

Beslutsunderlag

Styrelsemöte 2025-01-31

Telefon: [031 64 74 00](tel:031647400)

Handläggare: Lars Tingström

Mejladress: lars.tingstrom@gryaab.se

Gryaabs policy för informationssäkerhet

Förslag till beslut

I styrelsen för Gryaab AB:

Gryaabs policy för informationssäkerhet, enligt beslutsunderlagets bilaga 1, fastställs.

Policyn ska revideras minst en gång per mandatperiod.

Beskrivning av ärendet

I ärendet lämnas förslag till en policy för informationssäkerhet för Gryaab. Den föreslagna policyn framgår av bilaga 1. Arbetet med att upprätthålla en god informationssäkerhet innebär inte bara att ha ett robust tekniskt skydd, såsom brandväggar och antivirusprogram. En allt viktigare del handlar även om att etablera effektiva processer och skapa en säkerhetsmedveten kultur i hela organisationen.

De största riskerna kommer ofta inifrån varför tydliga processer, rutiner och policys är avgörande för att nå bra resultat och ett tillräckligt bra skydd. Gryaab har tidigare saknat en policy för informationssäkerhet och den nya policyn är en viktig del i det fortsatta arbetet med att stärka informationssäkerheten.

Syftet med policyn är att sätta de övergripande principerna för arbetet med informationssäkerhet som tillkommande rutiner och instruktioner kan förhålla sig till. Det pågår ett större arbete att ta fram rutiner och riktlinjer för att styra verksamheten till ett säkert användande av informationstillgångar. Denna policy är tänkt att hålla samman detta.

Policyn föreslås, liksom merparten av Gryaab:s övriga policyer, fastställas av styrelsen en gång per mandatperiod eller vid behov.

Bedömning ur ekonomisk dimension

Policyn är viktig ur ett ekonomiskt perspektiv eftersom brister i skydd av informationstillgångar kan resultera i höga kostnader för Gryaab i samband med olika typer av incidenter.

Det kan handla om stora kostnader för återställning efter ett intrång med till exempel kryptering eller förlorad data men det finns också risk för sanktioner utifrån gällande lagstiftning inom området (EU:s dataskyddsförordning (GDPR) samt kommande Cybersäkerhetslagen.)

Nödvändiga kostnader

Att arbeta med informationssäkerhet i enlighet med policyn kan innebära ökade kostnader för Gryaab. Att ställa höga krav på informationssäkerheten är viktigt både utifrån lagstiftning och utifrån rådande säkerhetsläge. Kostnaderna bedöms därför som nödvändiga för att ordna och driva anläggningen enligt lagen om allmänna vattentjänster.

Bedömning ur ekologisk dimension

Risken för incidenter som stöld av informationstillgångar eller sabotage genom till exempel kryptering är fortsatt hög. En sådan incident skulle försämra Gryaab:s möjligheter att genomföra sina huvuduppdrag med risk för till exempel ett sämre reningsresultat.

Bedömning ur social dimension

Gryaab:s policy för informationssäkerhet är viktig ur en social dimension. Skydd av personalens känsliga personuppgifter är en viktig del av detta. Spridning av känsliga personuppgifter kan leda till stora negativa konsekvenser för enskilda individer samt för Gryaab som helhet.

Att säkerställa en hög grad av informationssäkerhet minimerar också risken för omfattande driftstörningar vilket medför minskad risk för påverkan på vattendrag samt människors hälsa.

Samverkan

Ärendet har behandlats på lokalt samverkansgruppmöte 22 januari 2025.

Bilagor

1. Gryaab policy för informations säkerhet

Bedömning av ärendets principiella beskaffenhet

Av Gryaabs ägardirektiv följer att Gryaab AB ska anta för verksamheten lämpliga policyer som ska utvärderas och omprövas i en takt som bolaget finner lämpligt. Gryaab har sett skäl att anta en policy för informationssäkerhet. Gryaabs styrelse fastställer majoriteten av bolagets policyer och Gryaab bedömer därför inte att ärendet är av principiell beskaffenhet eller annars av större vikt.

Bolagets bedömning

Med det arbete som utförs på Gryaab inom informationssäkerhetsområdet både kopplat till den kommande Cybersäkerhetslagen och allmänt utifrån det försämrade säkerhetsläget är det viktigt att ha en övergripande policy för informationssäkerhet. Bedömningen är att den föreslagna policyn beskriver bolagets inriktning och ambitionsnivå på ett ändamålsenligt sätt. Styrelsen föreslås därför fastställa Gryaabs policy för informationssäkerhet enligt bilaga 1 och att policyn, ska revideras minst en gång per mandatperiod.



Datum 2025-01-31

Avdelning/grupp TF-AIT

Namn Lars Tingström

Gryaab AB, Box 8984, 402 74 Göteborg, [031-64 74 00](tel:031-647400), gryaab.se

Bilaga 1 Gryaabs policy för informationssäkerhet

Inledning

Denna policy utgår från och ligger helt i linje med Göteborgs Stads riktlinje för informationssäkerhet men förhåller sig till Gryaabs specifika verksamhet.

Policyn kompletteras av underliggande riktlinje och rutinbeskrivningar.

Syfte och omfattning

Syftet med denna policy är att redovisa Gryaabs åtagande samt de mål och principer som gäller för informationssäkerhetsarbetet på Gryaab.

Policyn gäller för alla användare som hanterar information tillhörande bolaget, däribland anställda, extern personal och Gryaabs politiska styrelse.

Policyn fastslås av styrelsen varje mandatperiod eller vid behov.

Introduktion till informationssäkerhet

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd av information. Detta innefattar information i alla dess former och oavsett hur informationen hanteras. Information, och de resurser som används för att hantera information, benämns informationstillgångar.

Rättsliga och rättsligt bindande krav i form av lagar, förordningar, föreskrifter och avtal ställer krav på informationshanteringen på Gryaab. Vad som är en lämplig nivå av skydd

för en viss informationstillgång blir avhängigt dessa krav, aktuell hotbild och i vilka situationer informationen hanteras.

Styrande principer och definition av informationssäkerhet

Arbetet med informationssäkerhet ska bedrivas systematiskt och riskorienterat. Skyddet av information ska anpassas efter tillämpliga krav, informationens värde för verksamheten och aktuell hotbild. Informationssäkerhetsarbetet på Gryaab har fokus på förebyggande och proaktiva aktiviteter, men ska samtidigt säkerställa att det finns kapacitet att hantera incidenter, allvarliga störningar och kriser, om sådana inträffar.

Informationssäkerhet innebär skydd av informationstillgångar avseende:

- **Konfidentialitet**, att information inte tillgängliggörs eller avslöjas för obehöriga.
- **Riktighet**, att informationen skyddas mot oönskad förändring, att information är korrekt och inte manipulerad eller förstörd.
- **Tillgänglighet**, att information är tillgänglig och användbar när den behövs.

Målsättning med informationssäkerhetsarbetet

En säker informationshantering är en förutsättning för, och syftar till att främja, ett högt förtroende från våra intressenter. Det huvudsakliga målet med informationssäkerhetsarbetet är att säkerställa en stabil drift av kärnverksamheten.

Långsiktigt uppnår vi detta genom att:

- Proaktivt skapa en robust och driftssäker IT/Automationsmiljö.
- Säkerställa god kompetens inom informationssäkerhet för Gryaabs anställda.
- God beredskap att förebygga och hantera incidenter.

Ansvar i informationssäkerhetsarbetet

Ansvar för att säkerställa en korrekt informationshantering följer det ordinarie verksamhetsansvaret. Alla som arbetar på Gryaab har ett ansvar att känna till och följa gällande regler avseende informationssäkerhet.

Ledningens genomgång

En gång per år ska Gryaabs ledningsgrupp och styrelse informeras om i vilken utsträckning införda informationssäkerhetsåtgärder motsvarar Gryaabs behov, kvarstående risker samt övriga hinder för att uppnå målsättningen med och inriktningen för arbetet med informationssäkerhet. Särskilda skäl som exempelvis allvarliga incidenter, brister, eller behov, kan motivera ytterligare rapporteringar.