Räddningstjänsten
ALINGSÅS-VÅRGÅRDA

Uppföljning internkontrollplan 2024

Tertial 2 – Informationssäkerhet

Typ av dokument: Redovisande dokument	**Gäller för:** Förbundet
Beslutande instans: Direktionen	**Giltighetstid:** Ej aktuellt
Datum för beslut: 2024-xx-xx § x	**Revideras senast:** Ej aktuellt
Diarienummer: 2024.052 AVRF	**Dokumentansvarig:** EC Insats och Beredskap

Internkontroll inom Alingsås och Vårgårda Räddningstjänstförbund 2024

Direktionen ska säkerställa att förbundet fullgör sitt förvaltningsansvar, det vill säga bedriver en effektiv verksamhet, följer lagar och förordningar och andra regler samt lämnar en tillförlitlig redovisning och rättvisande rapportering. Ett verktyg som direktionen har till sitt förfogande är intern kontroll och direktionen beslutade om internkontrollplan 2024 för Alingsås och Vårgårda Räddningstjänstförbund AVRF den 7 december 2023, § 32.

Av internkontrollplanen framgår att redovisning ska ske efter tertial 1, tertial 2 och tertial 3.

Ett av de identifierade områdena för internkontroll under 2024 är informationssäkerhet.

1. Finns riktlinje för informationssäkerhet?
2. Är ansvar och roller tydliggjorda?
3. Är riktlinjen känd och förankrad i förbundet?
4. Är information i förbundets kritiska IT-system klassad utifrån konfidentialitet, riktighet och tillgänglighet?

Bakgrund

Vi lever idag i ett informationssamhälle där större mängder information än någonsin tidigare bearbetas, lagras, kommuniceras och mångfaldigas. Informationssäkerhet omfattar hela samhället och är en angelägenhet för alla. Både vi som individer och samhället i stort använder mängder av information för att vår vardag ska fungera. Dagens informationshantering utförs dessutom i allt högre grad med stöd av IT, och inte sällan över Internet. Detta ökande beroende av IT innebär ökade risker – det sker en tydlig ökning av incidenter såsom dataintrång, bedrägerier och spridning av skadlig kod. Bakomliggande aktörer utgörs av enskilda individer, men också i form av organiserad brottslighet, terrorister och statsmakter. Detta ställer krav på organisationer att bedriva ett systematiskt och genomarbetat informationssäkerhetsarbete.

Informationssäkerheten omfattar förbundets alla informationstillgångar. Information är en av förbundets viktigaste tillgångar och hanteringen av den är en förutsättning för att verksamheten ska fungera. Med informationstillgångar avses all information oavsett om den behandlas manuellt eller automatiserat och oberoende av dess form eller miljön den förekommer i.

AVRF ska uppfylla lagar och regler kring informationssäkerhet, likaså uppfylla och motsvara privatpersoners, företags och andra organisationers förväntningar och behov kring att vi hanterar information på ett säkert sätt. Medarbetares kunskap och medvetenhet kring informationssäkerhet utgör en viktig del av förbundets informationssäkerhetsarbete.

Sammanfattning

Granskningen visar att förbundet lever upp till förväntningarna när det gäller att ha en tydlig riktlinje för informationssäkerhet och att fördela ansvarsområden på ett tydligt sätt.

Arbetet med att utbilda personalen i informationssäkerhet pågår just nu för att säkerställa att alla medarbetare har den kunskap som krävs.

Arbete pågår också med att genomföra en klassificering av förbundets samtliga informationstillgångar, vilket är en viktig del av det övergripande säkerhetsarbetet.

Uppföljning och tidsplan för pågående klassificeringsarbete föreslås i granskningen.

Eftersom det ofta är den mänskliga faktorn som utgör den svagaste länken inom IT- och informationssäkerhet, föreslås att förbundet inför regelbundna och återkommande utbildningsinsatser för personalen. Detta skulle bidra till att stärka både medvetenhet och förståelse kring säkerhetsfrågorna på ett långsiktigt och hållbart sätt.

Uppföljning av kontrollmoment för perioden 1 maj 2024 – 31 Augusti 2024.

1. Finns riktlinje för informationssäkerhet?

Ja, Diarienummer 2024.018 AVRF.
Riktlinjen beslutad 2024-03-01.
Kommunicerad till samtlig personal i veckobrevet vecka 10 där den även bifogas till samtliga medarbetare.
I aktuellt veckobrev skriver informationssäkerhetssamordnare att hon skall ut och muntligt kommunicera innehållet vid lämpligt tillfälle för de olika arbetsgrupperna. Detta arbete pågår just nu.

2. Är ansvar och roller tydliggjorda?

Säkerhetsskyddschef, Informationssäkerhetsansvarig, informationssäkerhetssamordnare samt Teknik och systemansvarig.

Vad som ingår i rollen framgår i dokumentet enligt nedan:

Alingsås kommun IT- avdelning
IT-avdelningen ansvarar för säkerheten i IT-miljön och att verksamhetens legala krav på IT följs.

Förbundsdirektionen
Förbundsdirektionen är ytterst ansvarig för informationssäkerheten i förbundet.

Säkerhetsskyddschef

Varje organisation som omfattas av Säkerhetsskyddslag (2018:585) ska ha en säkerhetsskyddschef. Förbundsdirektören har utsett en säkerhetsskyddschef inom AVRF. Följande ingår i rollen:

- *Leder och samordnar säkerhetsskyddsarbetet, och där inkluderas även informationssäkerhet.*
- *Kontrollerar att verksamheten bedrivs enligt säkerhetsskyddslagen och de föreskrifter som har meddelats i anslutning till lagen.*

<u>Informationssäkerhetsansvarig (CISO)</u>
Inom förbundet ska det finnas en utsedd person med ansvaret att leda, utveckla och samordna informationssäkerhetsarbetet. Detta ingår i ansvaret:

- *Ansvarar för att förbundets styrande dokument inom området är aktuella.*
- *Utvecklar och förvaltar metoder, vägledningar och annat stödmaterial inom informationssäkerhetsområdet.*
- *Ansvarar för kompetensförsörjning och att öka informationssäkerhetsmedvetandet inom förbundet, t.ex. genom rådgivning och utbildning.*
- *Stöttar förbundet i frågor som rör informationssäkerhet.*
- *Genomför kontroll och uppföljning av informationssäkerheten i förbundet.*
- *Omvärldsbevakar inom informationssäkerhetsområdet.*
- *Administrerar SKR:s KLASSA-verktyg.*

<u>Informationssäkerhetssamordnare</u>
Förbundets informationssäkerhetssamordnare leder och samordnar arbetet med informationssäkerhet och dataskydd i förbundet och genomför årliga aktiviteter för informationssäkerhet och dataskydd. Följande ingår i rollen:

- *Leder genomförandet av verksamhets- och riskanalys för förbundet.*
- *Leder genomförandet av informationsklassningar för förbundet.*
- *Administrerar och är främsta utförare av SKR:s KLASSA-verktyg.*
- *Ansvarar för att förbundets behandlingsregister hålls uppdaterat.*
- *Samordnar och hanterar registrerades rättigheter.*
- *Leder genomförandet av konsekvensbedömning om dataskydd om så behövs.*
- *Stöttar vid incidenthantering, inklusive personuppgiftsincidenter.*
- *Stöttar vid anskaffning av nya tjänster vad gäller informationssäkerhet och dataskydd.*
- *Deltar i medlemskommunernas informationssäkerhetsnätverksträffar.*
- *Bidrar med information för kontroll och uppföljning av informationssäkerheten.*
- *Stöttar i förbundets kontinuitetsplanering.*

<u>Teknik- och systemansvarig</u>
Följande ingår i rollen:

- *Säkerställer att förbundet har en säker drift av IT-miljö, nätverk och tillhörande infrastruktur.*
- *Deltar i medlemskommunernas informationssäkerhetsnätverksträffar.*

Förbundets revisorer
Förbundets revisorer utför kontroll av informationssäkerheten inom ramen för ordinarie revisioner.

Vem som har tilldelats vilken roll framgår i riktlinjens bilaga:

Roll	**Rollinnehavare**
Säkerhetsskyddschef	Fredrik Alenström, insatsledare
Informationssäkerhetsansvarig (CISO)	Chef Myndighetsavdelningen, Emma Gustafsson
Informationssäkerhetssamordnare	Kvalificerad handläggare, Jeanette Seehase
Teknik- och systemansvarig	Driftledare, Claes Sannestål

3. Är riktlinjen känd och förankrad i förbundet?

För att kunna svara på denna fråga har en enkät delats ut och besvarats av 32 medarbetare inom förbundet. Syftet med enkäten är att få en inblick i hur väl medarbetarna känner till den riktlinje som finns samt dess syfte. Deltagarna har fått besvara frågor kring deras kunskap om riktlinjen, deras förståelse av syftet bakom den, och hur den tillämpas i verksamheten. Enkäten innehåller fem frågor som berör själva innehållet i riktlinjen, samt ytterligare frågor som handlar om vem som bär ansvaret för olika områden inom förbundet. Resultaten visar att det har varit en stor variation i hur många rätt svar medarbetarna har gett. I genomsnitt har medarbetarna svarat korrekt på 70 % av frågorna. Denna variation kan sannolikt förklaras av huruvida medarbetarna deltagit i den pågående utbildningsinsatsen som just nu genomförs inom förbundet.

Eftersom det verkar finnas ett tydligt samband mellan deltagande i utbildningen och hur väl medarbetarna svarar på enkäten, kommer återkommande utbildningsinsatser att föreslås som en lämplig åtgärd framöver. Detta skulle bidra till att säkerställa en bättre kunskap om riktlinjen och stärka medarbetarnas förståelse för IT och informationssäkerhet inom förbundet.

4. **Är information i förbundets kritiska IT-system klassad utifrån konfidentialitet, riktighet och tillgänglighet?**

Alingsås och Vårgårda Räddningstjänstförbund står bakom Alingsås kommuns Informationssäkerhetspolicy som innehåller långsiktiga övergripande mål (3 – 5 år) och inriktning med informationssäkerhet. Dessa mål är:

AVRF ska uppnå och upprätthålla informationssäkerhet som

- innebär en robust, säker och tillförlitlig informationshantering.
- i möjligaste mån motsvarar medborgares och externa verksamheters behov och förväntningar.

- möjliggör och underlättar digitalisering och att den sker med tillräcklig säkerhet.
- möjliggör att samtliga kritiska informationstillgångar informationsklassas.

Under 2023 anslöt sig AVRF till SKR:s klassificeringsverktyg KLASSA. Fokus under det året var att klassa de tjänsteappar som används på privata telefoner. Anledningen till att valet föll på just apparna var dels för att det var något som upplevdes kunna utgöra en risk för informationssäkerheten, men dels också för att objekten i sig är mindre och därmed bra att börja med när man är ovan vid verktyget. Målet var att genomföra tre stycken men utfallet blev fyra. Planen under 2024 är att genomföra tre klassningar och att det ska vara tre delar av verksamhetssystemet Daedalos genomförs. Två av de planerade delarna gick att genomföra i samma klassning, vilket gjordes under Q3 2024. Därmed kvarstår en del som planeras genomföras under Q4.

Klassning är en omfattande process där många frågor ska besvaras avseende varje objekt. I Alingsås kommun har man applicerat en kravmall som innebär att ett flertal av frågorna besvarats redan i mallen, det vill säga de frågor som är generella rörande organisationen och alltid har samma svar. Vi på AVRF har inte kunnat tillämpa mallen på samma sätt, utan ett arbete att manuellt lägga in svar på liknande frågor har gjorts, dock ännu inte i sin helhet.

Innan Handlingsplan för informationssäkerhet 2025 görs, kommer ansvariga att göra en bedömning av vilken prioritet övriga objekt ska ha och utifrån det göra en mer långsiktig plan för fortsatt arbete med klassning av kritiska system och övriga informationstillgångar.

Förslag till åtgärd.

Eftersom det verkar finnas ett tydligt samband mellan deltagande i pågående utbildningsinsats och hur väl medarbetarna svarar på enkäten, föreslås återkommande utbildningsinsatser som en lämplig åtgärd framöver.

Granskningen har inte visat om det finns en tydlig tidsplan och prioritering för klassificeringen av informationstillgångarna. Därför föreslås att en prioriteringsordning och tidsplan tas fram, samt att detta arbete följs upp löpande på lämpligt sätt.