
- Ansvarar för att bedömning av en informationstillgångs riktighet, tillgänglighet, konfidentialitet och spårbarhet är gjord det vill säga en informationsklassning av olika informationstillgångar. Utförs av informationsansvarig, skrivs under av ägaren.
- Ansvarar för att det finns principer för styrning av åtkomst och behörighet.
- Ansvarar för att RSA genomförs av processer och system som använder informationstillgången samt utifrån resultat ansvarar för att kontinuitetsplaner finns vid behov.

Ansvar för att personuppgifter hanteras korrekt (beslutsfattande enligt delegationsordning)

2.1.7 IT systemägare

Principer för systemägare IT
- Ägande och ansvar bör i första hand samlas på avdelningen Verksamhetsutveckling för en samordnad, effektiv och säker utveckling och förvaltning av IT-system inom bolaget.
- Utveckling och förvaltning ska ske i nära samarbete med verksamheterna och bolagets ledningsgrupp spelar en avgörande roll när det gäller prioriteringar och långsiktig inriktning.

Ansvar för IT-systemägare
- Utser systemansvarig och ansvarar så att IT-organisationen har rätt förutsättningar för att utföra sitt uppdrag.
- Övergripande ansvar för IT-tjänster och lösningar.
- Agerar ambassadör för bolagets arbete med bolagets IT-system och tjänster samt att bolagets IT-system utvecklas i samverkan på ett enhetligt sätt
- Vid behov informera och eskalera till VD och bolagsledning för beslut.

Nedan kan delegeras
- Ansvarar för att dokumentation finns för system och drift av system.
- Ansvarar för att avtal finns och samverkan med finansavdelningen vid inköp/upphandling.

- Ansvarar för att IT-system som hanterar personuppgifter har sådan funktionalitet som krävs för detta.
- Ansvarar för att IT-system uppfyller de krav som ställs enligt informationsklassningen av informationen i systemet.
- Ansvarar för att IT-system som hanterar allmänna handlingar uppfyller relevant delmängd av Stadsarkivets krav på sådana system.
- Ansvarar för att IT-systemet uppfyller de verksamhetskrav som ställs från övriga relevanta intressenter, som process-/informationsägare.
- Ansvarar för att bolagets systemportfölj följer lagar och förordningar samt stadens IT-riktlinjer.
- Ansvarar för utveckling och avveckling av system

2.2 Stödjande och uppföljande

2.2.1 Informationssäkerhetsansvarig (ISAM)

Bolagets informationssäkerhetsansvarige är utsedd av bolagschefen. Nu tjänstgörande informationssäkerhetsansvarig utsågs 2018-06-11.

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

Informationssäkerhetsansvarig ansvarar för:

- Att vara kontaktpunkt för stadens centralt informationssäkerhetsansvariga (CISO) samt rapportera allvarliga incidenter till denna.
- Att fungera rådgivande gentemot förvaltningens/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 anmäldes till nämnd/styrelse datum 2022-03-24.

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.. DSO har ett nära samarbete och kontakt med Informationssäkerhetsansvarig, 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 ILS-samordnare 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 och arkivarie

Övergripande arkivfunktioner har en viktig funktion i stadens informationssäkerhetsarbete. Arkivfunktionen, arkivansvarig och arkivarie deltar aktivt i bolagetsinformationssäkerhetsarbete och i dess inventeringar av informationstillgångar – både digitala och fysiska.

Arkivansvarig och arkivarier är stödfunktioner i framtagandet av de dokument där hantering och arkivering av Styrelsens samtliga informationstillgångar beskrivs, det vill säga bolagets informationshanteringsplaner och övrig arkivdokumentation.

Arkivansvarig (utses på delegation av VD, förvaltningschef)

- Fastställa arkivorganisation och planer för arkivverksamheten.
- Svara för formella framställningar om gallring till Stockholms stadsarkiv samt närvara vid inspektioner.
- Teckna avtal om leveranser till stadsarkivet.

Arkivfunktionernas roller beskrivs i bolagets arkivinstruktion/arkivorganisation.

2.3 Övriga funktioner

2.3.1 Medarbetare

Medarbetare inom bolaget 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. Bolaget 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 bolagetsverksamhet rollerna IT-chef, systemförvaltare, IT-strateg, IT-samordnare, IT-tekniker, IT-partner och systemspecialist.

2.3.3 Särskild systemspecialist/objektspecialist

Inom bolaget finns även de som genom administratörsbehörigheter på olika sätt förvaltar IT-system i verksamheten.

3 Nätverk och grupper

Respektive ansvarig deltar i Stadens nätverk för:

- Informationssäkerhetssamordnare
- Dataskyddsombudsnätverket
- IT-chefer
- Säkerhetschefer

4 Årshjul

Arbete pågår med att skapa ett årshjul som schemalägger utförandet av följande aktiviteter:

- Arbetet med VOR (november)
- Uppföljning/klassning av informationssäkerhet i
    - System
    - Processer
    - Informationstillgångar

- Kontroll/revision av registret över personuppgiftsbehandlingar.
- Kontroll/revision av behörighetstilldelning i system
- Kontroll/revision av ändringshantering i system.
- Kontroll/revision av utförd RSA (enligt Stadens riktlinjer sker i januari)

5 Rutiner och praktiskt arbete

Följande lokala rutiner har bolaget på plats. Rutinerna följs upp/revideras.

- Internkontroll
- Information till nyanställda
- Introduktionsutbildning för nyanställda
- Underskrift av sekretessförbindelse
- Medgivande och samtycke
- Hemarbete
- Behörighetsadministration
- Uppdatering av intranätssida
- e-utbildning
- Följa upp PUB-avtalshanteringen
- NIS-incidenter
- Registerförteckning
- Ändringshantering (inkluderar uppdatering och kapacitet)

Fastställd 2024-06-18

Christian Rockberger
VD