Malin Ekblad
Säkerhetschef
malin.ekblad@trelleborg.se

Kommunstyrelsen

Riktlinje för informationssäkerhet i Trelleborgs kommun och dess bolag

Innehåll

1. Inledning

Information är en av grunderna till hur det moderna tekniksamhället fungerar. Utvecklingen visar hur beroende Trelleborgs kommun och bolagen är av information, oavsett form och kommunikationskanal, för att verksamheten ska kunna fungera. Det ställs höga krav på att vår information ska hanteras på ett korrekt och säkert sätt och att vi har spårbarhet där det behövs. Det krävs en medvetenhet om vilka hot som finns, och det krävs att det arbetas systematiskt mot dessa.

Med en ökad satsning på informationssäkerhetsarbete ska Trelleborgs kommun och dess bolag höja kvaliteten på de tekniska och fysiska informationstillgångar som finns inom kommunen och bolagen avseende sekretess, riktighet, tillgänglighet och spårbarhet. Ett ramverk för informationssäkerhet ska säkerställa att kommunen och bolagen kan upprätthålla en god kvalitet på information som hanteras inom IT-system och i fysiskt format, samt minska risken för att information hamnar i fel händer och skadar antingen kommunen eller dess invånare. Arbetet ska bygga på den framtagna standarden ISO-27000 inom informationssäkerhet som används brett inom området och rekommenderas av Myndigheten för Samhällsskydd och Beredskap (MSB).

Riktlinjerna riktar sig till samtliga medarbetare och förtroendevalda inom kommunen och dess bolag. De riktlinjer som ges ska ses som ett minimumkrav för hantering av information inom kommunen och bolagen samt ett komplement till policy för informationssäkerhet. För att kommunen och dess bolag ska ha en god informationssäkerhet krävs det ett gemensamt arbete med gemensam syn och förhållningssätt. Riktlinjerna är tänkt att fungera som ett praktiskt stöd i detta arbete.

I policy för informationssäkerhet anges följande:

Roller

Som förvaltningschef i Trelleborgs kommun eller VD för bolagen ska du:

- Ansvara för informationssäkerheten inom förvaltningen eller bolaget.
- Informera informationssäkerhetssamordnaren och IT-chef om behov av förändring inom området.

Som chef i Trelleborgs kommun och dess bolag ska du:

- Säkerställa att alla anställda är införstådda med policy och riktlinje för informationssäkerhet.
- Rapportera behov av förändringar till förvaltningschef, IT-chef, bolagschef och/eller informationssäkerhetssamordnare.

Som informationssäkerhetssamordnare i Trelleborgs kommun och dess bolag ska du:

- Ha övergripande samordningsansvar för förvaltning och utveckling av arbetet kring informationssäkerhet
- Ansvara för att det alltid finns en uppdaterad policy och riktlinje för informationssäkerhet.

Som IT-Chef i Trelleborgs kommun eller dess bolag ska du:

- Säkerhetsställa att driftsäkerheten överensstämmer med systemägarens anvisningar.
- Om fel och brister uppmärksammas som är av betydande karaktär och kan påverka säkerheten i hela IT-miljön, så har IT-chefen rätt att vidta lämpliga åtgärder för att säkerhetsställa driftsäkerheten.

Som systemägare i Trelleborgs kommun och dess bolag ska du:

- Ansvara för säkerheten i systemet.
- Ansvara för att riskanalys genomförs enligt LIS.
- Säkerhetsställa att grundläggande krav för IT-system uppfylls.

Som medarbetare i Trelleborgs kommun och dess bolag ska du:

- Följa policy och riktlinje för informationssäkerhet.

- Rapportera uppmärksammade brister i informationssäkerhetsarbetet till närmaste chef och/eller informationssäkerhetssamordnare.

Som förtroendevald i Trelleborg kommun ska du:

- Följa informationssäkerhetspolicyn och riktlinjer för informationssäkerhet.
- Rapportera uppmärksammade brister i informationssäkerhetsarbetet till nämndsordförande och/eller informationssäkerhetssamordnare.

2. Grundläggande arbete

För att policyn och riktlinjerna ska kunna efterlevas krävs det att dessa är välkända bland alla medarbetare och förtroendevalda i kommunen och dess bolag. Förtroendevalda ska i denna riktlinje hantera information på samma sätt som medarbetare. Policyn och riktlinjerna ska precis som andra beslutade policys och riktlinjer inom kommunen och bolagen, kontinuerligt förankras hos medarbetarna samt delges till nya medarbetare i samband med introduktionen. Utbildning i informationssäkerhet ska årligen ges till samtliga medarbetare under våren genom E-Learning.

3. Ledningssystem (LIS)

Kommunen och dess bolag har ett ledningssystem för informationssäkerhet som baseras på ISO/IEC 27001, *Ledningssystem för informationssäkerhet* och ISO/IEC 27005 - *Riskhantering*. Detta innebär att informationssäkerhetsarbetet sker på ett systematiskt och standardiserat sätt. Detta möjliggör fortlöpande utveckling och att verksamhetens kvalitet säkerställs. Ledningssystemet utgår från tanken planera, leda, kontrollera, följa upp, utvärdera och säkra informationssäkerhetsarbetet utifrån ett årshjul där samtliga delar genomförs årligen.

Nämnder och bolag som är egna vårdgivare ska årligen få en rapport om hur arbetet med informationssäkerhet fortlöper. Detta sammanställs och presenteras i en rapport av informationssäkerhetssamordnaren, och i de fall kommunen är vårdgivare tillsammans med ansvarig för respektive vårdenhet. Samtliga nämnder och bolag ska få en kopia av informationssäkerhetsrapporten.

3.1 Avgränsning

Riktlinjerna omfattar inte styrning avseende information som ska hanteras enligt Säkerhetsskyddslagen (2018:585).

3.2 Definitioner

Begrepp	Beskrivning
Autentisering	Verifiering av uppgiven identitet
Externa lagringsutrymmen	Portabla lagringsutrymmen (databärare) som USB-minnen och externa hårddiskar.

Hot	Möjlig, oönskad händelse med negativa konsekvenser för verksamheten.
Incident	Händelse som kan påverka säkerheten
Information	Information (data) i fysisk eller elektronisk form.
Informationssäkerhet	De åtgärder som vidtas för att förhindra att information läcker ut, förvanskas, förstörs samt att information ska vara tillgänglig när den behövs.
Ledningssystem	Arbetssätt enligt fastställd riktlinje, i denna riktlinje utifrån ISO 27000 standarden.
Logg	En datorfil som beskriver ett historiskt förlopp.
Personuppgifter	Information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.
Extra skyddsvärda personuppgifter	Personnummer, omdömen (av individ), viss ekonomisk information (känslig karaktär) och annan information som ligger nära privatlivet.
Känsliga personuppgifter	Känsliga personuppgifter är sådana som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetisk eller biometrisk information samt personuppgifter som rör hälsa eller sexualliv. Uppgifter om hälsa kan vara till exempel sjukfrånvaro, graviditet och läkarbesök. Biometriska eller genetiska uppgifter kan vara DNA eller fingeravtryck.
Risk	Sannolikheten för att något oönskat ska inträffa.
Stark autentisering	Kontroll av uppgiven identitet på flera sätt.
Systemförvaltare	Den person som ansvarar för det dagliga arbetet med drift och underhåll av ett eller flera datasystem. Rapporterar till systemägaren. Normalt en person i verksamheten som dagligen arbetar i systemet.
Systemägare	Den personen som har det överordnade ansvaret för strategi, utveckling, administration och drift av ett eller flera datorsystem. Normalt är detta en förvaltningschef eller avdelningschef, personen har budgetansvar.
Säkerhetskopiering	En kopia av information (data) för att kunna återställa information i fall den skulle förstöras eller förvanskas.

4. Klassificeringsmodell

Nedan följer kommunens klassificeringsmodell för information.

Kategori av information	Konfidentialitet	Riktighet	Tillgänglighet	Spårbarhet	Klassningsnivå
Allmän information	Information som medför endast **obetydlig/ingen** konsekvens för verksamheten och kommunen om den röjs för obehörig.	Information som medför endast **obetydlig/ingen** konsekvens för verksamheten och kommunen om den har ändrats.	Information, vars otillgänglighet endast innebär obetydlig/ingen konsekvens för verksamheten och kommunen.	Information med inga eller obetydliga krav på spårbarhet. Om spårbarhet saknas medför det endast obetydlig eller ingen negativ konsekvens för verksamheten och kommunen. medför endast obetydlig/ingen konsekvens för verksamheten och kommunen	0. Mindre viktig
Intern / verksamhetsinformation	Information som kan medföra viss **mindre allvarlig, negativ** konsekvens för verksamheten och kommunen om den röjs för obehörig.	Information som kan medföra viss **mindre allvarliga negativa** konsekvenser för verksamheten om informationen har förändrats.	Information som behöver vara tillgänglig för att inte medföra viss **mindre allvarlig negativ** konsekvens för verksamheten och kommunen.	Information med visst krav på spårbarhet. Om spårbarhet saknas medför det viss mindre allvarlig, negativ konsekvens för verksamheten och kommunen.	1. Viktig
Information med extra krav på konfidentialiet åtkomst och riktighet **Sekretessbelagda uppgifter enligt Offentlighets- och Sekretesslagen**	Information som kan medföra **allvarliga negativa** konsekvenser för verksamheten och kommunen om den röjs för obehöriga.	Information som kan medföra **allvarliga negativa** konsekvenser för verksamheten och kommunen om informationen har förändrats.	Information som behöver vara tillgänglig för att inte medföra **allvarliga, negativa** konsekvenser för verksamheten och kommunen.	Information med krav på spårbarhet. Om spårbarhet saknas medför det **allvarliga negativa** konsekvenser för verksamheten och kommunen.	2. Mycket viktig
Information med betydelse för Sveriges säkerhet **Information om totalförsvaret eller information som rörs av säkerhetsskyddslagen**	Information som röjs innebär **hot mot riket säkerhet**.	Information som kan medföra **hot mot rikets säkerhet** om den förändras.	Information som behöver vara tillgänglig för att inte medföra **hot mot rikets säkerhet**.	Information med krav på spårbarhet för att inte medföra **hot mot rikets säkerhet.**	3. Kritisk

5. Konsekvensnivåer för verksamheten och/eller kommunen

Nedan följer en förtydligande modell över vilka konsekvenser de olika klassificeringsnivåerna får för verksamheten och/eller kommunen.

Nivå	Konsekvenser för verksamhet och/eller kommunen
Nivå 0	Inga märkbara större svårigheter för verksamheten att nå målen. Ingen påverkan på samhällsviktiga funktioner vid egen eller annan organisation. Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas inte eller i försumbar omfattning av otillgänglighet till systemet/informationen. Externa individer eller andra myndigheter och organisationer kan notera störningen eller uppleva lindriga besvär men utan påvisbar ekonomisk påverkan.
Nivå 1	Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Andra myndigheter och organisationer kan påverkas (ekonomiskt eller genom behovet av att vidta extraordinära åtgärder). Samhällsviktiga funktioner vid egen eller annan organisation påverkas troligen inte. Enskilda individer kan uppleva konsekvenser, såsom besvär eller ekonomisk påverkan, av störningen. Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas i en begränsad omfattning av otillgänglighet till systemet.
Nivå 2	Skapar stora svårigheter för organisationens verksamhet. Omöjligt eller nästan omöjligt att fullfölja uppdragen. Samhällsviktiga funktioner i egen eller annan organisation påverkas sannolikt. Individers liv och hälsa äventyras. Verksamhetens förmåga att utföra sina arbetsuppgifter påverkas i en allvarlig omfattning av otillgänglighet i systemet.
Nivå 3	Ett avbrott som medför skada för Sveriges säkerhet. Systemet behandlar information som omfattas av sekretess och rör rikets säkerhet (hemliga uppgifter) där otillgänglighet kan ge oöverskådliga konsekvenser där t ex omfattande fara för liv och hälsa föreligger. Informationen omfattas av t ex säkerhetsskyddslagstiftningen eller totalförsvaret.

6. Klassificering av olika typer av information

Nedan är exempel på klassificering av olika typer av normalt förekommande information.

Klassificering av vanlig information	Klassningsnivå
Offentlig information	0. Mindre viktig

Personuppgifter	1. Viktig
Extra skyddsvärda personuppgifter	2. Mycket viktig
Känsliga personuppgifter	2. Mycket viktig
Sekretessbelagd information	2. Mycket viktig alternativt 3. Kritisk beroende på sekretessnivå.

7. Hantering av information

Samtliga system som hanterar information ska identifieras och förtecknas hos IT-avdelningen. Det är systemägarens ansvar att rapportera in detta till IT-avdelningen och varje system ska ha en systemägare. Samtliga system som har information enligt nivå 1 eller högre (modell ovan) ska göra en riskanalys enligt LIS. Om det är ett mindre system, ska mallen *Grundläggande genomgång för IT och Informationssäkerhet* användas. Med system avses allt från verksamhetssystem till molntjänster. Vid förändringar i system som kan påverka säkerheten ska rapport skickas IT-avdelningen så rätt säkerhetsnivå kan säkerställas. Information som är i fysiskt format ska hanteras utifrån skyddsnivå och arbetsplatsens instruktioner.

8. Riskanalyser enligt LIS

Det ska göras en riskanalys på samtliga system inom kommunen, bolagen som hanterar information som klassificeras som 1 eller högre. För mindre system som hanterar information som klassificeras som nivå 1 eller lägre i väldigt liten omfattning behövs endast grundläggande genomgång för IT och informationssäkerhet genomföras. Huruvida en riskanalys behöver göras på ett system eller inte bedöms i samråd med IT-avdelningen och informationssäkerhetssamordnare. Systemägaren ansvarar för att kontrollera detta.

Information om riskanalys finns i bilaga 1 och bilaga 4a, 4b samt bilagan *Informationssäkerhet vid hantering av mindre IT System LIS.*

Leverantörer av samhällsviktiga tjänster ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ISO 27000-standarden. Även leverantörer av digitala tjänster ska vidta säkerhetsåtgärder för att hantera risker och säkerställa kontinuiteten.

9. Hantering av information och lagringsutrymmen

Vilket lagringsutrymme som får användas ska spegla informationens klassificering. Information ska i första hand sparas i verksamhetssystem. Information som sparas utanför verksamhetssystem som exempelvis i dokument och e-post är innehavaren själv ansvarig för, samt att gallring och arkivering enligt gällande bestämmelser följs. Dokument i fysisk form ska förvaras på lämpligt sätt utifrån gällande lagkrav.

Förvaringen ska säkerställa att information inte förstörs, tappas bort eller röjs för obehörig.

Grundprincipen är att ett dokument som klassificeras som nivå 1 eller högre endast bör finnas på ett ställe om det inte kan motiveras att det sparas på flera lagringsytor. Externa lagringsutrymmen innehållandes information som klassas som nivå 1 eller högre kan medföra skada för Trelleborgs kommun om dessa kommer i orätta händer. Filer lagrade på externa lagringsutrymmen bör endast innehålla kopior och inte originalfiler och information som är absolut nödvändig. Originalversionen av en handling ska sparas i något av nedanstående lagringsutrymmen (se nedan lagringsmatris). Vid användning av tillfälliga lagringsytor, som USB-minnen, är det tillåtet att tillfälligt frångå principen med att en fil endast ska finnas på ett ställe. Detta för att säkerställa en god informationssäkerhet och för att kunna bedöma skada vid eventuell förlust och för att information inte ska gå förlorad.

Externa lagringsutrymmen som innehåller information som klassificeras som nivå 2 eller högre ska vara krypterade. För lägre klassificerad information rekommenderas även krypterade lagringsutrymmen. Externa lagringsutrymmen som USB-minnen ska ses som tillfälliga lagringsytor och information på dessa ska gallras eller överföras till ett annat lagringsutrymme när behovet är uppfyllt.

Användaren ansvarar för att informationen sparas på angivna lagringsutrymmen. Systemägare ansvarar för att kontrollera regelefterlevnaden på respektive system.

Gemensamma lagringsutrymmen ska alltid ha en ansvarig. Det är viktigt med behörighetsstyrning på gemensamma lagringsutrymmen, för att information inte delas med fel medarbetare.

Information som i fysisk form ska tas med utanför verksamheten ska hanteras på lämpligt sätt utifrån innehållet. Information som klassificeras som nivå 2 eller högre får endast i undantagsfall och med största försiktighet föras utanför kommunens lokaler. Endast kopior av originalhandlingen bör, i största möjliga mån, tas med utanför kommunens lokaler så inga originalhandlingar går förlorade.

Dagligen körs en central backup på alla filer som lagras på både personliga (H:\)och gemensamma (G:\) nätverksenheter. För att hålla mängden lagrade filer på nätverket på en rimlig nivå så ska medarbetaren regelbundet rensa inaktuella filer. Vid behov kan central lagringsbegränsning införas. De centrala lagringsresurserna får endast användas för lagring av arbetsrelaterad data och är dimensionerade för lagring av data- och dokumentfiler, ej för bild, ljud(mp3/wma) eller videofiler. De sistnämnda ska lagras på annan media (CD,DVD, USB-minne) eller på servrar speciellt avsedda för detta.

Vid osäkerhet ska kontakt tas med IT-avdelningen eller informationssäkerhetssamordnare.

Nedan listas vilka lagringsutrymmen och kommunikationssätt som får användas beroende på klassningsnivå:

Kategori av information	Klassningsnivå	Lagringingsutrymmen	Externa lagringsutrymmen	E-post	Fysisk form	Internpost
Allmän information	0. Mindre viktig	Eget skrivbord (dator), gemensamma diskutrymmen (G osv), Sharepoint & verksamhetssystem.	Ja.	Ja.	Inga begräsningar.	Ja
Intern / verksamhetsinformation	1. Viktig	Eget skrivbord (dator), gemensamma diskutrymmen (G osv), Sharepoint & verksamhetssystem.	Ja, krypterade lagringsutrymmen rekomenderas.	Ja.	Ja, under uppsikt eller i låsta utrymmen.	Ja
Information med extra krav på konfidentialitet åtkomst och riktighet **Sekretessbelagda uppgifter enligt Offentlighets- och Sekretesslagen**	2. Mycket viktig	Sharepoint & verksamhetssystem. Eget skrivbord eller gemensamt diskutrymme (G osv) får användas vid åtkomstbegränsning och loggkontroll.	Ja, vid krypterade lagringsutrymmen.	Vid säkerhetställning av hög säkerhet (Kryptering & i proportion med omfattningen av information).	Ja, under uppsikt eller i låst skåp i låst utrymme.	Ja, vid slutet kuvert i det bruna kuvertet
Information med betydelse för Sveriges säkerhet **Information om totalförsvaret eller information som rörs av säkerhetsskyddslagen**	3. Kritisk	Lagringsytor ska beslutas i samråd med IT-avdelningen och säkerhetsavdelningen.	Lagringsytor ska beslutas i samråd med IT-avdelningen och säkerhetsavdelningen.	Nej.	Lagringsytor ska beslutas i samråd med säkerhetsenheten.	Nej

Vid osäkerhet om en lagringsyta uppfyller ovanstående ska kontakt tas med IT-avdelningen eller med informationssäkerhetssamordnaren.

Övriga lagringsytor ska genomgå en riskanalys innan beslut kan tas huruvida dessa utrymmen får användas eller inte. Det material som tas fram genom medarbetarens tjänsteutövning är kommunens information. Information som klassificeras som nivå 1 eller högre får inte sparas på externa molnlagringsytor som exempelvis iCloud, Dropbox och/eller Hotmail om dessa inte genomgått en riskanalys och det finns av förvaltningen godkänt avtal för lagring på dessa ytor.

9.1. Säkerhet- och Informationssäkerhetsincidenter

Vid inrapportering av;

- Säkerhetsincidenter
- Säkerhetsincidenter för NIS
- Personuppgiftsincidenter

ska detta rapporteras till MSB eller Integritetsskyddsmyndigheten (IMY). Se mer information i bilaga 3 a för säkerhetsincidenter samt på Intranätet om personuppgiftsincidenter.

10. Skyddsåtgärder och hantering av utrustning samt hemarbete

Nivån på skyddet gällande den fysiska miljön och system ska stå i proportion till informationsklassningen och riskanalyserna. Utrustningen ska skyddas mot skada, stöld, förlust eller skadlig påverkan. Vitala system och vitala delar i IT-miljö, nätverk och tillhörande infrastruktur ska regelbundet kontrolleras av IT-

avdelningen så att driftsäkerheten kan upprätthållas. Endast datorprogram eller applikationer som behövs för medarbetarens arbete får installeras på utrustningen.

Utrustning såsom datorer, telefoner, surfplattor och liknande räknas som arbetsredskap och användningen av dessa ska som huvudregel vara arbetsrelaterad. Medarbetaren har ansvar att efter eget gott omdöme använda sig av utrustningen på ett ändamålsenligt sätt så att risken för obehörig tillgång, stöld eller förlust minimeras.

Platstjänster och kontroll vart enheter befinner sig ska som regel vara avstängda.

Ingen åtkomst till lagrade kontakter i telefonen får ges till nerladdade applikationer eller liknande.

Information får inte synkroniseras med aktörer som inte har avtal med Trelleborgs kommun. Detta innebär att det inte är möjligt att synkronisera information från telefonen till privata konton. IT-avdelningen kan inte hjälpa till med support mot aktörer som kommunen inte har avtal med eller support av information till privata konton.

10.1. Hantering av utrustning

Endast sådan utrustning som tillhandahållits eller kontrollerats av kommunen får anslutas till kommunens IT-miljö. Detta omfattar exempelvis USB-minnen, externa hårddiskar, TV-apparater, routrar, switchar och hubbar. Dessa får inte kopplas in i kommunens nätverk utan IT-avdelningens godkännande. Om fel och brister av betydande karaktär, och som kan påverka säkerheten i IT-miljön, uppmärksammas har IT-chefen rätt att vidta lämpliga åtgärder för att säkerställa driftsäkerheten. Detta ska så fall rapporteras till förvaltningschef & systemägare. Utrustning och kommunikationsförbindelser ska tillhandahållas av Trelleborgs kommun. Privat utrustning får inte användas för information som klassificeras som nivå 1 eller högre. Stöldbegärlig bärbar utrustning ska vara stöldskyddsmärkt.

För mer information se bilaga 5 om Informationssäkerhet och GDPR vid hemarbete.

11. Delning av skärm, delat skrivbord och fjärrstyrning samt digitala möten

Vid föredrag och likande när medarbetaren kopplat in sin dator på projektor eller liknande är det viktigt att stänga av samtliga andra program och applikationer så att ingen information delas felaktigt. Exempelvis vid inkommande e-post avisering.

Vid användning av funktionen ”dela skrivbord” eller fjärrstyrning är det viktigt att tänka på att de som skrivbordet delas med/fjärrstyr ser allt som finns på medarbetarens skrivbord och samtliga ytterligare program eller applikationer ska vara avstängda.

12. Digitala möten

Säkerheten vid digitala möten måste tillgodose skyddsbehovet som följer av riskerna med behandlingen. Det är viktigt att endast de som är behöriga får tillgång till systemet, vilket kräver att organisationen tar såväl tekniska, som organisatoriska åtgärder för att skydda dessa. Skyddsnivån när det gäller sekretessärenden och integritetskänsliga personuppgifter över lag bör vara på den högre skalan. Ju mer integritetskänsliga uppgifter, desto högre säkerhetsnivå.

De rättsliga krav som ställs på oss som kommun återfinns bl a i Dataskyddsförordningen, som ställer krav på säkerhet vid en personuppgiftsbehandling - särskilt när det är extra skyddsvärda och känsliga personuppgifter.

Som ”personuppgiftsbehandling” räknas all typ av information som kan kopplas till en enskild, även ljud och bild om enskilda kan identifieras. Offentlighets- och sekretesslagen ställer dessutom krav på att sekretessuppgifter inte får röjas för obehöriga.

Se mer i bilaga 6.

13. Medarbetare och säkerhet

För att säkerställa korrekt hantering av informationstillgångar ska lämpliga säkerhetsåtgärder vidtas för att minimera felaktig hantering, stöld, bedrägeri och missbruk av informationstillgångar.

Både vid nyanställning och för befintliga medarbetare ska lämpliga säkerhetskontroller genomföras, utifrån vilken information personen ska få tillgång till. Extern medarbetare som får tillgång till kommunens information ska även omfattas av lämpliga säkerhetskontroller och åtgärder (exempelvis utdrag från belastningsregistret, sekretessavtal & personuppgiftsbiträdesavtal). Krav är att alltid kontrollera ID vid anställning och anlitande av extern medarbetare. För medarbetare som avslutar sin anställning, ändrar tjänst eller för förtroendevalda som avslutar sitt uppdrag ska det säkerställas att dennes behörigheter för samtliga system och lokaler upphör/ändras i samband med att tjänsten/uppdraget avslutas/förändras. Medarbetaren och den förtroendevalda ska vid avslut återlämna all utrustning som kommunen tillhandahållit. Medarbetaren och den förtroendevalda ansvarar själv för rensning/gallring, diarieföring samt arkivering av de handlingar i fysisk och digital form som ligger under dennes ansvar. Samtliga ärende ska innan avslut/förändring vara avslutade eller överlämnade till annan medarbetare samt behörigheter ska vara förändrade eller borttagna. Ansvarig chef säkerhetsställer att detta sker.

Samtliga utrymmen med information som klassificeras som nivå 1 eller högre ska vara skalskyddade och ha lämpliga säkerhetsåtgärder mot brand, stöld och obehörig åtkomst. Endast behörig medarbetare får vistas i lokalerna. Besökare, reparatörer och annan extern personal ska normalt inte befinna sig i lokalen utan någon ansvarig medarbetare. I de fall extern personal tagit del av gällande bestämmelser kan de efter beslut av närmaste chef få röra sig i lokalerna själva för att kunna utföra sitt uppdrag. Passerkort, taggar och annan personlig legitimering

får ej lånas ut. Vid förlust ska detta skyndsamt inrapporteras till närmsta chef och ansvarig.

14. Telefon och muntlig information

Utlämnande av information till andra myndigheter, företag eller privatpersoner, som inte är allmän, får endast ske efter identifiering av mottagaren. Detta kan ske antingen genom motringning (mot växel), tidigare verifierat telefonnummer eller efter validering genom exempelvis tre kontrollfrågor som personen själv endast kan antas känna till. Det behöver även säkerställas att mottagaren är behörig att ta del av informationen. Det är den som förmedlar informationen som ansvarar för att säkerställa att mottagaren är den avsedda och att lämpliga åtgärder vidtas för att inte fel personer kan höra eller avlyssna samtalet.

Om samtal ska spelas in ska medarbetaren informera/informeras i förhand och gällande lagstiftningar ska följas.

15. Fysisk säkerhet serverrum, lokaler och utrustning

Lämpliga skyddsåtgärder ska vidtas för att förhindra obehörigt tillträde eller störningar/skador på lokaler, utrustning och information. Det sker bland annat genom passerkontrollssystem, inbrottslarm, övervakning och systematiskt brandskyddsarbete. Kritiska funktioner för verksamheten ska prioriteras och driftsäkerhet ska säkerställas genom redundans. Servrar och kommunikationsutrustning placeras i avsedda utrymmen. Lokalisationen av dessa bör inte kommuniceras ut till obehöriga. Utrustning (såsom datorer, telefoner eller smarta kort) ska förvaras under uppsikt eller i låst utrymme. Vid förlust av utrustning ska detta utan dröjsmål anmälas till närmaste chef, IT-avdelningen och vid behov spärras hos leverantör. Det är den som blivit utsatt för stölden som är ansvarig för att polisanmälan sker.

16. Post och internpost

Inkommande post ska hanteras enligt gällande rutiner. Vid extra behov att skydda informationen och säkerställa att den når mottagaren ska brev skickas som rekommenderat brev.

Avsedda kuvert (bruna) ska användas för internpost. Fullständigt namn och avdelning ska anges när internpost skickas. Kontrollera båda sidorna av det bruna kuvertet. Endast avsedd mottagare eller av förvaltningen utsedd person (vid längre frånvaro) får öppna posten. Är internposten adresserad till avdelning så får utsedd person från avdelningen öppna posten för att delegera ärendet vidare.

För information som klassas som nivå 2 ska intern posten läggas i slutet kuvert först och sedan i de avsedda kuverten för internpost. För information som klassas som nivå 3 ska kontakt tas med säkerhetsenheten för bedömning kring hur informationen ska kommuniceras.

17. Skrivare

Vid utskrift av information ansvarar medarbetaren som beställt utskriften för att säkerställa att samtliga papper skrivits ut. Funktionen säker utskrift ska användas. Säker utskrift innebär att medarbetaren behöver registrera sin TAG för att utskrift ska kunna ske.

18. Arkiv och gallring

Information ska gallras eller arkiveras i enlighet med förvaltningens, bolagens dokumenthanteringsplan. En rutinbeskrivning finns särskilt framtagen för gallring och bevarande av e-postmeddelanden.

19. E-post

Varje förvaltning och bolag ansvarar för att allmänna handlingarna som skapas i verksamheten hanteras enligt gällande regelverk. Handlingar som kommer in eller expedieras via e-post är som huvudregel allmänna handlingar och hanteras efter samma principer som handlingar som kommer in eller expedieras på annat sätt. Detta oberoende av om e-post tas emot eller skickas via en tjänstemans, en förtroendevalds eller en förvaltnings funktionsbrevlåda (e-post).

Information som klassificerats som nivå 0 eller 1 får skickas via kommunens e-postsystem. Information som klassificerats som 2 får lov att skickas om lämpliga säkerhetsåtgärder vidtagits beroende på skyddsvärdet och omfattningen. Information som klassificerats som 3 får inte skickas via e-post.

Information med klassificering 1 eller högre får ej skickas med privat e-post.

Bifogade filer i e-post meddelande ska endast öppnas om de kommer från en känd avsändare och en bilaga är att förvänta. E-post som kan misstänkas innehålla infekterade filer ska anmälas till IT-avdelningen. Endast kända länkar ska klickas på i meddelandet. Se riktlinjer kring personuppgifter i e-post för ytterligare vägledning kring hur e-posten får hanteras.

Kommunens och bolagens e-post får inte användas för registrering av icke arbetsrelaterade tjänster. Tjänste-e-posten får endast användas i begränsad omfattning för privata meddelande. I de fall privata bruk förekommer ska dessa sparas i en mapp märkt privat. Information och material som är pornografiskt, diskriminerande eller har anknytning till kriminell verksamhet är inte tillåtet.

Kalender i e-posten ska inte innehålla någon information som klassas som 2 eller högre.

20. Internet

Användande av internet är en naturlig del i arbetet som bedrivs inom kommunen, bolagen. Detta ska användas med gott omdöme. Privat användning av internet är tillåtet i sådan omfattning att de inte inkräktar på arbetet, medför risker/lagöverträdelser, sker i strid mot gällande policys eller generar extra kostnader för kommunen.

Samtliga medarbetare ska vara medvetna om att besök på hemsidor lämnar elektroniska spår efter sig. Detta innebär att andra kan registrera vilka hemsidor som kommunens medarbetare besöker. Medarbetarens användning av internet loggas.

Finns det misstanke om skadlig kod eller något annat som kan påverka säkerheten ska IT-avdelningen kontaktas. Hemsidor innehållandes material som är pornografiskt, diskriminerande eller har anknytning till kriminell verksamhet är inte tillåtet. Undantag kan tillåtas om det kan bedömas relevant för tjänsten, detta ska ske i samråd med närmsta chef. Nerladdning och/eller lagring av programvaror för privat bruk är inte tillåtet. Uppföljning av internetanvändandet kan förekomma.

21. Sociala medier

Sociala medier är ett verktyg som får hantera information som klassas enligt nivå 1 eller lägre, förutsatt att befintlig lagstiftning följs gällande exempelvis personuppgifter. Övrig information som klassas som nivå 2 eller högre får inte publiceras på sociala medier.

22. IT-säkerhet

IT-avdelningen ansvarar och arbetar för den övergripande IT-säkerheten för kommunen och bolagen genom aktivt arbete mot skadlig kod och kontinuerliga säkerhetsuppdateringar. Kommunens och bolagens nätverk ska skyddas utifrån verksamhetens krav. Respektive systemägare ansvarar för säkerheten i sitt system.

Medarbetaren rekommenderas att inte använda publika nätverk. Medarbetaren får använda sitt privata nätverk. Besökare får ansluta sin utrustning till kommunens, bolagens Wifi gästnätverk.

Roaming innebär att vandra från en operatörs nät till en annans . Detta sker automatisk när du åker över en landsgräns. Det ska vara uppdragstyrt från ansvarig chef huruvida en medarbetare ska använda sin telefon utomlands och utnyttja roaming.

Endast kända enheter får anslutas via Bluetooth. Om ingen Bluetooth enhet används ska denna funktion vara avstängd.

23. IT-utrustning och tredjeland

Portabel utrustning som har åtkomst till kommunens e-post eller IT-system får endast användas i tredjeland (Länder utanför EU/ESS) vid behov (utifrån medarbetarens tjänst) och efter samråd med närmaste chef. Användning av utrustning enligt ovan ska det ske med stor försiktighet i tredjeland. Vid användning av utrustning i utanför kommunens miljö ska överföring ske via kommunens, bolagens VPN-tunnel. Medarbetaren bör undvika att använda publika nätverk på flygplatser, hotell, restauranger och liknande. Vid osäkerhet ska kontakt

tas med IT-avdelningen eller kommunens Dataskyddsombud för rådgivning om hanteringen är förenlig med gällande lagstiftning.

24. Behörigheter, åtkomst och loggkontroll

All åtkomst till information inom kommunen, bolagen ska styras med hjälp av organisatoriska och tekniska skyddsåtgärder i form av bland annat åtkomstadministration, åtkomstkontroll samt loggning och logguppföljning. Detta för att säkerställa att endast behöriga får tillgång till IT-system och informationen i dem, samt kunna spåra eventuellt missbruk av information. Den som är inloggad i ett system ansvarar för vem som får ta del av informationen kopplat till inloggningen.

Systemägaren ansvarar för att personerna som finns i systemet har rätt behörighet. Behörigheter ska alltid vara personliga för system som hanterar information som klassificeras som nivå 1 eller högre. Systemadministratörer/tekniker ska alltid ha individuella behörigheter. Om det inte är möjligt ska manuell logg föras över vem som använt ett gruppkonto. Åtkomst med utvidgade rättigheter, så kallade administratörsrättigheter, ska begränsas till så få personer som möjligt utan att drift och underhåll av systemet riskeras.

Vid behörighetstilldelning ska behörighet och åtkomst ges utifrån den arbetsuppgift medarbetaren ska utföra i systemet. Medarbetaren ska endast ha tillgång till sådana uppgifter som den har behov av för att sköta sitt arbete. Även om en medarbetare har teknisk möjlighet att få tillgång till en viss information får medarbetaren endast söka och ta del av information om det är motiverat för att den ska kunna utföra sina arbetsuppgifter. Vid bedömning av vilka uppgifter en medarbetare ska ha åtkomst till ska särskild hänsyn tas till om uppgifterna är sekretessbelagda uppgifter eller känsliga personuppgifter. Det ska finnas användarrutiner för medarbetaren där det framgår vad de får och inte får lov att göra i ett system. Vid förändring eller avslut av tjänst ska behörigheten anpassas eller tas bort.

Information om vad som sker på en medarbetares dator lagras centralt och lokalt i utrustningen, så kallade systemloggning. Systemloggning är till för driftövervakning, felsökning och uppföljning av att gällande lagar och policys följs samt för att identifiera IT-incidenter och hot (exempelvis skadlig kod och intrångsförsök) mot kommunens utrustning, system eller information.

Systemägaren ska säkerställa att kontinuerlig uppföljning av loggar och behörigheter görs utifrån behov och lagkrav.

I de fall medarbetaren har tillgång till mycket data, alternativt tillgång till känsliga uppgifter, bör det minst kvartalsvis göras en slumpmässig loggkontroll av användarna och vad de har gjort. Minst en gång om året ska användarbehörigheter gås igenom.

25. Drift och systemförvaltning

För att upprätthålla säker och tillförlitlig tillgång till information ska varje IT-system ha fastställda och dokumenterade rutiner för administration, drift och underhåll.

Leverantörens säkerhetsuppdateringar ska installeras skyndsamt.

26. Säkerhetskopiering

Säkerhetskopiering av information och programvara ska utföras regelbundet. Frekvensen och omfattningen ska bero på vilken typ av information IT-systemet innehåller samt vilka regler och lagar som systemet omfattas av. Innan ett system ska tas i drift ska säkerhetskopieringen vara fastställd och dokumenterad. Tester för att återskapa information från säkerhetskopior ska genomföras regelbundet utifrån behov.

27. Lösenord och autentisering

Åtkomst till information, klassificerat som nivå 1 eller högre, ska endast ges om användaren är behörig och autentiserad. Lösenord ska uppfylla kommunens, bolagens lösenordspolicy som är enligt följande:

- Minst 12 tecken långt.
- Inte samma som de senaste 30 lösenorden.
- Inte återanvända samma lösenord inom 1 år.
- Bytas minst var 90:e dag.
- Innehålla versaler och specialtecken.

Lösenord och annan utrustning som används för autentisering (exempelvis smarta kort, ID) är personliga och får inte lånas eller lämnas ut. Medarbetaren ansvarar för att lösenord och andra känsliga användaruppgifter inte blir kända för andra. Om lösenord eller motsvarande har exponerats för annan ansvarar medarbetaren för att byta lösenordet utan dröjsmål.

Autentiseringen av användaren ska spegla skyddsvärdet som bedöms vid riskanalysen. System som har information som klassificeras som nivå 2 eller högre bör ha stark autentisering. För viss typ av information är det lagkrav med stark autentisering, det är därför av största vikt att identifiera eventuella lagkrav utifrån informationen i systemet. Detta identifieras under riskanalysen. Lösenord som används ska överensstämma med kommunens lösenordspolicy.

Bärbar utrustning som telefoner och surfplattor som har tillgång till information som klassificeras som nivå 1 eller högre ska alltid ha pinkod. Det är systemägarens ansvar att det finns rutin som säkerställer ovanstående i respektive system. Detta ska ske utifrån behov och gällande lagstiftningar. Arbetsuppgiften att utföra ovanstående kan delegeras av en systemägare till en systemansvarig. Ansvaret för bärbar utrustning är respektive innehavare.

För att förhindra obehörig åtkomst till IT-system och information som lagras på enheten ska utrustning aldrig lämnas i inloggat läge utan uppsikt. När medarbetare lämnar utrustningen ska den låsas eller stängas av. Smarta kort eller liknande får de inte lämnas kvar i datorn, utan ska förvaras under uppsikt eller i låst utrymme. Förlust av smarta kort ska utan dröjsmål förlustanmälas till närmaste chef eller annan utsedd medarbetare.

28. Personuppgifter och Skyddad identitet

Personuppgifter ska hanteras enligt gällande regler i Dataskyddsförordningen och annan svensk lagstiftning. Detta innebär att personuppgifter endast får samlas in och behandlas för berättigade ändamål, det ska finnas en rättslig grund för behandlingen och mängden personuppgifter som behandlas ska begränsas till vad som är nödvändigt för ändamålet. Uppgifterna får inte sparas längre än nödvändigt (utifrån dokumenthanteringsplanen) eller behandlas på ett oförenligt sätt med ändamålet för vilket de samlades in. Personuppgifter behöver skyddas på ett lämpligt sätt tekniskt, fysiskt och organisatoriskt. Detta ska ske i enlighet med dataförordningens (GDPR) grundprinciper P*rivacy by design* och *Privacy by default*, vilka innebär att så lite personuppgifter ska samlas in som möjligt utifrån ändamålet och standardinställningen för ett system ska vara integritetsskyddande. Vill medarbetaren få ytterligare funktionalitet i ett system (som inte är nödvändigt) ska detta vara ett aktivt val från medarbetaren.

Samtliga behandlingar som sker inom kommunen, bolagen ska registreras i kommunens, bolagens registerförteckning Draftit. Detta sker genom kontakt med förvaltningens, bolagets GDPR-samordnare.

Uppgifter kring personer med skyddad identitet ska hanteras med största försiktighet inom organisationen. Dessa behöver ha lämpligt skydd, innehålla så lite information som möjligt samt vara behörighetsstyrt. Detta ska ske med stöd av Skatteverkets vägledning för hantering sekretessmarkerade personuppgifter i offentlig förvaltning. Denna finns på:
https://www.skatteverket.se/privat/folkbokforing/skyddadepersonuppgifter/hanteringavsekretessmarkeradepersonuppgifter.4.18e1b10334ebe8bc80002541.html

29. Säkerhet- och Informationssäkerhetsincidenter

Säkerhetsincidenter som kan påverka informationssäkerheten ska utan dröjsmål rapporteras till närmaste chef som tar ärendet vidare med berörda parter samt IT-avdelningen och informationssäkerhetssamordnare. Detta gäller även misstänkta säkerhetsincidenter. Nödvändiga åtgärder ska vidtas skyndsamt. Vid osäkerhet ska kontakt tas med informationssäkerhetssamordnaren.

Informations- och IT-säkerhetsincidenter för samhällsviktiga tjänster beträffande NIS-direktivet ska rapporteras samt fyllas i och sändas i enlighet med anvisning. Kontaktuppgifter och konton skapas per nämnd och behöver aktualiseras inom nämnden till att säkerställa kravet.

Vid personuppgiftsincidenter ska dessa rapporteras till förvaltningens eller bolagets GDPR-samordnare enligt separat rutin för personuppgiftsincident.

30. Avveckling av utrustning, information och system

Vid avveckling av IT-utrustning som innehåller information så ska informationen överföras till verksamhetssystem för bevarande alternativt gallras i enlighet med förvaltningens dokumenthanteringsplan. Lagringsmedia ska förstöras alternativt återanvändas på lämpligt sätt. Det ska säkerställas att den information som lagrats inte kan läsas eller återskapas av obehöriga. Detta ska ske av eller i samråd med IT-avdelningen.

Dokument i fysisk form ska i första hand hanteras i enlighet med förvaltningens dokumenthanteringsplan. Information som klassificerats som nivå 1 eller högre ska, om den inte ska diarieföras eller arkiveras, förstöras på sätt som säkerställer att de inte går att återskapas. Detta sker genom att informationen körs i en dokumentförstörare, vars innehåll töms och destrueras på ett säkert sätt, alternativt läggs i avsedda upphandlade kärl för sekretessavfall. Avveckling av system ska ske med god planering där analys görs hur det påverkar andra system, säkerställas att ingen information förloras samt att alla avtal sägs upp.

31. Kontroll och efterlevnad av policy samt riktlinjer för informationssäkerhet

Om misstanke finns att utrustning eller information har hanterats felaktigt har kommunen, bolagen rätt att gå genom loggar med mera för att kontrollera efterlevnad av lagstiftning och regler. Otillåten hantering kan leda till disciplinära åtgärder, och alla misstänkta brott polisanmäls. Uppmärksammade felaktigheter kommer rapporteras till ansvarig chef.

32. Kontinuitet och avbrottsplanering

Informationssäkerhet ska vara en integrerad del av den överordnade processen för verksamhetens kontinuitetsplanering enligt kommunens policy för kontinuitet.

Processen ska behandla nödvändiga informationssäkerhetskrav som behövs för verksamheten i kontinuitet.

I verksamhetens kontinuitetsplan bedöms kritiska beroenden samt bedömningen sker hur verksamheten ska bedrivas vid avsaknad av kritiska funktioner, informationstillgångar och IT-system samt hur återgång till normalläge ska ske.

33. Lagar och förordningar:

Informationssäkerhetsarbetet ska säkerställa att kommunens och bolagens hantering av information uppfyller säkerhetskraven utifrån gällande lagstiftningar. Vanligt förekommande lagstiftningar inom den kommunala verksamheten är:

- Arkivlagen (1990:782)
- Arkivförordningen (1991:446)
- Bokföringslagen (1999:1078)
- Dataskyddsförordningen (2016/679)
- Förvaltningslagen (2017:900)
- Kommunallagen (2017:725)
- Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning
- Lag (1997:614) om kommunal redovisning
- Offentlighets- och sekretesslagen (2009:400)
- Patientdatalagen (2008:355)
- Socialtjänstlagen (2001:453)
- Säkerhetsskyddslagen (2018:658)
- Särskild myndighetslagstiftning
- Upphovsrättslagen (1960:729)

34. Dokumenthistorik

34.1. Versioner

Version	Datum	Beskrivning	Ändrat av
0.1	2019-04-08	Första utkast	JD
0.2	2019-07-18	Ändringar efter remiss hos förvaltningar	JD
0.3	2021-02-11	Uppdatering	PS

Bilagor till riktlinjer kring informationssäkerhet

Bilaga 1 - Information om riskanalys för informationssäkerhet

Bilaga 2 - Formulär för intern säkerhetsincidentrapportering

Bilaga 3 a - Formulär för riskanalys (LIS) av mindre IT System
Bilaga 3 b – Formulär för IT-säkerhetsincident

Bilaga 4 a – NIS-direktivet
Bilaga 4 b – NIS-direktivet riskanalys för informationssäkerhet

Bilaga 5 – Informationssäkerhet och GDPR vid hemarbete

Bilaga 6 – Digitala möten