TJÖRNS kommun

Riktlinjer för informationssäkerhet

Typ av styrdokument	Riktlinjer
Beslutsinstans	Kommunstyrelsen
Beslutsdatum och paragraf	2023-06-01, § 134
Diarienummer	KS 2023/154
Datum för senaste revidering	2023-05-06
Giltighetstid	Tills vidare
Dokumentansvarig funktion	Informationssäkerhetssamordnare
Målgrupp för dokumentet	Styrelser och nämnder

TJÖRNS kommun

Revideringar

Beslut	Diarienummer	Revidering avser

TJÖRNS kommun

Innehåll

1 Inledning

1.1 Bakgrund

Information är en grundläggande byggsten i Tjörns kommun, på samma sätt som medarbetare, lokaler och utrustning är andra grundläggande byggstenar.

Arbetet med informationssäkerhet omfattar införandet och förvaltandet av administrativa regelverk så som en riktlinje likt den här, tekniskt skydd med bland annat brandväggar och kryptering samt fysiskt skydd med till exempel skal- och brandskydd. Det handlar om att skapa och bevara ett helhetsgrepp och ett fungerande långsiktigt arbetssätt för att ge organisationens information det skydd den behöver. Genom ett systematiskt arbete med informationssäkerhet kan kommunen öka kvaliteten i och förtroendet för sin verksamhet.

Sammantaget handlar informationssäkerhet om den samlade effekten av organisatoriska, administrativa och tekniska åtgärder som vidtas för att skydda informationstillgångar.

1.2 Ledningens styrning och prioriteringar

I det systematiska informationssäkerhetsarbetet reviderar kommunledningen årligen den övergripande riskaptiten. I det här avsnittet ges en bild av hur kommunledningens riskaptit inom informationssäkerhetsområdet ser ut för tillfället.[1]

Kommunledningsgruppen är informerad och involverad i arbetet med informationssäkerhet, och har insikter i vad som kan inträffa om kommunen inte arbetar aktivt med dessa frågor. Ledningsgruppens samlade bedömning är att händelser som leder till avbrott i det kommunen utför, händelser som leder till att IT-system/tjänster är otillgängliga, vilket i sin tur leder till avbrott/störningar i kommunens verksamheter, ska undvikas i största möjliga utsträckning.

Inte heller är ledningsgruppen villig att kompromissa med säkerheten för information vars läckande kan innebära skada på individ/individer och/eller annan organisation samt det omgivande samhället. Ledningsgruppen är också ovillig att kompromissa på säkerheten i förhållande till eventuella miljöskador.

[1] Ledning är ett begrepp vars innebörd varierar beroende på sammanhang. I vissa fall menas kommunledningsgruppen och ibland menas förvaltningsledning. När det är fråga om större ställningstaganden och vägval åsyftas den politiska ledningen.

Ledningen visar dock tendens till högre riskaptit gällande ekonomiska konsekvenser, exempelvis negativa ekonomiska påföljder likt sanktionsavgifter som en följd av informationssäkerhetsincidenter. Det är i sammanhanget viktigt att poängtera att eventuella försök att eliminera alla risker som kommunen ställs inför är förenat med extremt höga kostnader. Ledningens samlade bild är således att det finns risker som behöver tas och accepteras för att kostnader för informationssäkerhetsåtgärder inte ska skena i väg.

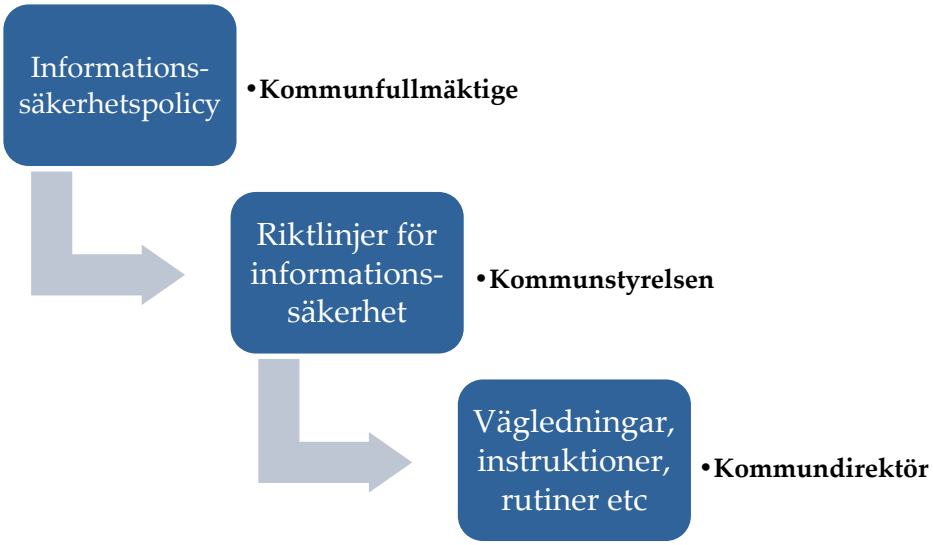
Med ovanstående i åtanke ska det här dokumentet bidra till att tydliggöra vilka säkerhetsåtgärder kommunens verksamheter förväntas införa för att undvika allvarliga negativa händelser. Dessa åtgärder vidtas för att hindra att information läcker ut, förvanskas eller förstörs och för att informationen ska vara tillgänglig när den behövs och för att säkra kvaliteten så att beslut fattas baserat på korrekt och tillförlitlig information.

1.3 Princip för ansvarsfördelning

Grundprincipen är att ansvaret för informationssäkerhetsarbetet ska följa det ordinarie verksamhetsansvaret. Det gäller från ledning till enskilda medarbetare. Det innebär att den person som har ett ansvar för ett särskilt verksamhetsområde också ansvarar för informationssäkerheten inom samma område.

1.4 Dokumentstruktur

Nedan finns en visualisering av de olika styrdokumentens struktur. Kommundirektören beslutar om vägledningar, instruktioner, rutiner etc som utvecklas och uppdateras kontinuerligt och över tid.



2 Dokumentets målgrupp

Dokumentet vänder sig till dig som är verksamhetschef eller har någon typ av formell eller informell ledarroll, exempelvis processägare, produktägare, projektledare eller utvecklingsledare. Dokumentet ska vara stöttande/vägledande för dig som ges en utförarroll i förhållande till fastställande av säkerhetsåtgärder. Dokumentet har också en tydlig koppling till ett antal olika underliggande vägledningar. Hänvisning till de vägledningarna görs i några av dokumentets avsnitt.

3 Organisering av informationssäkerhetsarbete

3.1 Allmänt om organisationen

Informationssäkerhetsarbetet i kommunen ska bedrivas med kontinuitet och systematik med utgångspunkt i standarden SS-EN ISO/IEC 27001.

Det ska finnas en central informationssäkerhetsorganisation som utgör ett samlat stöd för ledare och nyckelpersoner i förvaltningar och bolag. En central informationssäkerhetssamordnare (CISO)[2] skall samordna stödet och ansvara för ledningssystemet (LIS)[3] samt för att uppföljning av efterlevnad sker kontinuerligt.

Förvaltningar och bolag ansvarar för att säkra kompetens och resurser för implementation och löpande uppdatering i verksamheten samt för att integrera informationssäkerhetsarbetet i befintliga rutiner och processer. En lokal informationssäkerhetssamordnare (LISO) skall agera ambassadör/samordnare och det ska finnas minst en i varje förvaltning och bolag.

Utöver nedan beskrivna roller involveras vid behov befintlig specialistkompetens inom koncernen t.ex. IT-specialist, jurist, arkivarie, dataskyddsombud, upphandlare, beredskaps- och säkerhetssamordnare.

3.2 Rollbeskrivningar

Centrala roller i kommunens informationssäkerhetsarbete är CISO, LISO, IT-säkerhetsansvarig, processägare och produktägare:

[2] CISO rollen i organisationen innebär den centrala informationssäkerhetssamordnaren. Begreppet CISO är en förkortning av chief information security officer och avser den som ansvarar för informationssäkerhetsarbetet.
[3] LIS betyder Ledningssystem för informationssäkerhet.

CISO (central informationssäkerhetssamordnare) samordnar arbetet i kommunen och är stödfunktion till kommundirektör och verksamheterna.

LISO (lokal informationssäkerhetssamordnare) är ett stöd till förvaltningschef/VD och till ledningsgruppen samt har tillräckligt med tid, resurser och mandat för att samordna och kontinuerligt driva vidareutveckling av förvaltningens/bolagets informationssäkerhetsarbete.

IT-säkerhetsansvarig ansvarar för att IT-avdelning/drift efterlever krav i regelverk och avtal samt deltar i klassningar och genomför beslutade åtgärder.

Processägaren ansvarar för att processen är effektiv och ändamålsenlig. Detta inkluderar att kravställa, driva, samordna och följa upp informationssäkerhetsarbetet i processen. Det handlar om att skydda organisationens informationstillgångar med lämpliga skyddsåtgärder, tillse att information är tillgänglig när den behövs samt att upprätthålla önskad kvalitet på informationen.

Produktägaren ansvarar för att produkters/systems säkerhets- och tillgänglighetsnivå överensstämmer med verksamhetens krav och agerar som processägarens ”förlängda arm” i informationssäkerhetsarbetet.

3.3 Ansvar för tillsättning av roller och resurser

Kommundirektör utser CISO och LISO för kommunstyrelsens förvaltning.

Förvaltningschef/VD utser LISO för sin förvaltning/sitt bolag.

Kommundirektör och förvaltningschef/VD tillser att det finns processägare respektive produktägare utsedda i sina respektive verksamheter.

Kommunens centrala ledning ansvarar för att tillräckligt med resurser, kompetens och mandat finns för att bedriva riskbaserat informationssäkerhetsarbete systematiskt över tid.

Se *vägledning för informationssäkerhetsorganisation* för fördjupad beskrivning av roller och ansvarsområden.

4 Klassificering av information

4.1 Bakgrund

Informationsklassning innebär att vi värderar vår information utifrån vilka konsekvenser otillräckligt skydd skulle kunna få. Klassningen syftar till att förstå och *fastställa en adekvat skyddsnivå* av den klassade informationen samt att *öka medvetenheten om negativa konsekvenser* som kan drabba oss om tillräckligt skydd inte upprätthålls. Samtidigt som det är viktigt att informationen klassas med tillräckligt hög nivå för att skydda informationen är det även viktigt att den inte klassas obefogat högt i förhållande till sin betydelse då det kan leda till onödiga kostnader och verkningslösa åtgärder.

4.2 Krav

Organisationen ska klassa sina informationstillgångar enligt följande:

- Konfidentialitet för skydd mot obehörig insyn
- Riktighet för skydd mot oönskad förändring
- Tillgänglighet för åtkomst för behörig person vid rätt tillfälle

Klassningen ska utgå ifrån skala med nivåerna 0-3 där 0 innebär lägst skyddsbehov och 3 innebär högst skyddsbehov.

Alla nya system ska informationsklassificeras. De system som är verksamhetskritiska ska informationsklassificeras en gång per år.

Se *vägledning informationsklassificering och riskhantering*.

4.3 Säkerhetsskyddslagen

Information som omfattas av säkerhetsskyddslagen ska hanteras enligt dessa bestämmelser och annan tillämpning. Finner man vid en klassning att informationen sannolikt omfattas av säkerhetsskyddslagen får den klassificeras med nivå 4 av betydelse för Sveriges säkerhet

5 Riskhantering

Riskhantering är en central del i det systematiska informationssäkerhetsarbetet i Tjörns kommun.

Verksamheter ska bedriva ett systematiskt arbete med riskhantering. Ett systematiskt arbete innebär att kommunen har ett enhetligt arbetssätt kring att identifiera, analysera, värdera, behandla samt följa upp risker för att kommunen över tid ska kunna upprätthålla en tillräcklig nivå av

informationssäkerhet. Riskarbetet ska dokumenteras enligt instruktioner.

Se vägledning informationsklassificering och riskhantering.

6 Principer för säkerhetsåtgärder

Verksamhet ansvarar för klassificering av information inom sin verksamhet så som det beskrivs i föregående avsnitt. Informationsklassificering styr därefter vilka säkerhetsåtgärder som ska vara gällande för att informationen ska erhålla rätt skyddsnivå. En ingående beskrivning av säkerhetsåtgärder tillhandahålls av CISO.

Processägaren ansvarar för att upprätta de säkerhetsåtgärder som är gällande. Om betydande avvikelser erkänns ska de rapporteras till CISO.

7 Styrning av åtkomst

Behörigheter ska tilldelas baserat på en användares behov av information och till de produkter (molntjänster, system, databaser, operativsystem eller nätverk) som personen behöver för att utföra sina arbetsuppgifter.

Styrning av åtkomst är en grundläggande säkerhetsåtgärd för att skydda information i kommunens produkter. Det ska i varje verksamhet finnas rutiner som beskriver vem som godkänner tillträden och behörigheter till verksamhetens olika informationstillgångar, hur identifiering och autentisering av användare görs samt hur reglering av behörigheter utförs. Det senare inkluderar att underhålla och förvalta behörigheter, till exempel hantera beställning av, ändra och ta bort behörigheter så att användares roller och åtkomst till information återspeglas i behörigheterna.

8 Hanteringsregler för information

Hanteringsregler är ett begrepp som syftar till att beskriva hur anställda får handskas med information i de vanligaste typer av aktiviteter som normalt utförs under en arbetsdag. Några exempel på områden där hanteringsreglerna blir tillämpliga är hur information får kommuniceras i muntliga samtal, över telefon, i e-postmeddelanden, vad som gäller kring utskrift av information och vad som gäller kring hur information ska lagras.

Informationsklassningen, det vill säga hur skyddsvärd informationen är, bestämmer normalt vilka hanteringsregler som gäller. Kommunens vägledning för hanteringsregler av information ska följas.

9 Kontinuitetsplanering

Kontinuitetshantering innebär att det för informationstillgångar (primärt kritiska sådana) finns uppdaterade och kommunicerade planer med information om reservrutiner som ersätter befintliga arbetssätt vid avbrott och störningar. Dessa kontinuitetsplaner ska utgå från och ta hänsyn till de risker som berörda verksamheter kan urskilja. Planerna ska hjälpa kommunen att upprätta god återhämtningsförmåga och att minimera konsekvenserna vid störningar och avbrott och desamma ska revideras och testas löpande utifrån nya hot och risker. Kommunens vägledning för kontinuitetshantering ska följas.

10 Incidenthantering

Verksamhet ansvarar för att incidenter hanteras, sammanställs, dokumenteras och rapporteras enligt rutin som anvisas i vägledning. Vägledningen klarlägger bland annat rutiner för hur kommunikation med de drabbade ska ske, att det ska finnas ett systemstöd för hantering av incidenter, vilka kommunikationsvägar som är gällande samt var ansvaret ligger. Det åligger också verksamheten att se till att en extern anmälan görs i de fall det är relevant till relevanta myndigheter så som exempelvis Myndigheten för samhällsskydd och beredskap samt Integritetsskyddsmyndigheten.

11 Inköp av nya produkter/system/tjänster

Det är av största betydelse att samma arbetsprocess alltid följs när det kommer till upphandling av digitala tjänster och produkter. Kommunens vägledning för upphandling av nya tjänster/system ska användas. Vägledningen tydliggör följande:

- Upphandlingsarbetet ska organiseras enligt vägledningen och följa den process som presenteras innehållande sju steg.
- Det finns ett antal mallar framtagna. Dessa mallar ska användas i upphandlingsarbetet.

- Vägledningen pekar på standarder och strategier och dessa ska efterlevas. De utgör grundläggande krav som alltid ska finnas med i upphandlingsarbetet.
- Vägledningen tydliggör vilka informationssäkerhetskrav som kan komma att behöva tas i beaktning, och dessa krav ska tas med i upphandlingsarbetet.

12 Säkerhet i leverantörskedjan

Information behandlas på olika sätt, ofta i en mer eller mindre komplex process. Därför är det av stor betydelse att hela processen är klart identifierad, analyserad och att skyddet uppfyller säkerhetskraven i alla delar oavsett var och hur informationen behandlas. Det är av stor vikt att risker knutna till leverantörskedjan beaktas. Processägarens m.fl. ansvar för kontroll av leverantörer och underleverantörer beskrivs i vägledning för ändamålet.

13 Utbildning

Alla användare (t.ex. anställda, förtroendevalda, praktikanter, konsulter, leverantörer) ska ges möjlighet att dels stärka sin egen kunskap om säker informationshantering dels ta del av de regler och rekommendationer som gäller inom kommunkoncernen.

CISO ska initiera lämpliga övergripande kompetenshöjande insatser och ger vid behov stöd till LISO i frågor om utbildningar och information.

LISO ska initiera lämpliga kompetenshöjande insatser inom sin förvaltning/bolag.

Informationssäkerhetsorganisationen ska sträva efter att insatser och kompetensnivå ska vara möjligt att mäta och utvärdera. Det möjliggör att lättare identifiera och prioritera kommande insatser.

14 Utvärdering och uppföljning

Varje år ska kommunens LIS utvärderas utifrån principerna lämplighet, tillräcklighet och verkan. Utvärderingen inkluderar om informationssäkerheten står i samklang med organisationens övergripande mål, om nuvarande styrning är tillräcklig för hantera de risker kommunen står inför samt om planerade säkerhetsåtgärder faktiskt finns på plats och fungerar tillfredsställande. CISOs ansvar för utvärderingen beskrivs i vägledning för ändamålet.

Med stöd av korrekt utförd utvärdering av övervakning och mätning kan organisationen få bättre kunskap om informationssäkerhetsläget och upptäcka brister som behöver korrigeras. Utvärdering kan ligga till grund för interna och externa revisioner.Incidenter och avvikelser ska rapporteras enligt beslutade rutiner och statistik ska rapporteras till ledning.

Ett särskilt årshjul för informationssäkerhetsarbetet ska finnas och bör i möjligaste mån integreras i befintliga verksamhetsprocesser såsom processer för budget, årsredovisning och intern kontroll.

Ledningen har en central roll för att ett framgångsrikt systematiskt informationssäkerhetsarbete. Därför ska *Ledningens genomgång* genomföras minst en gång om året för förvaltningsledning och kommunledningsgrupp. Respektive politisk ledning avgör formerna för återrapportering av arbetet. Större beslut fattas på rätt nivå enligt delegation och andra föreskrifter.