KOMMUNINVEST I SVERIGE AB

Policy för informationssäkerhet

R5P

Fastställd av styrelsen	Dokumentansvarig	Dokumentägare	Informationsklass
2023-12-06	Chef Juridik och Inköp	Styrelsen	Intern

Externa regler

FFFS 2014:1
FFFS 2014:4
FFFS 2014:5
Offentlighets och sekretesslagen (2009:400)
Arkivlag (1990:782)
Dataskyddsförordningen (GDPR)
EBA/GL/2019/04
EBA/GL/2021/05
Bolagets regelverk för styrning av informationssäkerhet baseras även på standarderna i ISO/IEC 27000-serien.

Tidigare versioner

2023-05-23

Bakgrund mm

Kommuninvest i Sverige AB (nedan Bolaget) ska ha en god styrning och intern kontroll. Styrelsen ansvarar för att tillse att Bolaget följer lagar och tillämpliga nationella och europeiska regelverk som reglerar Bolagets verksamhet. Bolagets styrdokument består av dokument beslutade av styrelse, VD eller respektive ansvarig. Styrelsen fastställer policyer och vissa styrelseinstruktioner. Vid behov kan dessa styrdokument brytas ned i instruktioner, som fastställs av VD. Därefter kan instruktionerna brytas ned i mer detaljerade beskrivningar vilka fastställs av respektive ansvarig. Styrelsen ska fastställa policyer årligen och tillse att dessa efterlevs och regelbundet bedöms i verksamheten. Styrelsen är ytterst ansvarig för att Bolaget har en ändamålsenlig och effektiv verksamhet samt ett väl utvecklat system för riskhantering och regelefterlevnad.

Denna policy omfattar Bolagets styrelse, ledning, samtliga anställda, konsulter, samarbetspartners, ombud och uppdragstagare som är berörda av Bolagets verksamhet. Policyn är tillämplig på alla delar av verksamheten och inkluderar även verksamheter och områden som lagts ut till annan part (outsourcing).

VD ansvarar för att implementera och följa upp efterlevnaden av denna policy samt rapportera detta till styrelsen. Det åligger också VD att årligen eller vid behov bedöma och uppdatera innehållet i denna policy och föredra den för styrelsen, med eventuella förslag på ändringar.

1 Inledning

I denna policy har bolagsstyrelsen för Kommuninvest i Sverige AB (Bolaget) fastställt interna regler för informationssäkerhetsarbetet i Bolaget.

Denna policy utgör tillsammans med IT-policy och Policy för säkerhet och kontinuitet grunden för Bolagets informationssäkerhetsarbete och anger riktningen för hur arbetet ska bedrivas. Informationen som hämtas in till, skapas och förvaltas inom Bolaget är en viktig resurs och ska:

- vara korrekt och fullständig,
- finnas tillgänglig vid behov,
- vara skyddad mot obehörig åtkomst och
- kunna återskapas och vara spårbar.

Målet för informationssäkerhetsarbetet är att riskfokuserat och utgående från aktuell hotbild medverka till att Bolagets verksamhet når sina affärs- och verksamhetsmål med högsta möjliga digitala motståndskraft.

2 Ledningssystem informationssäkerhet

Chef Juridik och inköp ansvarar för Bolagets ledningssystem för informationssäkerhet. Ledningssystemet innehåller flera olika delar bl a rutiner för och kontroller kopplade till:

- Fysisk säkerhet
- Skydd av datakommunikation och drift
- Loggning och övervakning
- Separation av utvecklings-, test och produktionsmiljöer
- Styrning av åtkomst och information
- Säkerhetskrav på IT-system vid inköp, vid köp av IT-tjänster, utveckling, underhåll och avveckling
- Incidenthantering
- Kontroll av IT-systemen mot fastställd informationssäkerhetsnivå

Regler om IT-säkerhet finns i Bolagets IT-policy. Regler om fysisk säkerhet finns i bolagets policy för säkerhet och kontinuitet. Vid köp av IT-tjänster eller andra tjänster eller produkter som innehåller frågor om informationssäkerhet ska också Bolagets regler om utlagd verksamhet beaktas.

Ledningssystemen för säkerhet och kontinuitet, informationssäkerhet och IT ska ses som en helhet för arbetet med alla frågor kring säkerhet i verksamheten och de olika områdena samarbetar för att gemensamt bidra till ett så effektivt arbete som möjligt.

2 Grundläggande krav

- Bolaget ska ha ett definierat grundskydd för all information.
- Informationssäkerhetsfrågor ska vara naturligt integrerade i Bolagets processer och i det dagliga arbetet.
- Informationssäkerheten ska som princip hålla lika hög nivå vid arbete utanför Bolagets ordinarie kontorslokaler.
- Alla medarbetare ska ha utbildning i gällande riktlinjer samt vara medvetna om det egna ansvaret för informationssäkerheten.
- Tilldelning av behörigheter ska ske i ett enhetligt administrerat behörighetssystem.
- Användare ska endast ha behörighet som krävs för att kunna utföra sina arbetsuppgifter.
- Alla medarbetare ska informeras om att deras aktiviteter i Bolagets utrustning kan komma att övervakas och följas upp av informationssäkerhetsskäl.
- Krav på informationssäkerhet ska integreras i systemutveckling och systemförvaltning både gällande egenutvecklade och utkontrakterade system.
- Informationssäkerheten ska vara en del av Bolagets kontinuitetsplanering.
- Efterlevnaden av Bolagets regler ska testas genom återkommande övningar och granskas genom uppföljningar.
- Bolaget ska eftersträva största möjliga digitala motståndskraft.

3 Åtkomstbehörigheter

Av ledningssystemet ska det framgå hur Bolaget ska tilldela, ändra och ta bort åtkomstbehörigheter till IT-system.

Bolaget ska regelbundet, dock minst årligen, kontrollera att befintliga åtkomstbehörigheter är begränsade till behov utifrån tilldelade arbetsuppgifter.

4 Säkerhetsnormer för informationssäkerhet

Bolagets informationstillgångar avser information som har muntlig, skriven eller elektronisk grundform oavsett hur den senare bearbetas, lagras eller transporteras.

Bolagets information ska skyddas mot intrång, förvanskning, förlust eller stöld på de medier som informationen förvaras.

En förutsättning för att uppfylla Bolagets övergripande mål för informationssäkerhet är ett systematiskt och långsiktigt säkerhetsarbete.[1] Bolagets informationssäkerhetsarbete ska därför bedrivas utifrån följande säkerhetsaspekter:

Konfidentialitet: Att information skyddas från obehörig insyn.

Riktighet: Att informationen ska skyddas mot oavsiktlig och avsiktlig förvanskning.

Spårbarhet: Händelser i informationsbehandlingen ska kunna spåras. Det ska vara möjligt att härleda specifika aktiviteter eller händelser till ett identifierat objekt, till exempel dokument, användare, komponent, fysisk plats eller IT-system. Det ska gå att se vilka förändringar som skett eller gjorts, när ändringen gjordes och av vem dessa har utförts**.**

Tillgänglighet: Att informationen finns tillgänglig för rätt person vid rätt tillfälle. Tillgång till system och resurser ska behovsbedömmas och vara präglade av en hög säkerhetsnivå.

5 Organisation och ansvar

Chef för Juridik och inköp har ansvar för att Bolagets informationssäkerhetsarbete efterlever aktuella regulatoriska krav och är anpassat mot rådande hotbild.

Ansvar för informationssäkerhet mellan kravställande och genomförande roller i verksamheten ska vara tydligt definierat och fastställt.

6 Riskanalys

Bolaget ska årligen och vid förändringar som har betydelse för informationssäkerheten, analysera de risker som är hänförliga till informationssäkerhet. Bolaget ska utifrån dessa analyser men också efter inträffade incidenter besluta om hur det ska hantera identifierade risker.

Riskanalysen och beslutade åtgärder ska dokumenteras.

Chef Juridik och Inköp ansvarar för att riskanalysen genomförs.

7 Rapportering

Informationssäkerhetsarbetet ska vid behov och minst årligen avrapporteras till styrelsen.

[1] Mer om Bolagets övergripande säkerhetsarbete och regelverk för kontinuitetshantering går att läsa i R4P Policy för säkerhet och kontinuitet.