Malmö stad

2022-02-16

Dokumentets namn: Malmö stads riktlinjer för informationssäkerhet	**Diarienummer:** STK-2021-1717
Typ av dokument: Riktlinje	**Version:** 1.0
Beslutad av: Kommunstyrelsen	**Datum för beslut:** 2022-XX-XX
Framtagen av: Stadskontoret	**Organisation/område**: Samtliga nämnder
Ansvarig chef: Ulf Nilsson	**Uppföljd:**
Reviderad av:	**Reviderad:**

Malmö stads riktlinjer för informationssäkerhet

Innehåll

Inledning

1.1 Bakgrund

Stora mängder information skapas och behandlas dagligen av Malmö stads medarbetare och verksamheter. Informationen finns överallt, till exempel på papper, datorer, på whiteboard- och anslagstavlor, molntjänster, verksamhetssystem och i arkiven. Bristande informationssäkerhet innebär alltid sårbarheter och inte sällan även lagbrott i vår informationshantering. I värsta fall kan både viktig och känslig information hamna i orätta händer, vilket kan bli mycket kostsamt och påverka medborgarnas förtroende för Malmö stad.

En av informationssäkerhetens största utmaningar är att informationen alltid ska ha ett tillräckligt skydd, utan att verksamheter och medarbetare upplever att implementerade säkerhetsåtgärder hindrar dem från att utföra sitt uppdrag. Genom att säkerställa att informationssäkerhet finns med som ett perspektiv i alla delar av stadens verksamheter och uppdrag kan vi tillsammans arbeta för att skydda informationen på ett tillräckligt och avvägt sätt.

1.2 Syfte och omfattning

Syftet med denna riktlinje är att på strategisk nivå fastställa ansvar, målsättning och arbetssätt för informationssäkerhet i Malmö stad och därigenom sätta ramarna för hur allt arbete med informationssäkerhet ska bedrivas. Detaljerade krav, beskrivningar och vägledning som förklarar hur stadens verksamheter ska implementera innehållet i denna riktlinje kommer att finnas i underliggande anvisningar, regler och rutiner.

Riktlinjen gäller för all hantering och alla typer av Malmö stads information. Oavsett om den behandlas manuellt eller automatiserat och oberoende av vilken form eller sammanhang informationen förekommer. Därmed ska denna riktlinje och underliggande styrdokument alltid beaktas vid framtagning och revidering av andra styrdokument som påverkar Malmö stads informationshantering.
Innehållet i riktlinjen och underliggande anvisningar, regler och rutiner baseras på standarden för informationssäkerhet SS-ISO/IEC 27000-serien. Dessa dokument bildar tillsammans stadens ledningssystem för informationssäkerhet (LIS).

1.3 Revidering och uppföljning

Riktlinjen revideras vid behov och gäller för stadens nämnder. Efterlevnaden av riktlinjen följs upp löpande och sammanställs av stadskontoret i en årlig återkoppling till stadens ledningsgrupp och kommunstyrelsen.

2. Ansvar

2.1 Ansvarsprincipen

Ansvaret för informationshantering och därmed även för informations-säkerheten följer det ordinarie verksamhetsansvaret inom nämndsorganisationen. Detta ansvar gäller från nämnd till enskild medarbetare. Den som är ansvarig för en viss verksamhet, process eller uppdrag (såsom förvaltning, avdelning, enhet, sektion, process, projekt eller enskilt uppdrag) är även ansvarig för informationssäkerheten inom sitt verksamhetsområde.

2.2 Kommunstyrelsen

Kommunstyrelsen har enligt sitt reglemente det övergripande ansvaret för stadens informationssäkerhet och beslutar om riktlinjer för informationssäkerhet.

2.3 Nämnd

Varje nämnd är ansvarig för informationssäkerheten inom sin förvaltning och ska tillse att riktlinjer och underliggande styrdokument efterlevs.

2.4 Verksamhetsansvarig

Chef (oavsett nivå) ansvarar för informationssäkerheten inom sin verksamhet. Varje chef ansvarar för att deras medarbetare efterlever riktlinjerna, har ett riskbaserat arbetssätt samt tillräcklig förståelse och kunskap för att nödvändig informationssäkerhet i verksamheten uppnås. Det inkluderar information och utbildning till medarbetare samt ekonomiskt och säkerhetsmässigt ansvar för de informationssystem där verksamhetsansvarig är systemägare.

2.5 Medarbetare

Alla medarbetare har ett eget ansvar för verksamhetens informationssäkerhet och ska i sitt eget arbete efterleva gällande styrdokument. Varje anställd har en skyldighet att rapportera informationsrelaterade brister och incidenter.

3. Målsättning

3.1 Målområden

Nedanstående målområden beskriver vad Malmö stad ska uppnå med sitt informationssäkerhetsarbete och ska alltid beaktas vid val av insatser för att höja informationssäkerheten. Respektive målområde fördjupas i efterföljande kapitel med samma namn.

3.2 Informationshantering

Ansvaret för informationssäkerheten ska vara tydlig. All information som Malmö stad äger eller på annat sätt ansvarar för ska behandlas på ett säkert och korrekt sätt. Skyddet av information ska anpassas efter dess skyddsvärde, rådande förutsättningar, hot och risker.

3.3 Medarbetare

Alla medarbetare ska ha tillräckliga kunskaper om informationssäkerhet i förhållande till sin roll och arbetsuppgifter. De ska vara säkerhetsmedvetna och ha god kännedom om de hot och risker som finns och hur de kan skydda sig mot dem. Det gäller även konsulter, leverantörer och personuppgiftsbiträden samt andra uppdragstagare som behandlar information för Malmö stads räkning.

3.4 Process

Informationssäkerhet ska vara ett integrerat perspektiv och en medveten del av verksamhetens arbetsprocesser och informationshantering. Arbetet ska bedrivas genom ett systematiskt, riskbaserat och långsiktigt perspektiv samt involvera relevanta kompetenser utifrån informationens skyddsvärde och verksamhetens behov.

3.5 Teknik

Malmö stads informationssystem ska vara robusta, funktionella och säkra med utgångspunkt i informationens skyddsvärde, riksbild och verksamhetens behov. Detta inkluderar även de informationssystem som Malmö stad köper.

4. Informationshantering

Ansvaret för informationssäkerheten följer det ordinarie verksamhetsansvaret inom nämndsorganisationen och i enlighet med nämndernas reglementen. Med information menas all information oavsett i vilken form eller sammanhang den förekommer, analog som digital. Informationens skyddsvärde beror på dess innehåll, sammanhang och syftet med dess behandling. Skyddsvärdet styr hur informationen ska behandlas. Att informationen ska behandlas utifrån rådande förutsättningar, hot och risker betyder att lagar, förordningar, interna policys, riktlinjer, anvisningar och aktuell riskbild alltid ska sammanvägas för att ge informationen ett korrekt skyddsvärde.

- För att identifiera informationens skyddsvärde ska den klassificeras och dess hantering riskbedömas.
- Information ska utifrån sitt skyddsvärde och riskbild skyddas med lämpliga organisatoriska, administrativa, fysiska och tekniska säkerhetsåtgärder utifrån perspektiven konfidentialitet, riktighet och tillgänglighet.
- Informationssäkerheten ska hålla samma nivå oberoende i vilken form och sammanhang som informationen behandlas.
- Information ska som regel endast vara tillgänglig för de personer som behöver informationen inom sitt uppdrag i syfte att kunna utföra sin arbetsuppgift.
- Vid prioritering av informationssäkerhetsåtgärder ska de informationsmängder som har högst skyddsvärde och riskbild åtgärdas först.

5. Medarbetare

Information och utbildning inom informationssäkerhet ska vara en del av anställningsprocessen likväl vid anställningens upphörande. Information och utbildning ska stå i proportion till den anställdes roll och uppdrag samt de hot och risker som kan förekomma i den anställdes informationshantering.

- Alla anställda ska erbjudas information och utbildning i informationssäkerhet. Kunskapen ska hållas aktuell och kompletteras utefter behov och inom ramen för sitt uppdrag.
- Konsulter och övriga uppdragstagare som behandlar information för Malmö stads räkning ska få anpassad information och utbildning i informationssäkerhet utifrån sitt uppdrag.
- Anställda ska vara observanta och hålla sig informerade om informationssäkerhetshot och risker samt rapportera risker och incidenter.

6. Process

6.1 Integrerat perspektiv

Riktlinjen ska tillsammans med underliggande styrdokument arbetas in i befintliga verksamhetsprocesser och rutiner av de som är ansvariga för dem. I de fall verksamhetsspecifika rutiner saknas är det upp till respektive verksamhet att utifrån identifierat behov ta fram kompletterande rutiner.

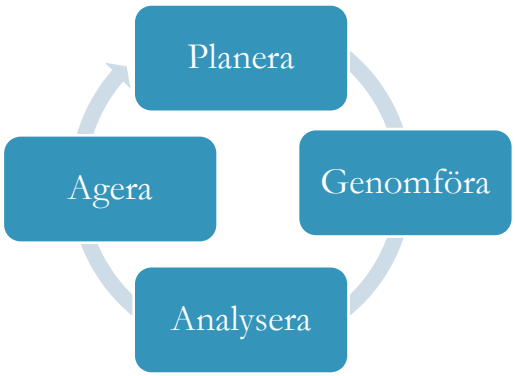
Det ska finnas möjlighet för verksamhetsansvarig chef att besluta om avsteg från denna riktlinje och underliggande styrdokument. I sådana fall ska det alltid finnas ett beslutsunderlag bestående av dokumenterad riskanalys och motivering till beslut.

6.2 Systematiskt arbetssätt

För att åstadkomma ett systematiskt, riskbaserat och långsiktigt informations-säkerhetsarbete samtidigt som kvalitén i arbetet upprätthålls ska allt arbete inom området bedrivas på följande sätt:

- **Planera:** Utifrån lagstiftning, styrdokument, informationsklassificeringar, incidenter och riskbedömningar identifiera och planera att införa säkerhetshöjande åtgärder.
- **Genomföra:** Genomföra planerade åtgärder.

- **Analysera:** Utvärdera införandet. Kontrollera att syftet med åtgärderna är uppfyllt.
- **Agera:** Ta fram förslag på nya säkerhetshöjande åtgärder.



6.3 Kommunstyrelsen

Kommunstyrelsen har i enlighet med sitt reglemente ansvar för det övergripande arbetet med informationssäkerhet och ska leda, samordna och ha uppsikt över området. Detta innebär att utifrån ett helhetsperspektiv leda och samordna stadens övergripande arbete, ta fram stadsövergripande styrdokument och processer samt följa upp att de efterlevs. Stadskontoret har därmed som styrelsens förvaltning ett centralt, stadsövergripande ansvar att sätta ramarna för hur allt arbete med informationssäkerhet i Malmö stad ska bedrivas. I detta ansvar ingår följande uppdrag;

- Förvalta och utveckla riktlinjer för informationssäkerhet
- Förvalta och utveckla stadsövergripande processer, regler och rutiner såsom informationsklassificering, riskanalys, avsteg, incidenthantering och uppföljning.
- Förvalta och utveckla systemstöd för klassificering och kravställning av Malmö stads information och informationssystem.
- Leda, utveckla och stödja stadens informationssäkerhetsnätverk.
- Utbilda och vägleda verksamheter i både stadsövergripande och verksamhetsspecifika informationssäkerhetsfrågor.
- Följa upp stadens arbete med informationssäkerhet och rapportera till resultatet till stadens ledningsgrupp och kommunstyrelsen.

6.4 Nämnder

Varje nämnd ska säkerställa att riktlinjen och underliggande styrdokument efterlevs. Varje förvaltning ska bedriva ett systematiskt, riskbaserat och långsiktigt informationssäkerhetsarbete. Efterlevnaden ska årligen följas upp och rapporteras till den egna förvaltningsledningen och nämnden.

Varje förvaltningsledning ska utse en informationssäkerhetssamordnare som ansvarar för att samordna och följa upp förvaltningens interna informationssäkerhetsarbete. Rollen ska arbeta långsiktigt och verksamhetsövergripande för att informationssäkerhet ska integreras i förvaltningens verksamheter av de som är ansvariga för dem. Samordnaren är stadskontorets motpart inom området och kommer att inkluderas i kommunens övergripande strategiska arbete. För att uppnå en god förmåga i staden ska samordnaren ges utrymme att arbeta strategiskt och tillsammans med motsvarande roller i andra förvaltningar. Inom uppdraget ska det finnas tid för innovation, omvärldsbevakning, och kunskapsutveckling. Rollen ansvarar även för att:

- Rapportera till förvaltningsledningen.
- Vara förvaltningens representant i Malmö stads interna informationssäkerhetssamordnarnätverk.
- Kunna leda och bistå med kompetens vid genomförande av informationsklassificeringar.
- Kunna leda och bistå med kompetens vid riskanalyser inom ramen för riktlinjens omfattning.

7.Teknik

Informationssäkerhetsperspektivet ska alltid beaktas vid all IT-användning under hela dess livscykel, från behov till avveckling. Identifiering av informationssäkerhetskrav ska integreras tidigt i samtliga IT-processers livscykel och finnas med kontinuerligt under alla delar av förändringshantering.

- All digital infrastruktur, Informationssystem och digitala tjänster ska ha en utpekad och dokumenterad ägare. Skyddet av informationen säkerställs av ansvarig ägare.
- Det ska finnas en beslutad och kommunicerad förvaltningsmodell för Malmö stads informationssystem.

Bilaga. Definitioner

Behandling/Hantering: En åtgärd eller kombination av åtgärder beträffande information, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring. (MSBFS:2020:6)

Incident: En oförutsedd händelse som får en oönskad effekt i form av skada för individ eller verksamhet.

Information: All information oavsett form eller sammanhang. (MSB-Publikationsnummer MSB976)

Informationsklassificering: Arbetsmetod för att säkerställa att information får en lämplig säkerhet med hänsyn till informationens skyddsvärde och riskbild. Informationens skyddsnivå säkerställs med lämpliga organisatoriska, administrativa, fysiska och tekniska säkerhetsåtgärder utifrån perspektiven konfidentialitet, riktighet och tillgänglighet. (MSB-Publikationsnummer MSB976)

Informationssystem: Samlingsnamn för alla typer av IT-system och digitala tjänster och applikationer som hanterar information. I begreppet ingår också nätverk och digital infrastruktur. (MSBFS:2020:6)

Informationssäkerhet: Bevarandet av konfidentialitet, riktighet och tillgänglighet hos information. (MSBFS:2020:6)

Informationsägare: Person som ansvarar för att informationen skyddas på avsett sätt. (MSBFS:2020:6)

Risk: Sannolikheten för att en oönskad händelse inträffar och konsekvenserna som detta i så fall skulle innebära. (MSB-Publikationsnummer MSB976)

Konfidentialitet: Att information avslöjas/röjs till obehörig

Ledningssystem för informationssäkerhet (LIS): Del av myndighetens övergripande ledningssystem. Syftar till att upprätta, införa, driva, övervaka, granska, underhålla och utveckla organisationens informationssäkerhet. (MSBFS:2020:6)

Riktighet: Att information är korrekt, aktuell och fullständig samt att den inte förändras, varken av obehörig eller av misstag.

Riskanalys: Strukturerat arbetssätt för att identifiera, bedöma och hantera hot, risker och sårbarheter.

Skyddsvärde: Informationens säkerhets- och hanteringsbehov utifrån bedömning av konfidentialitet, riktighet och tillgänglighet, gällande lagar och aktuell riskbild.

Tillgänglighet: Åtkomst till information för behörig person vid rätt tillfälle. (Terminologi informationssäkerhet, SIS-TR 50:2015)