Dokumentnamn: **Informationssäkerhetspolicy**	Dokumenttyp: **Policy**
Godkänt av: **Styrelsen för Kraftringen Energi AB (publ)**	Godkänt datum: **2026-03-17**

Informationssäkerhetspolicy

Kraftringen är den regionala drivkraften som tar ansvar för ett hållbart energisystem och tryggar energi för framtida generationer.

Denna policy säkerställer skyddet av företagets informationstillgångar och IT-infrastruktur, med särskilt fokus på driftsäkerhet, kontinuitet samt efterlevnad av lagar och branschstandarder.

Styrelsen har det övergripande ansvaret för att informationssäkerhetsarbetet styrs, följs upp och utvecklas i enlighet med tillämpliga lagkrav, inklusive cybersäkerhetslagen. Styrelsen godkänner och utövar tillsyn över koncernens åtgärder för hantering av cybersäkerhetsrisker samt säkerställer att tillräckliga resurser och befogenheter finns.

Mål för Kraftringens systematiska informationssäkerhetsarbete är att:

- Skydda energisystemets stabilitet mot cyberhot, sabotage och tekniska fel.
- Upprätthålla konfidentialitet, riktighet och tillgänglighet i affärskritisk och operativ information.
- Främja en stark säkerhetskultur - Genom kontinuerlig utbildning och riskmedvetenhet.
- Leverera robust redundans – genom driftssäkerhet och systemtillgänglighet
- Skydda kritiska system och styrfunktioner – Förhindra obehörig åtkomst till SCADA-system och andra verksamhetskritiska system.
- Stärka cybersäkerheten och incidentberedskapen – Implementera effektiva detekterings-, respons- och återställningsförmågor vid säkerhetsincidenter.
- Öka medvetenhet och ansvar hos medarbetare och leverantörer – Genomföra regelbunden utbildning och kravställa säkerhet i hela leverantörskedjan.

Vi uppnår våra mål genom att:

- Alla bidrar aktivt till en säker arbetsplats genom att uppmärksamma brister, hantera risker, följa rutiner och förstå sitt bidrag till säkerhetskulturen.
- Varje chef har ansvar för att implementera policyn i sin verksamhet och driva det löpande systematiska informationssäkerhetsarbetet, identifiera och hantera risker, formulera mål och uppmuntra en lärande säkerhetskultur.
- Varje medarbetare tar ansvar för att känna till verksamhetens mål och uppdrag, förstå sin roll och betydelsen av det egna arbetet, påverka sin egen arbetssituation och utveckla sin kompetens inom informationssäkerhet.

Denna policy gäller för hela koncernen, alla som vistas på våra arbetsplatser samt externa samarbetspartners med åtkomst till företagets information.

Efterlevnad av denna policy följs upp systematiskt inom ramen för koncernens ledningssystem för informationssäkerhet. Minst årligen rapporteras informationssäkerhetsarbetets status, riskbild och väsentliga händelser till koncernledning och styrelse som underlag för styrning, beslut och förbättringsåtgärder.

Bristande efterlevnad av denna policy ska rapporteras och hanteras som en avvikelse. Korrigerande åtgärder ska vidtas för att minska risker och förhindra upprepning. Allvarliga eller upprepade överträdelser kan medföra arbetsrättsliga, avtalsrättsliga eller andra konsekvenser enligt gällande regelverk. Denna policy utvärderas årligen av koncernledning och styrelse.