

Dokumentnamn: Informationssäkerhetspolicy	Dokumenttyp: Policy
Godkänt av: VD för Krafringen Energi AB (publ)	Godkänt datum: 2025-01-28

Informationssäkerhetspolicy

Krafringen 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 och efterlevnad av lagar och branschstandarder. Vi är starkt beroende av information för produktivitet, kvalitet och effektiv måluppfyllnad för att driva en trygg och stabil leverans till våra kunder.

Mål för vårt systematiska informationssäkerhetsarbete är att:

- Skydda energisystemets stabilitet mot cyberhot, sabotage och tekniska fel.
- Upprätthålla konfidentialitet, riktighet och tillgänglighet i affärskritisk och operativ information.
- Följa gällande regelverk, såsom NIS2-direktivet, GDPR och säkerhetsskyddslagstiftningen.
- Främja en stark säkerhetskultur - Genom kontinuerlig utbildning och riskmedvetenhet.
- Säkerställa driftssäkerhet och systemtillgänglighet – Implementera robusta skyddsåtgärder för att förhindra driftstörningar och säkerställa redundans.
- Skydda kritiska system och styrfunktioner – Förhindra obehörig åtkomst till SCADA-system och andra verksamhetskritiska system.
- Efterleva nationella och internationella regelverk – Säkerställa att företagets hantering av information uppfyller krav från myndigheter och standarder (t.ex. NIS-2 direktivet, Säkerhetsskyddslagen m fl.).
- 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 och alla som vistas på våra arbetsplatser samt externa samarbetspartners med åtkomst till företagets information.