# Policy för informationssäkerhet Tyresö kommun och dess bolag

| | | | |
|---|---|---|---|
| **Beslutsdatum** | 2021-xx-xx | **Dokumenttyp** | Policy |
| **Beslutad av** | Kommunfullmäktige | **Dokumentägare** | Chef Stöd och servicekontoret |
| **Diarienummer** | 2021/KS0073 003 | **Giltighetstid** | Tillsvidare |

tyresö kommun

# Innehållsförteckning



| | |
|---|---|
| **Senast reviderad av dokumentägaren** | [Ska inte vara ifylld om nämnden ska besluta om revidering] |
| **Reviderad med anledning av** | [Ska inte vara ifylld om nämnden ska besluta om revidering] |

# 1 Bakgrund

Tyresö kommun och dess bolag ska sträva efter ett ständigt förbättringsarbete inom alla verksamheter för att höja kvaliteten och kostnadseffektiviteten. Tyresö kommun och dess bolag är beroende av att medborgare, företag och övriga intressenter har ett starkt förtroende för verksamheten.

För att möta dessa grundläggande krav behandlar och tillgängliggör kommunen information i olika format, ofta med en stark koppling till information och data om enskilda individer. Information är därmed en av kommunens mest kritiska tillgångar och en korrekt och säker informationshantering är därför en absolut grundläggande del för kommunens anställda och de affärspartners som kommunen anlitar.

# 2 Grundläggande principer och mål för informationssäkerhetsarbetet

Kommunen är en komplex organisation med viktiga samhällsuppdrag och därför finns ett grundläggande behov av ett informationssäkerhetsarbete som bedrivs metodisk, systematiskt och dokumenterat. Informationssäkerhetsarbetet motverkar hot som kan skada kommunens verksamheter och samhällsuppdrag, negativt, påverka regionala eller nationella intressen samt skydda medborgares, anställdas och andra myndigheters och intressenters information och personuppgifter. Informationssäkerhetsarbetet ingår som en del i kommunens övergripande ”Handlingsplan för trygghet och säkerhet i Tyresö kommun” som fastställs inför varje ny mandatperiod.

Denna policy kommer att vara en del av kommunens ledningssystem för informationssäkerhet (LIS) som bygger på standarden ISO27000. Policyn avser att beskriva övergripande definitioner och ramar för kommunens informationssäkerhetsarbete. Hur policyns intentioner ska tolkas i detalj och följas beskrivs i underordnade styrdokument som ska spänna över kommunens samtliga nämnders ansvarsområden. Ledningssystemets komponenter ska följa organisationens struktur för dokumenthantering, kommunikation och förankring av information för verksamhetens medarbetare.

Informationssäkerheten omfattar all verksamhet i Tyresö kommun, dess bolag och upphandlade leverantörer/utförare utan undantag.

**Målsättningen med informationssäkerhetsarbetet är att säkerställa följande**:

**Konfidentialitet**: Att innehållet i dokument, information och handlingar etc. inte görs tillgängligt eller avslöjas för obehörig om det innehåller uppgifter som kan komma att beläggas med sekretess efter prövning.

**Riktighet**: Att upprättad information inte kan förändras vare sig av obehöriga, av misstag eller på grund av störning i tjänsten. Informationen ska vara tillförlitlig, korrekt och fullständig.

**Tillgänglighet**: Att information och informationstillgångar kan utnyttjas efter behov, i förväntad utsträckning och inom önskad tid utifrån de krav som ställs på verksamheten.

**Spårbarhet**: Att i efterhand så långt som möjligt kunna härleda specifika aktiviteter eller händelser till identifierade användare, skrivare, dator eller system/program. Det bör gå att se vilka förändringar som har hänt eller gjorts och av vem dessa har utförts.

## 2.1 Vad skall uppnås med informationssäkerhetsarbetet

För organisationen i stort betyder kontroll av kommunens informationstillgångar en möjlighet till ordning och reda i verksamheternas processer, informationshantering och dataflöden. Det ger positiva effekter i form av kontinuerlig följsamhet med lagstiftning, ökad kostnadskontroll, bättre styrning och prioriteringar i verksamheten, kortare ledtider vid förändringar, förbättrad upplevelse och förtroende till kommunens service hos medborgare och externa gränssnitt, men även ökad nöjdhet hos medarbetare.

Kommunens informationssäkerhetsarbete styrs och utgår från:

- Lagar, förordningar och föreskrifter
- Kommunens egna krav på prestanda och kvalitet
- Avtal som har koppling till informationssäkerhet

Syftet med kommunens informationssäkerhetsarbete är att säkerställa att:

- Lagar, förordningar och föreskrifter efterlevs
- Ingångna avtal är kända och följs
- Informationsförsörjningen är säker och effektiv för verksamheten
- Informationssäkerhet bibehålls även vid krissituationer
- Information klassas och hanteras med sekretess
- Organisation, rutiner, infrastruktur och systemstöd finns för skydd av känslig (verksamhetskritisk) information och data

- Medarbetare har kännedom om regler, ansvar och befogenheter samt aktivt rapporterar avvikelser
- Att kraven för informationssäkerhet integreras i organisationens verksamhetsprocesser
- Kontroll- och revisionsarbete sker löpande, samt att verksamheten åtar sig att ständigt arbeta med förbättringar inom området

## 2.2 Definition av informationssäkerhet och dess centrala begrepp

Kommunens *information* hanteras i olika format och genom olika bärare såsom pappersdokument, elektroniska (digitala) format eller vid samtal. Denna policy omfattar och gäller oavsett i vilket format uppgifterna hanteras. I takt med samhällsutvecklingen används digitala tjänster i ökande grad, vilket medför ett ökat fokus på kontroll och skydd gällande kommunens hantering av elektronisk information och data.

Med begreppet *informationssäkerhet* avses alla de åtgärder som samtliga medarbetare inom kommunen behöver vidta för att hindra att information läcker ut, förvanskas eller förstörs oavsiktligt eller genom medveten handling. Att informationen ska vara tillgänglig och korrekt när den behövs är ytterligare faktorer som ska beaktas. Inom kommunen används begreppet *informationstillgångar*. Med det avses information som har ett skyddsvärde, och analogt också ett verksamhetsvärde för kommunens uppdrag och huvudsyfte att leverera tjänster och service till kommunens invånare.

*Informationssystem* används för behandling av information och data, och är företrädesvis elektroniska men kan även avse manuell hantering (mappar och akter).

## 2.3 Dataskyddsförordningen (GDPR)

Personuppgifter är den skyddsvärda informationstillgång som är störst i kommunens verksamhet.

Behandlingen av personuppgifter regleras i dataskyddsförordningen och tillsynsmyndighet är Integritetsskyddsmyndigheten (IMY). IMY:s grundläggande principer som gäller vid personuppgiftsbehandling är bland annat;

- Följ alla de grundläggande principerna i dataskyddsförordningen
- Ha en korrekt rättslig grund för personuppgiftsbehandlingar
- Dokumentera hur arbetet är tänkt och hur det görs

- Ha ett systematiskt informationssäkerhetsarbete: struktur, rutiner och förutsägbarhet

I kommunen finns ett dataskyddsombud som ansvarar för att kontrollera följsamhet av dataskyddsförordningen inom kommunens verksamheter [1].

## 2.4 Organisatorisk omfattning och ansvar

Grundprincipen är att ansvaret för själva informationssäkerhetsarbetet ska följa det ordinarie verksamhetsansvaret. Detta gäller ända från ledning ner till enskilda medarbetare.

Denna princip innebär att den person som är ansvarig för ett visst verksamhetsområde också är ansvarig för själva informationssäkerheten inom det specifika området. En verksamhet kan bedrivas i en organisatorisk del (t.ex. förvaltning, avdelning eller enhet), ett löpande arbetsflöde (t.ex. process) eller ett tidsbegränsat arbete (t.ex. projekt).

De personer som arbetar specifikt med informationssäkerhet har en viktig stödfunktion i sin organisation – ungefär på samma sätt som de personer som har stödfunktioner inom andra verksamhetsområden, som ekonomi, personal (hr) eller kommunikation.

Dessa personer ansvarar för att själva arbetet med informationssäkerhet fungerar på ett lämpligt sätt. De ska däremot inte ha ett formellt ansvar för informationssäkerheten, utan det huvudsakliga syftet med detta ansvar och arbete är i stället att stötta ledningen, verksamhetscheferna och medarbetarna. Ansvarsområdet innebär alltså att se till så att ledning, verksamhetschefer och medarbetare i sin tur tar ansvar för informationssäkerheten i sin verksamhet.

**Nedan beskrivs kommunens roller inom arbetet med informationssäkerhet[2]**

*Kommundirektör;*
Kommundirektören har det strategiska verksamhetsansvaret för kommunens informationssäkerhetsarbete, organisation och resurser, mål, kommunövergripande styrdokument och revisionsverksamhet.

*Informationssäkerhetssamordnare (CISO)*
Informationssäkerhetssamordnarens huvudsakliga arbetsuppgifter är att leda och samordna informationssäkerhetsarbetet. Här ingår bland annat att leda och

[1] avser inte kommunala bolag, om inte något särskilt beslutats
[2] avser inte kommunala bolag, om inte något särskilt beslutats

samordna arbetet, genom att utbilda, följa upp och ta fram årliga planer för informationssäkerheten.

*Säkerhetschef*
Säkerhetschefen är rådgörande och har övergripande strategiskt ansvar för framtagandet och förvaltandet av kommunens säkerhetsramverk, i vilket informationssäkerhet ingår som en del.

*Kommunjurist och kommunarkivari*
Kommunjuristen och kommunarkivarien är rådgörande för frågor gällande bestämmelserna i tryckfrihetsförordningen, arkivlagen och offentlighets- och sekretesslagen samt förvaltningslagen.

*IT och digitaliseringschef*
Kommunens IT- och digitaliseringschef är rådgörande och har övergripande strategiskt ansvar att utifrån kommunens uppdrag, behov och gällande reglering, vidmakthålla en relevant IT organisation som har den kunskapsmässiga och tekniska förmågan att vidmakthålla och utveckla kommunens informationssystem utifrån **konfidentialitet**, **riktighet**, **tillgänglighet** och **spårbarhet**.

Alla *medarbetare*, *leverantörer* och *förtroendevalda* som hanterar kommunens information skall följa styrande dokument såsom policy, riktlinjer och rutiner för informationssäkerhet.

## 2.5 Risk- och sårbarhetsanalys

Risk- och sårbarhetsanalyser är viktiga delar av det systematiska informationssäkerhetsarbetet. Med hjälp av dessa identifieras de hot och oönskade händelser som kan leda till negativa konsekvenser för kommunen och dess invånare. En riskanalys går ut på att besvara de tre frågorna ”Vad kan hända?”, ”Hur sannolikt är det?” och ”Vad blir konsekvenserna?”. Slutligen ska det beslutas vilka åtgärder som ska införas. I detta arbete används kommunens mallar för riskhantering.

## 2.6 Informationssäkerhetsincident

En *informationssäkerhetsincident* påverkar negativt **riktigheten**, **tillgängligheten**, **konfidentialiteten** och/eller **spårbarheten** hos information som bedömts ha behov av fastställd nivå inom ett eller flera av dessa områden. Avvikelsen identifieras och hanteras utifrån den eller de regleringar som gav upphov till incidenten.

Incidenter som berör hantering och behandling av information och data inom kommunen ska rapporteras, kategoriseras och åtgärdas. Detta samlas i ett incidentregister som ska ligga till grund för risk- och sårbarhetsanalyser och kontinuerligt förbättringsarbete inom informationssäkerhetsområdet.

### 2.7 Systemförteckning och klassning

Kommunens informationssystem ska vara förtecknade och klassade. Information som hanteras i kommunen ska klassificeras med avseende på krav gällande konfidentialitet, riktighet, tillgänglighet och spårbarhet. Klassning sker vid handlingens upprättande (skapande av information) och vid handläggning av ärenden. All hantering, bearbetning och lagring av information ska motsvara kraven i dess klassning Förteckning av system och informationsklassning ska vara kopplade.

### 2.8 Kunskap och utbildning

För att upprätthålla kontinuitet och för kommunen rätt nivå i informations-säkerhetsarbetet ska samtlig personal och förtroendevalda inom Tyresö kommun och dess bolag informeras om och utbildas i relevanta styrdokument inom informationssäkerhet. Intervall för repetition ska finnas.

## 3 Uppföljning

Kommunstyrelsen ska årligen hålla sig informerad om informations-säkerhetsarbetet inom kommunen. Uppföljningen ska baseras på underlag med rekommendationer som koordineras och sammanställs av informationssäkerhetssamordnaren.

Underlaget kan innefatta bevakning och information om:

- förändringar inom eller utanför kommunen som kan påverka informationssäkerheten, t.ex. organisation och resurser, förändringar i styrdokument och processer, lagstiftning, regionala initiativ
- redovisning av policy- och regelefterlevnad samt utbildningsinsatser
- status för informationssäkerhetsmål, dataskydd (GDPR) och risk- och sårbarhetsanalys från förvaltningarna
- rekommendationer till förbättringar, revision av styrdokument och nya mål

## 4 Revidering

Revidering av detta styrdokument ska göras varje år i augusti.