MORA KOMMUN

RIKTLINJER INFORMATIONSSÄKERHET OCH DATASKYDD

Dokumentbeskrivningar

Strategi
En strategi anger på vilket sätt, vilka åtgärder eller metoder , kommunen ska uppnå specifika mål.

Policy
En policy ska ange viljeinriktningen för ett specifikt område. Den ska vara vägledande för beslut och styrning. En policy som är av principiell beskaffenhet eller av större vikt ska beslutas av kommunfullmäktige och i övrigt av kommunstyrelsen. En policy gäller tills vidare och bör därför revideras vart fjärde år och följa mandatperioden.

Program och planer
Ett program anger långsiktiga avsikter i en fråga av större vikt. Ett program är mer beskrivande än en policy och mer övergripande än en plan. Om program ska gälla för hela kommunen ska den antas av kommunfullmäktige.

En plan eller handlingsplan innehåller åtgärder som ska vidtas inom ett särskilt område och syftar till att förverkliga exempelvis mål, policy, lagar mm. En handlingsplan är mer konkret och specifik än en plan och innehåller exempelvis ansvar. De bör revideras vart fjärde år och följa mandatperioden

Föreskrifter
Regeringen har i förordningar gett kommunerna rätt att utfärda lokala föreskrifter med mer detaljerade bestämmelser än i förordning.

Riktlinjer och rutinbeskrivningar
En riktlinje innehåller anvisningar om hur en fråga ska hanteras. Den är vägledande i hur tjänstemän bör agera.

Reglemente
Kommunfullmäktige beslutar hur kommunen ska organiseras och vilka nämnder som skall finnas och hur de skall vara sammansatta. Det är obligatoriskt för kommunfullmäktige att utfärda reglementen för nämnderna. Reglementen är ett regelverk om nämndernas arbetsformer och har till uppgift dels att klargöra befogenhetsfördelningen mellan de olika nämnderna. Kommunfullmäktige beslutar också om sitt eget reglemente s.k. arbetsordning samt revisionens.

Bolagsordning och ägardirektiv
För de kommunala bolagen motsvaras reglementena av bolagsordning och ägardirektiv. Dessa kommunala aktiebolag ska följa såväl aktiebolagslagen som delar av kommunallagen.

Regler och stadgar
Ett äldre begrepp för riktlinjer är stadgar, vilka antas av fullmäktige. Stadgar används mest i formen av regler för hur en förening eller stiftelse ska arbeta.

Taxor och avgifter
Kommunen har så kallad avgiftsmakt det vill säga befogenhet att ta ut avgifter av enskilda som ersättning antigen för kommunala prestationer eller för rätten att nyttja allmänna platser och inrättningar. Avgift som är privaträttsliga och är grundade på frivilliga avtal kallas avgifter. Avgifter som är offentligrättsliga det vill säga påtvingad prestation med stöd av bestämmelser i en allmän författning kallas taxor. Taxor och avgifter beslutas av fullmäktige.

Arvoden och andra kommunala stöd
Fullmäktige får besluta att förtroendevalda i skälig omfattning får ersättning för sitt uppdrag och därtill uppkomna omkostnader.

Kommunen har möjlighet att ge olika stöd exempelvis till föreningar.

Riktlinjer för informationssäkerhet och dataskydd

Fastställd	Kommunstyrelsen 2021-05-04 § 89
Reviderad	-
Produktion	Kommunledningskontoret
Dnr	2021/00033 003

Innehållsförteckning

Inledning

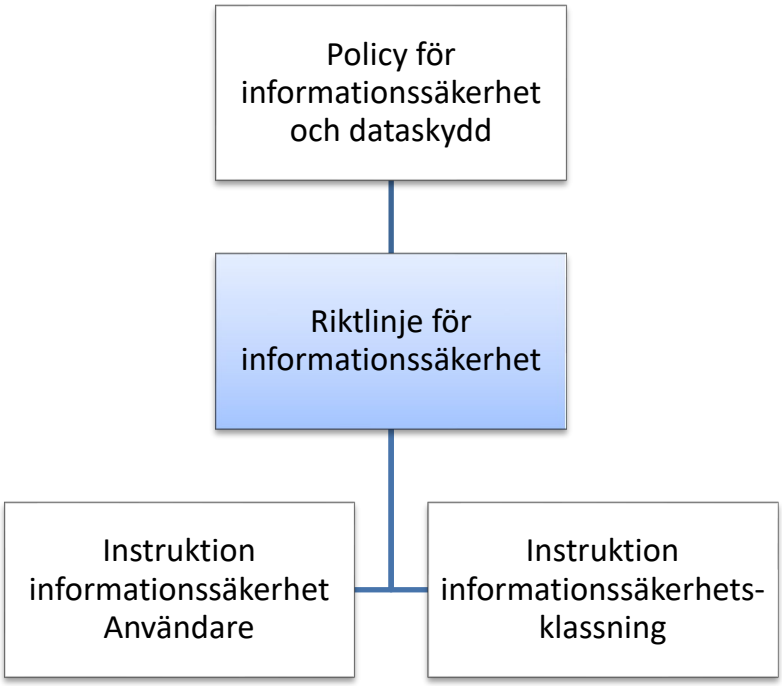
Riktlinjens roll

De här riktlinjerna syftar till att konkretisera styrdokumentet *Policy för informationssäkerhet och dataskydd* och ska ge verksamheterna och användarna vägledning i hur policyn ska tillämpas. Den är en del av de beslutade dokument som reglerar informationssäkerhetsrelaterade aktiviteter i organisationen och ingår därmed i kommunens ledningssystem för informationssäkerhet - LIS.

Målet för kommunernas informationssäkerhetsarbete är att systematiskt arbeta med att skydda verksamhetens information anpassat efter skyddsvärde, risk, kostnad och lagkrav.

Det övergripande målet är formulerat i den centrala policyn som redovisar kommunledningens viljeinriktning. Policyn följs av tillämpningsanvisningar som de här riktlinjerna men även instruktioner med övergripande regler och därutöver kan detaljerade rutiner som rör specifika säkerhetsåtgärder i olika verksamheter behövas.

Riktlinjerna följer den internationella standarden ISO/IEC 27002 - Informations- och säkerhetsteknik inom informationssäkerhet, kompletterat med ISO/IEC27701 - Krav och vägledning för säkerhetstekniker vid hantering av personuppgifter och beskriver hur verksamheterna ska agera för att initiera, bibehålla och förbättra informationssäkerheten i kommunen. Den ska ses som ett minimikrav vid utveckling eller anskaffning av nya system och e-tjänster och även som mål för redan driftsatta sådana.



Omfattning

Dessa riktlinjer gäller för all verksamhet inom kommunkoncernen och omfattar alla informationstillgångar som hanteras.

Alla användare - anställda, extern personal, förtroendevalda - som hanterar information i verksamheten omfattas av policyn och dess tillhörande riktlinjer och instruktioner.

Med informationstillgång avses all information och resurser som hanterar den, som är av värde för organisationen. Exempel på informationstillgång är:

- information (databas, metodik, dokument)
- program (applikation, operativsystem)
- tjänster (kommunikationstjänst, abonnemang, internetförsörjning)
- fysiska tillgångar (dator, datamedier, lokala nätverk)
- människor och deras kompetens, färdigheter och erfarenheter
- immateriella tillgångar (rykte, framtoning, profil).

Vad är informationssäkerhet?

Informationssäkerhet handlar om att skapa och upprätthålla lämpligt skydd för att motsvara de krav som finns på att hantera information på ett säkert sätt.

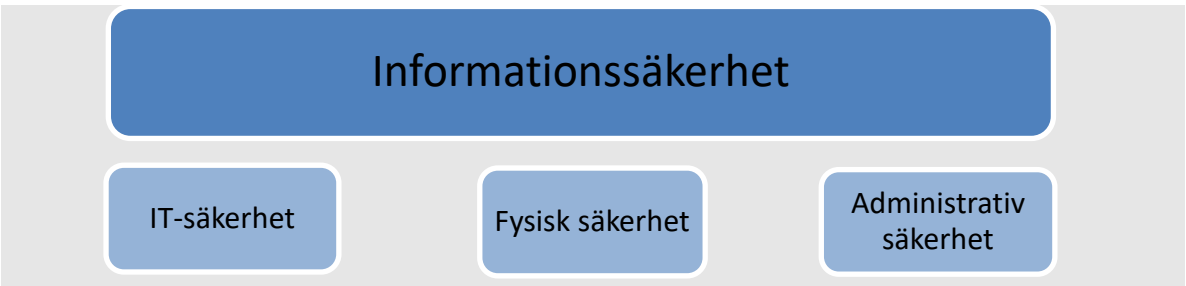
Viss information är känslig och måste skyddas från obehöriga att ta del av. Det handlar ofta om hänsyn till den personliga integriteten och för att undvika att enskilda individer kommer till skada men även annan konfidentiell information. Det finns många lagar och föreskrifter som kommunen måste leva upp till och därtill förväntar sig privatpersoner, företag och andra att kommunen hanterar information säkert.

Informationssäkerhet omfattar skydd av all information oavsett form och innebär en strävan att skydda information så att:

- endast behöriga personer får ta del av informationen (konfidentialitet),
- informationen går att lita på, att den är korrekt och inte manipulerad (riktighet),
- informationen finns tillgänglig när den behövs (tillgänglighet) samt
- att hanteringen av informationen i väsentliga delar är spårbar (spårbarhet).

Informationssäkerhet delas upp i:

- IT-säkerhet - skydd för digital information när man behandlar, överför och lagrar den.
- Fysisk säkerhet - åtkomst till informationstillgångar, passersystem, lås, inbrotts- och brandlarm.
- Administrativ säkerhet - riktlinjer, styrning, organisation, regler och rutiner.



Brister i informationssäkerhet kan leda till risk för liv och hälsa, hot mot den personliga integriteten eller leda till negativ ekonomisk påverkan och att förtroendet för organisationen skadas.

Sammantaget finns stora krav på informationssäkerhet och därför är systematik och en fast styrning nödvändig för att upprätthålla säkerhet och kvalitet.

Informationssäkerhetsklassning är ett grundläggande och återkommande begrepp inom området där informationsägare ansvarar för att värdera en informationstillgång i aspekterna *konfidentialitet*, *riktighet* och *tillgänglighet* för att kunna bestämma vilka skyddskrav man har.

Det finns en särskild instruktion för informationssäkerhetsklassning.

Kraven som ställs rör ofta säkerhet för IT-komponenter som bär informationen. Detaljer om IT-säkerhet finns i en särskild riktlinje för IT-säkerhet framtagen av IT-enheten och fastställd av kommunstyrelsen.

Begrepp och definitioner

Delvis från Teknisk rapport SIS-TR 50:2015, Terminologi för informationssäkerhet, framtagen av SIS tekniska kommitté för informationssäkerhetsstandarder, med syfte att finna lämpliga svenska uttryck för vanliga begrepp inom området.

Begrepp	Definition
Administrativ säkerhet	Säkerhetsåtgärder i verksamheten som styr informationssäkerhetsarbetet, formellt och informellt.
Användare	Individ eller system som nyttjar informationstillgångar. Förtroendevalda, anställda och extern personal som till exempel inhyrda konsulter.
Autentisering	Den tekniska processen vari äktheten, autenticiteten bekräftas. Äkthet avseende uppgivna uppgifter; att någon är den de utger sig för att vara, särskilt rörande påstådd identitet och meddelandens ursprung och innehåll. Kan vara en person eller IT-komponent.
Behörighet	Tilldelad rättighet att använda informationstillgång på ett specificerat sätt.
BKS	Behörighetskontrollsystem –tekniska och administrativa säkerhetsfunktioner som kontrollerar och registrerar användares aktiviteter.
Dataskydd	Begrepp som används för att ange skydd för den personliga integriteten i de regelverk som ska tillämpas vid behandling av personuppgifter.
Fysisk säkerhet	Tekniska säkerhetsåtgärder relaterade till skydd av person, lokal och utrustning av betydelse för informationssäkerhet.
Information	Alla former, såväl digital som analog och muntlig information.
Informationsbehandlingsresurs	System, tjänst eller infrastruktur för hantering av information.
Informationssystem	Applikationer, tjänster eller andra komponenter som hanterar information med hjälp av IT för att stödja individer, grupper, organisationer eller samhällen.
Informationssäkerhet	En uppsättning av säkerhetsåtgärder som syftar till bevarande av egenskaper som konfidentialitet, riktighet och tillgänglighet hos information, men även spårbarhet, autenticitet och ansvarsskyldighet. Omfattar administrativ och teknisk säkerhet (fysisk och IT-säkerhet).
Informationssäkerhetsklassning	Metod för att värdera och prioritera information genom konsekvensanalys för att identifiera skyddsbehovet för en viss information efter krav på konfidentialitet, riktighet och tillgänglighet. Olika nivåer anger olika skyddskrav.
Informationstillgång	Information, och resurser som hanterar den, som är av värde för en organisation.

Informationsägare	Person som har ansvar för information som skapas och hanteras i verksamheten, således *riskägare* för informationen som ska hanteras. Ett IT-system kan ha flera informationsägare.
IT-system	Se informationssystem.
IT-säkerhet	IT-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet. Omfattar datasäkerhet och kommunikationssäkerhet.
Konfidentialitet	Skydd mot obehörig insyn.
Konsekvensbedömning	Process för att beskriva en personuppgifts-behandling och för att hantera risker för den enskilde individen, enligt artikel 35 i dataskyddsförordningen (GDPR).
Ledningssystem för informationssäkerhet, LIS	Del av organisationens övergripande ledningssystem, baserad på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet. Omfattar organisationsstruktur, styrdokument, planerade aktiviteter, ansvar, praxis, rutiner, processer och resurser.
Objektstyrning	En modell för styrning av objekt. Objekten består av verksamhetskomponenter (t ex processer, rutiner, manualer) och IT-komponenter (t ex IT-system). Det handlar om att stärka samverkan mellan verksamhet och IT för att åstadkomma rätt stöd till verksamheten. Gemensamma mål sätts upp och prioriteras. Objekten hanterar vidmakthållande, vidareutveckling, nyutveckling och avveckling. För mer information om modellen läses dokumentet *Grunderna i Styrmodell för objekt* och för mer information kopplat till IT-säkerhet läses dokumentet *Riktlinjer IT-säkerhet*.
Redundans	Tillstånd då mer än ett medel finns för att upprätthålla ett givet funktionssätt i syfte till att säkerställa kontinuerlig drift.
Riskanalys	Process för att förstå en risks natur och avgöra sannolikhet för negativa händelser och dess konsekvenser.
Riktighet	Skydd mot oönskad förändring.
Spårbarhet	Entydig härledning av utförda aktiviteter till en identifierad användare.
Teknisk säkerhet	Säkerhetsåtgärder för att upprätthålla informationens konfidentialitet, riktighet och tillgänglighet. Omfattar områdena IT-säkerhet och fysisk säkerhet.
Tillgänglighet	Att information är åtkomlig och användbar för behörig person vid rätt tillfälle.
Åtkomsträttighet	Användares behörigheter uttrycks i tilldelade åtkomsträttigheter som definierar vad en användare har rätt att utföra, t ex läsa, söka, skriva, radera, skapa, exekvera.

Organisation, ansvar, roller

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret.

Den politiska ledningen i form av kommunfullmäktige har det yttersta ansvaret för kommunens informationssäkerhet genom att ha antagit en kommunövergripande policy.

Kommunstyrelsen fastställer de övergripande riktlinjerna.

Nämnder och bolagsstyrelser har ansvar för informationssäkerheten inom deras verksamhetsområden och ska tydligt visa ledarskap i frågan, ha en uppdaterad lägesbild över identifierade risker avseende informationshantering och tilldela tillräckliga resurser för informationssäkerhetsarbetet.

Kommundirektör/VD ansvarar för att informationssäkerhetsarbetet bedrivs enligt styrdokumenten och beslutar om de övergripande instruktionerna som rör informationssäkerhet.

Verksamhetsansvarig ansvarar för att all informationshantering inom egna verksamheten sker i enlighet med lagar och fastställda styrdokument. Denne ansvarar för att informationstillgångarna i verksamheten är identifierade och samlade i en förteckning, med utsedda ägare som ansvarar för att vidta nödvändiga skyddsåtgärder. Vidare ansvarar den verksamhetsansvarige för att fatta beslut om inriktning och resurser och säkerställer att det finns rätt kompetens i den egna organisationen. Ansvaret för att alla i verksamheten som hanterar information har ett säkerhetsmedvetande och tillräcklig kunskap för att informationssäkerhet kan uppnås åligger även det den verksamhetsansvarige.

Informationsägare ansvarar för informationstillgångarna och är därmed riskägare. Informationsägaren ansvarar för att informationssäkerhetsklassning av tillgångar sker och beslutar om skyddsnivån utifrån klassningsvärdet samt ansvarar för att kravställa leverantör av tjänst/drift. I objektstyrningsmodellen motsvarar det ofta en objektägare men i de fall där objektägaren inte är informationsägare, till exempel i ett diariesystem eller inom personaladministration, så är informationsägaren kravställare på objektägaren, vad gäller informationssäkerhet. Särskild beskrivning av objektstyrning och organisation finns i dokumenten *Grunderna i Styrmodell för objekt* och *Riktlinjer IT-säkerhet*.

Samverkan informationsägare – objektägare:

Informationsägare	**Objektägare**
Ägarskapet gäller *informationen*. Informationsägaren ansvarar för att informationen hanteras utifrån interna regelverk och externa krav som lagstiftning. Det sker bland annat genom informations-säkerhetsklassificering och riskanalyser. Beslut som fattas för en informationstillgång gäller för alla som hanterar informationen.	Ägarskapet gäller *systemet/objektet/IT-komponenten*. Objektägare/objektägare IT ansvarar för drift och säkerhet av IT-komponenten och kan utifrån informationsägarens krav ansvara för att systemet utformas så att informationen skyddas på ett adekvat sätt.

Användare har en del i ansvaret för säkerheten i informationshanteringen och ansvarar för att följa de styrdokument som finns. De ansvarar även för att vara uppmärksam på brister och incidenter rörande informationssäkerhet och att rapportera dessa till närmsta chef, IT-enhetens Service Desk eller till informationssäkerhetssamordnaren.

Informationssäkerhetssamordnaren är en stödfunktion i organisationen ungefär som andra stödfunktioner inom andra verksamhetsområden som ekonomi-, personal- och kommunikationsfunktioner. Samordnaren arbetar i samråd med utsedda inom administrativ säkerhet, fysisk säkerhet och IT-säkerhet, dataskyddsombud samt verksamhetsrepresentanter. Ansvarsområdet för informationssäkerhetssamordnaren är att ge stöd till ledning, verksamhetschefer och medarbetare så att de kan ta ansvar för informationssäkerheten i sin verksamhet. Informationssäkerhetssamordnaren ska kontrollera och följa upp

informationssäkerheten internt och ansvarar för att förvalta och utveckla ledningssystemet för informationssäkerhet (LIS).

Säkerhetssamordnaren i kommunen är ett stöd till förvaltningar och bolag i risk- och säkerhetsfrågor rörande det fysiska skyddet inom informationssäkerhet och inom risk- och sårbarhetsanalyser.

IT-säkerhetsansvarig utses av IT-enheten och ansvarar för att kravställa, stödja och kontrollera arbetet med att nå och upprätthålla rätt nivåer av IT-säkerhet enligt riktlinjen för IT-säkerhet, där detaljer i rollen beskrivs.

Personuppgiftsansvariga är nämnder och styrelser i organisationen. De ansvarar för att all behandling av personuppgifter inom sitt verksamhetsområde sker i enlighet med gällande dataskyddslagstiftning. Respektive nämnd/styrelse ska fastställa sin roll som personuppgifts-ansvarig (inklusive gemensamt personuppgiftsansvar) och/eller personuppgiftsbiträde.

Dataskyddsombud ska utses av nämnd/styrelse och har som uppgift att övervaka och rapportera om efterlevnaden av gällande dataskyddslagstiftning samt ge råd och vägledning i dataskyddsfrågor. Är även en kontaktperson för de registrerade och för tillsynsmyndigheten.

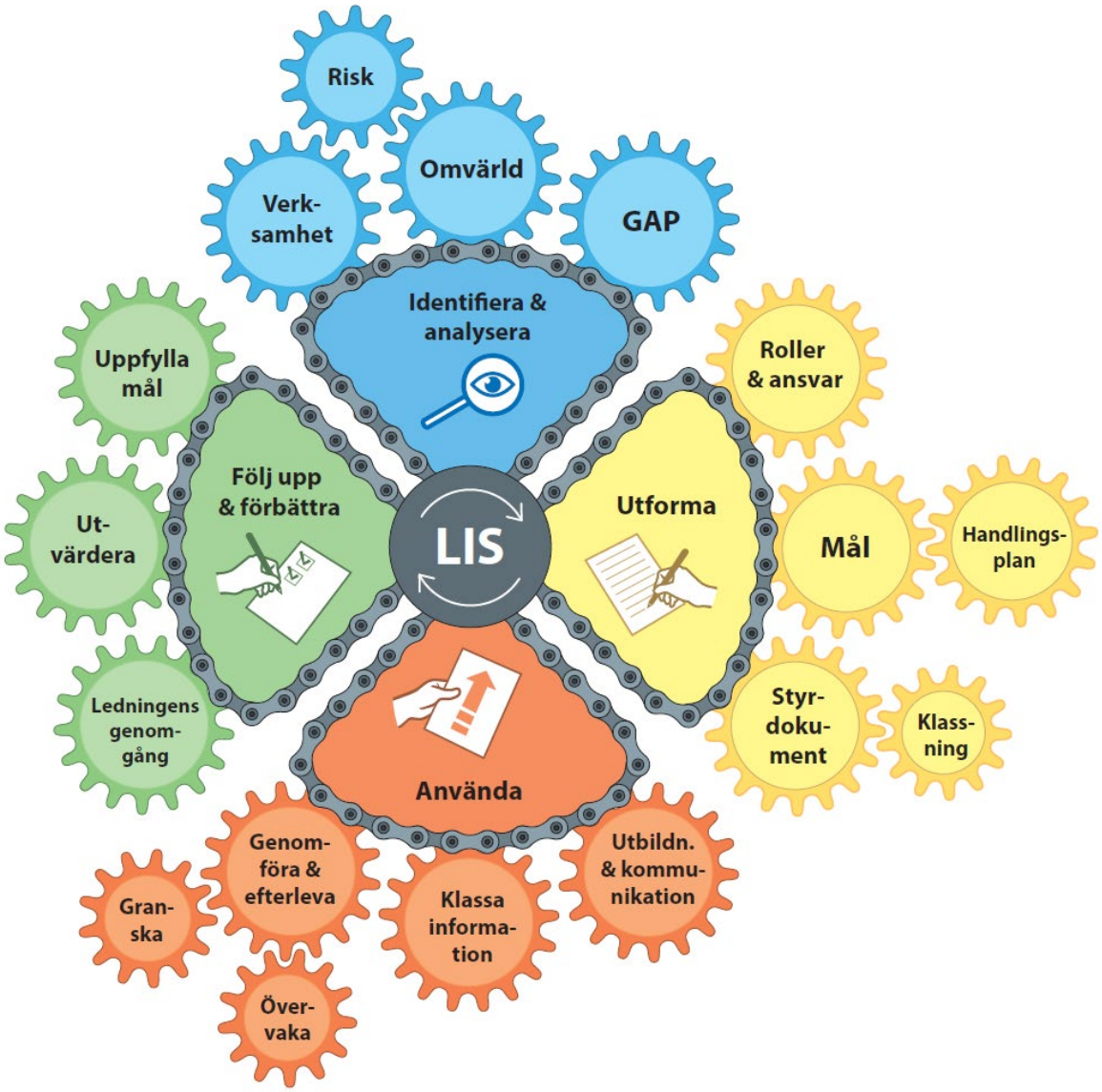
Dataskyddskontaktperson finns i verksamheterna och är kontaktpunkt både för registrerade och för medarbetare. Personen behöver vara insatt i de personuppgiftsbehandlingar som nämnd/styrelse ansvarar för och hålla registret för behandlingarna uppdaterat, enligt artikel 30 i dataskyddsförordningen. Personen behöver delta i frågor som gäller personuppgiftsbehandlingar i verksamheten, och t ex medverka vid konsekvensbedömningar enligt artikel 35. Dataskydds-kontaktpersonen är en första kontakt vid personuppgiftsincidenter enligt gällande rutin.

Projektägare ansvarar för att informationssäkerhetsfrågor beaktas i projekt. Tidigt i projekt ska en juridisk och informationssäkerhetsmässig analys och bedömning göras för att kunna identifiera lagkrav och nödvändiga säkerhetsåtgärder. Informationssäkerhetsmål ska ingå i projektets mål.

Att arbeta systematiskt

I policyn för informationssäkerhet och dataskydd framgår att alla nivåer ska bedriva ett aktivt och systematiskt informationssäkerhetsarbete så att rätt information finns tillgänglig för rätt personer vid rätt tidpunkt. Informationstillgångar behöver skyddas utifrån sitt skyddsvärde och information ska inte hamna i orätta händer och missbrukas.

Myndigheten för samhällsskydd och beredskap (MSB) erbjuder ett metodstöd med underliggande metoddelar som kommunen använder sig av. Det är ett hjälpmedel för att kunna planera och följa upp informationssäkerhetsarbetet och ska leda till ständiga anpassningar och förbättringar för att skydda information på önskad nivå till rätt kostnad med en tydlig styrning.



Metodstödet hjälper till med att implementera ett systematiskt informationssäkerhetsarbete enligt den etablerade internationella standardserien ISO 27000.
Det hjälper organisationen att upprätta, införa, underhålla och ständigt förbättra sitt LIS enligt ISO 27001. Ett LIS är ett begrepp för ett systematiskt arbete med informationssäkerhet och innefattar allt från styrande dokument till metodik. Den här riktlinjen är en del av ett LIS och innehåller regler enligt ISO 27002, ISO 27701 och enligt MSB:s rekommendationer.

Personalsäkerhet

Mål: Att säkerställa att anställda, förtroendevalda och leverantörer förstår och uppfyller sitt ansvar och är lämpliga för de roller de är tilltänkta för.

Före anställning/uppdrag

Verifiering av personers identitet ska göras och bekräftelse av akademiska och yrkesmässiga kvalifikationer ska inhämtas.

Vissa roller kräver en bakgrundskontroll före anställning/uppdrag. Det ska finnas en rutin där det framgår vem som är kvalificerad att utföra kontrollen samt när och hur verifieringsåtgärder utförs. Om en förändring av arbetsuppgifter eller uppdrag medför att personen får tillgång till informationstillgångar som är konfidentiella ska kontroll också utföras. Ansvar för kontroll av leverantörer behöver anges i avtal.

Under anställning/uppdrag

Anställda, förtroendevalda och leverantörer ska följa informationssäkerhetskraven i fastställda styrdokument. Avsiktliga överträdelser medför disciplinära åtgärder.

I informationsägarens ansvar ingår att se till att alla

- är tillräckligt informerade om sina roller och ansvar innan åtkomst ges till konfidentiella informationstillgångar
- omfattas av en förbindelse om konfidentialitet när personuppgifter och konfidentiell information hanteras
- har lämpliga kunskaper för att hantera informationen
- uppmuntras att rapportera informationssäkerhetsbrister
- motiveras att upprätthålla en god informationssäkerhetskultur.

I *Informationssäkerhetsinstruktion för användare* finns regler för distansarbete, mobila enheter och lösenord bland annat. Chefer har ett ansvar att delge allmän information och utbildning i informationssäkerhet och dataskydd till alla användare.

Vid underlåtenhet att följa riktlinjer för informationssäkerhet och underliggande instruktioner följer kommunen regler enligt lagar och avtal. Lagbrott polisanmäls.

Efter anställning

Anställda, förtroendevalda och leverantörer ska få tydlig kommunikation om vilket ansvar rörande informationssäkerhet de omfattas av efter avslut eller ändring av anställning.

Hantering av informationstillgångar

Ansvar för tillgångar

Mål: Organisationens tillgångar ska identifieras och ett ägarskap med tillhörande ansvar för att skydda dem ska fastställas.

Verksamhetsansvarig ansvarar för att informationstillgångar identifieras och att en förteckning över tillgångarna upprättas och underhålls. Alla tillgångar ska tilldelas ägare när de skapas eller när de överförs till organisationen.

Regler för tillåten användning av information ska identifieras, dokumenteras och införas för informationens hela livscykel; skapande, bearbetning, lagring, överföring, radering och destruktion. Tillgångens ägare ansvarar för att:

- tillgångar är inventerade
- tillgångar klassas och skyddas
- behörigheter definieras och periodvis granskas
- korrekt hantering när tillgången raderas eller destrueras säkerställs.

Tillgångar ska återlämnas till organisationen när anställning, uppdrag eller avtal upphör.

Informationssäkerhetsklassning

Mål: Information ska ha en lämplig skyddsnivå beroende på dess betydelse.

Informationstillgångar ska ha ett relevant skydd. Känsliga och kritiska informationstillgångar kräver ett högre skydd och särskilda hanteringsregler än mindre kritiska. För att kunna applicera rätt skydd ska tillgången informationssäkerhetsklassas för egenskaperna konfidentialitet, riktighet och tillgänglighet. Informationsägare ansvarar för att klassificering utförs enligt kommunens modell, som är SKR:s verktyg KLASSA.

Exempelfrågor för att bilda sig en uppfattning om de olika kraven: Vilka konsekvenser kan det bli för individen, för verksamheten, för ekonomin och för samhället om informationen

- kommer i orätta händer? ***Konfidentialitet***
- inte stämmer? ***Riktighet***
- inte kan nås, på kort och längre sikt? ***Tillgänglighet***

Och ***Spårbarheten*** – hur viktigt är det att det går att se vem som gjort vad?

Klassningen ska ge en tydlig bild av hur den bör hanteras och skyddas för de som arbetar med informationen.

Klassningen ska utföras tidigt i projekt så att rätt krav kan ställas på både interna och externa leverantörer.

IT-system och infrastruktur ska ha minst motsvarande klassning som informationen komponenterna bär.

En särskild instruktion för informationssäkerhetsklassning finns.

Styrning av åtkomst

Mål: Regler för styrning av åtkomst ska upprättas, dokumenteras och vara föremål för uppföljning utifrån verksamhets- och informationssäkerhetskrav för att begränsa åtkomst till informationstillgångar.

All tillgång till information ska styras med hjälp av administrativa och tekniska skyddsåtgärder så att endast behöriga får tillgång till informationen. Det ska finnas regler och rutiner för användare hur informationstillgångar får hanteras, baserat på informationens skyddskrav. Reglerna ska baseras på förutsättningen att allt generellt är förbjudet om det inte uttryckligen tillåts, snarare än regeln att allt är tillåtet om det inte uttryckligen förbjuds.

Informationsägaren beslutar om vilka säkerhetsåtgärder som krävs, baserat på genomförd informationssäkerhetsklassning och riskbedömning. Styrkan på användarautentiseringen ska motsvara klassningsnivån som informationen har. Ju mer skyddsvärd information desto mer detaljrika och stränga säkerhetsåtgärder krävs. Integritetskänsliga personuppgifter till exempel, ställer krav på en högre säkerhetsnivå och på god IT-säkerhet, vilket innebär säkrare inloggning, stark autentisering och en tydlig behörighetsstyrning.

Det samlade systemet för styrning benämns behörighetskontrollsystem (BKS) och beskrivs närmare i riktlinjer för IT-säkerhet.

Säkra inloggningsrutiner

Tillgång till system och applikationer behöver styras med säkra inloggningsrutiner så att så lite som möjligt avslöjas vid inloggning. Inga hjälpmeddelanden bör finnas, som skulle kunna hjälpa en obehörig användare. En bra åtkomstrutin bör innehålla:

- ett allmänt meddelande att datorn bara får användas av behöriga användare
- loggning av misslyckade inloggningsförsök och lyckade inloggningar
- att systemet inte avslöjar vilken del av informationen som var fel, vid misslyckat försök
- skydd mot ”Brute Force”-inloggningsförsök (brute force är en metod för att pröva alla möjliga kombinationer av lösenord och nycklar)
- att lösenord inte visas i klartext eller överförs i klartext över nätverket
- automatiskt avslut av sessioner efter en definierad tidsperiod av inaktivitet, särskilt på offentliga platser eller utanför organisationens säkerhetshantering och på mobila enheter
- att skärmar på datorer och mobila enheter låses automatiskt efter en definierad tids inaktivitet
- begränsad uppkopplingstid för högriskapplikationer med åtkomst till konfidentiell information.

Behörigheter ska godkännas formellt vid begäran om åtkomst.

Behörigheter ska baseras på aktuella arbetsuppgifter och organisatorisk tillhörighet.

Användarnas åtkomsträttigheter behöver granskas regelbundet av ägaren av tillgången. Tillstånd för privilegierad åtkomst bör ses över oftare.

Vid administrativa åtkomsträttigheter ska funktion för privilegiehöjning användas när det finns, till exempel att växla till administratör tillfälligt för en viss arbetsuppgift och sedan växla tillbaka till sitt vanliga användarkonto.

Användares identitet ska vara spårbar till en fysisk person. I vissa fall behöver loggning och uppföljning genomföras för att säkerställa rätt användning av behörigheter.

Lösenord är alltid konfidentiella och ska skyddas från alla andra än ägaren. Rutiner ska finnas som säkerställer att lösenord skyddas från till exempel administratör oavsett om lösenord tilldelas, förändras eller återställs.

Exempel på identifiering och autentisering finns i riktlinje för IT-säkerhet.

Process för att hantera användarkonton

Användarkonton är unika och användare hålls ansvariga för sina handlingar. Användning av delade konton ska endast tillåtas om de anses vara nödvändiga för verksamhet eller av operativa skäl och ska då vara godkänt och dokumenterat enligt rutinen för dispens från informationssäkerhetshöjande åtgärder, som återfinns i *Informationssäkerhetsinstruktion för användare*.

Konton som inte är aktuella längre ska inaktiveras – inte tas bort. Det blir då lättare att följa loggar och risken att samma kontonamn används vid ett senare tillfälle minimeras.

Rutin för att säkerställa rätt behörighetsnivå vid anställning, vid förändring av arbetsuppgifter eller roll och vid upphörande av anställning ska finnas. För användare som lämnat organisationen ska användarkonto genast avslutas/inaktiveras.

Rutin för att identifiera och inaktivera överflödiga konton ska finnas.

Rutin för att inaktivera konton som inte använts under en viss tid ska finnas.

Rutin för att inte dubbla konton utfärdas ska finnas.

För externa användare ska tilldelning av åtkomst vara tidsbegränsad.

Kryptering

Mål: att säkerställa korrekt och verkningsfull användning av kryptering för att skydda informationens konfidentialitet, äkthet och riktighet.

IT-enheten tillhandahåller vid behov godkända krypteringslösningar och instruktioner hur de ska användas. Krypteringslösningar beskrivs i riktlinje för IT-säkerhet.

En strategi för nyckelhantering, inklusive metoder för att hantera skyddet av kryptografiska nycklar och återvinning av krypterad information om nycklar förloras, äventyras eller skadas bör finnas.

Regler för användning, skydd och giltighetstid för kryptografiska nycklar för hela livscykeln – generering, lagring, arkivering, hämtning, distribution, återkallande och destruering bör finnas.

Principen för kryptering ska ta hänsyn till regelverk, nationella restriktioner och frågor avseende gränsöverskridande flöde av krypterad information.

Fysisk och miljörelaterad säkerhet

Mål: att förhindra otillåten fysisk åtkomst till, skador på och störningar i tillgången till information.

Informationssäkerhetsklassningen ger ett stöd för att utforma det fysiska skyddet, utifrån vilken information som hanteras och hur skyddsvärda tillgångarna är.

Säkerhetsåtgärder bör vidtas för att minimera risken för potentiella fysiska och miljömässiga hot som stöld, brand, vatten, elförsörjningsproblem, damm, vibrationer, kemiska skador, elektromagnetisk strålning och vandalism.

Fastighetsägaren ska bedriva underhåll enligt policy och regelverk. Ansvarig för kontroll är ansvarig verksamhet i samråd med kommunens säkerhetssamordnare.

Säkra utrymmen

Om en informationstillgång har högt skyddsvärde ska den skyddas med extra säkerhetskrav enligt MSB:s rekommendationer om fysisk informationssäkerhet. Hit hör till exempel serverrum, rum med switchar och annan kommunikationsutrustning samt utrymmen där känslig information hanteras.

Platser/byggnader bör vara fysiskt starka och tak, väggar och golv av solid konstruktion. Yttre dörrar skyddas på lämpligt sätt mot obehörig passage. Dörrar och fönster låses när de är obevakade och för fönster på marknivå kan yttre skydd övervägas.

Viktiga anläggningar bör placeras så att inte allmänheten kan få tillgång dit. I förekommande fall bör byggnader vara diskreta och inga tecken ska synas på att informationsbehandling finns där.

Lämplig åtkomstkontroll behöver införas, som till exempel tvåfaktorsautentisering med passerkod och hemlig PIN-kod till vissa utrymmen.

Endast behörig personal får tillträde till områden där säkerhetskrav finns. Personal ska bara känna till säkra utrymmen och aktiviteter där, baserat på vad de behöver känna till. Det ska finnas dokumenterat vem som ges tillträde för att arbeta i säkra utrymmen.

Extern servicepersonal ska beviljas begränsat tillträde bara när det behövs. Tillträde ska godkännas och övervakas, regelbundet granskas och återkallas vid behov.

Det ska finnas en instruktion för hur arbete i respektive lokal får bedrivas och personer med arbetsuppgifter i säkra utrymmen ska ha god kännedom om dessa regler. Fotografering, filmning och annan inspelningsutrustning bör inte tillåtas utan särskilt godkännande.

Driftsäkerhet

Mål: Att säkerställa korrekt och säker drift av informationsbehandlingsresurser.

Dokumenterade driftsrutiner ska finnas för uppstarts- och nedtagningsrutin, säkerhetskopiering, underhåll av utrustning, hantering av media och datahall. Rutinerna ska vara dokumenterade och tillgängliga för alla som behöver dem. De bör innefatta instruktioner om installation och konfiguration av system, säkerhetskopiering, hantering av fel, rutiner för återställande av system i händelse av systemfel, hantering av loggar och rutiner för övervakning.

Ändringshantering

Förändringar i IT-resurser ska ske enligt fastställd ändringshanteringsrutin som används inom IT-enheten i samordning med objekten. Det ska säkerställa att ändringar som införs på tjänster, moduler och komponenter i IT-miljön sker strukturerat och är riskbedömda, planerade, kommunicerade, testade och godkända.

Skydd mot skadlig kod

För att skydda mot skadlig kod behövs metoder för att förebygga, upptäcka och återställa miljön efter ett angrepp. Alla användare behöver veta hur de kan minska risken för att drabbas av skadlig kod. Tekniskt skydd behöver finnas på plats i form av antivirusprogramvara på servrar och klienter. Skyddet ska regelbundet uppdateras.

Säkerhetskopiering

Säkerhetskopior av information, program och speglingar av system ska tas och testas regelbundet enligt överenskomna regler för att säkerställa kraven i kontinuitetsplaner.

Loggning och övervakning

Händelseloggar ska finnas och ska granskas utifrån olika krav som framkommer i informations-säkerhetsklassningen. Eftersom loggarna kan innehålla konfidentiella uppgifter ska lämpliga säkerhetsåtgärder vidtas. Logginformation ska skyddas från manipulation och obehörig åtkomst. Systemloggar ska skyddas och helst realtidskopieras till ett system utan åtkomsträtt från privilegierad användare. Synkronisering av systemklockor ska göras till en och samma referenskälla för tid.

Hantering av tekniska sårbarheter

Uttalat ansvar för hantering av tekniska sårbarheter ska finnas, inkluderat övervakning av sårbarheter, riskbedömning av sårbarheter, uppdateringar och övervakning av system. I riktlinje för IT-säkerhet anges detaljer och rutiner.

Restriktioner för vilka program en användare får installera ska finnas för att minska sårbarheten och att incidenter uppkommer, som att obehörig får åtkomst till information, förlust av riktighet eller överträdelse av immateriella rättigheter. Innan ett program eller applikation kan bli godkänd att installeras ska en kontroll av programmet/appen göras även ur ett dataskyddsperspektiv.

Kommunikations- och nätverkssäkerhet

Mål: Att säkerställa skyddet av information i kommunikation.

Det finns risk för att information kan komma i orätta händer genom avlyssning, intrång eller att information förändras i överföring. För att kunna garantera konfidentialitet och riktighet är säkerhetskraven därför höga både på den tekniska nätverksmiljön men även vid muntlig överföring eller fysisk flytt av information.

Regler och rutiner för hur information med hög konfidentialitet hanteras i elektronisk kommunikation ska finnas så att lämpligt skydd erhålls.

Regler och rutiner för hur lagring och hantering av verksamhetskorrespondens ska finnas, i enlighet med relevanta nationella och lokala lagar och förordningar.

Personuppgifter och sekretessbelagda uppgifter som överförs via icke-betrodda nätverkstjänster ska skyddas med t ex kryptering. Icke-betrodda nätverk inkluderar publika internet och andra resurser utanför organisationens kontroll.

Det ska finnas utpekade ägare till nätverksutrustning med ansvar för förvaltning med tillhörande rutiner. Skyddsåtgärder ska införas utifrån klassificeringsnivån av de objekt som ansluts. I riktlinjerna för IT-säkerhet redogörs det för nätverkssäkerhet, till exempel kryptering, nätverkssegmentering, loggning, övervakning, brandväggar och begränsningar av systemanslutningar. Att segmentera nätverk betyder att man delar upp nätverket i olika segment för att t ex tillåta endast ekonomiadministratörer tillgång till nätverket med ekonomisystem eller för att separera en test- och utvecklingsmiljö från produktionsmiljön. Segmentering är en del av den totala säkerhetslösningen för att skydda information. Det mest grundläggande är att skilja interna nät från internet.

I styrningen av informationsbehandlingsresurser behöver följande rutiner och säkerhetsåtgärder finnas:

- rutin för att skydda information från avlyssning, kopiering, ändring och förstörelse vid överföring inom organisationen eller till en extern enhet
- rutiner för identifiering av och skydd mot skadlig kod som kan överföras, t ex att endast tillåta kontrollerad app-installation
- användares ansvar att inte kompromettera organisationen, till exempel genom vidarebefordran av kedjebrev, obehöriga köp osv
- användning av krypteringsteknik för att säkerställa konfidentialitet och riktighet
- kommunikationstjänster med externa nätverk ska dokumenteras och godkännas enligt riktlinje för IT-säkerhet.

Vad gäller informationssäkerhet för överföring av information i elektroniska meddelandetjänster som e-post eller chatt, ska rutiner och säkerhetsåtgärder finnas för:

- skydd av meddelanden från obehörig åtkomst
- att säkerställa korrekt adressering
- tillförlitlighet och tillgänglighet av tjänsten
- legala överväganden, t ex krav på elektroniska signaturer
- att inte externa sociala nätverk, fildelning eller meddelandetjänster (chatt) används utan godkännande.

Även annan kommunikation och informationsöverföring kräver säkerhetsåtgärder. Följande rutiner och säkerhetsåtgärder ska finnas:

- inte lämna meddelanden med konfidentiell information på telefonsvarare
- rådgivande information till medarbetare som använder faxar att det är lätt att skicka fel och att obehöriga kan ta del av uppgifterna
- rådgivande information till medarbetare att inte samtala om konfidentiella ämnen på platser där obehöriga kan ta del av uppgifterna
- rutiner för att identifiera bud
- regler och rutiner för att skydda information under transport ska regleras i avtal.

Avtal rörande konfidentialitet och tystnadsplikt skyddar organisationens information och upplyser den som undertecknar om deras ansvar för att skydda, använda och tillgängliggöra information på ett ansvarsfullt och godkänt sätt.

Tjänster för informationsöverföring ska i övrigt uppfylla alla relevanta legala krav.

Anskaffning, utveckling och underhåll av system

Mål: Att säkerställa att informationssäkerhet är en integrerad del av informationssystemet över hela livscykeln. Inkluderar krav på system som tillhandahåller tjänster via publika nätverk.

Vid anskaffning av nya IT-system och vid utveckling och förbättringar av befintliga IT-system ska informationssäkerhetskrav ställas baserat på informationens klassningsnivå. Identifiering och hantering av informationssäkerhetskrav ska ske tidigt i projekteringsstadiet för att kunna leda till verkningsfulla och kostnadseffektiva lösningar. Identifiering av krav baseras på externa och interna regelverk, riskanalyser och analys av tidigare incidenter. Kraven behöver inkludera nivå på förtroende som krävs mot den påstådda identiteten hos användaren för autentisering och eventuella krav på loggning och övervakning. Resultatet ska dokumenteras.

Vid upphandling av system ska krav på systematiskt informationssäkerhetsarbete enligt ISO 27000 efterfrågas och utvärderas vid anbud. Om personuppgifter ska hanteras i systemet tillkommer extra säkerhetsåtgärder rörande personuppgifter att beakta:

- ev konsekvensbedömning
- tredjelandsöverföringar
- personuppgiftsbiträdesavtal
- ev sekretessavtal
- rätt till tredjepartsrevision
- inbyggt dataskydd.

Grundlig testning och verifiering krävs av nya och uppdaterade system. För att säkerställa att systemet fungerar som förväntat ska acceptanstest göras. Omfattningen står i proportion till systemets betydelse.

Vid systemutvecklings- och integrationsåtgärder ska säkra utvecklingsmiljöer upprättas och skyddas. En säker utvecklingsmiljö inkluderar människor, processer och teknik som är involverade i utvecklingen/integrationen.

Personuppgifter bör inte användas för testningsändamål; fiktiva eller automatiskt genererade personuppgifter bör istället användas. Om det inte går att undvika att använda personuppgifter ska likvärdiga tekniska och organisatoriska åtgärder som används i produktionsmiljö tillämpas, för att skydda personuppgifterna.

Information i programtjänster på publika nätverk behöver skyddas från bedräglig aktivitet, obehörigt röjande och modifiering. Tillämpningar som är tillgängliga via publika nätverk är föremål för ett antal nätverksrelaterade hot. Detaljerade riskbedömningar och säkerhetsåtgärder är nödvändiga. Normalt omfattar åtgärderna kryptering för autentisering och säker överföring av data.

Leverantörsrelationer

Mål: Att säkerställa skydd av de av organisationens tillgångar som leverantörer har åtkomst till.

Det ska finnas avtal med varje leverantör som kan tillgå, behandla, lagra eller kommunicera kommunens information eller som tillhandahåller infrastrukturkomponenter för informationen. Informationssäkerhetskrav motsvarande klassningsnivån ska ställas i avtalen för att minska riskerna som finns när en leverantör har åtkomst till informationstillgångar och för att säkerställa att det inte finns några missförstånd mellan verksamheten och leverantör. Följande områden kan ingå för att uppfylla informationssäkerhetskrav:

- beskrivning av informationen och metoder för att få tillgång till den

- klassningsnivån (mappat till leverantörens klassningssystem)
- rättsliga krav och beskrivning av hur det säkerställs att det uppfylls
- regler för tillåten/otillåten användning av information
- krav och rutiner för incidenthantering
- rutiner och villkor för att få tillgång till information (behörigheter)
- eventuella krav på bakgrundskontroll av leverantörens personal
- rätt att granska leverantörens processer och säkerhetsåtgärder, även av oberoende tredje part
- hantering av oenigheter
- hur avtalet omfattar underleverantörer
- leverantörens skyldigheter att uppfylla kommunens säkerhetskrav.

Särskilt avtal rörande hantering av personuppgifter ska upprättas enligt gällande rutin i organisationen. Där ska bland annat en instruktion finnas som beskriver hur leverantören får behandla personuppgifter. Eventuella underbiträden behöver godkännas av den personuppgiftsansvarige. I dataskyddsförordningens artikel 28 är det angivet vad som måste finnas med i ett avtal rörande personuppgiftsbehandlingar å den personuppgiftsansvariges räkning.

Hantering av informationssäkerhetsincidenter

Mål: Att säkerställa ett konsekvent och verkningsfullt tillvägagångssätt för hantering av informationssäkerhetsincidenter inklusive kommunikation kring säkerhetshändelser och svagheter.

En informationssäkerhetsincident är en händelse som har eller kunde ha försämrat konfidentialiteten, riktigheten eller tillgängligheten av information. Alla användare av information i organisationen är skyldiga att rapportera brister i informationssäkerheten och incidenter. Det skulle kunna röra sig om att en obehörig fått tillgång till kommunens lokaler, att information har röjts till obehöriga eller har ändrats felaktigt, att information som borde ha varit arkiverad har försvunnit, att användare kan varandras lösenord eller att skadlig kod har påträffats i IT-miljön. Informationssäkerhetsincidenter täcker händelser inom det tekniska skyddet (IT-säkerhet, fysisk säkerhet) och inom det administrativa (rutiner, regler).

Informationsägare ansvarar för att det finns rutiner för att incidenter rörande informationens säkerhet upptäcks, analyseras och rapporteras. I rutinen för incidenter ska det framgå om en incident är rapporteringsskyldig, hur rapporteringen görs, vad som ska rapporteras och till vem.

Erfarenheter från incidenter ska ligga till grund för framtida beslut för att förbättra skyddet, t ex att investera i nya säkerhetslösningar eller införa nya rutiner och kontroller för att förhindra att incidenten sker igen.

Anmälan av informationssäkerhetsincidenter inryms i samma process som den för IT-säkerhets-incidenter som beskrivs i riktlinje för IT-säkerhet. Det är en konsekvent effektiv process med mottagning, styrning, analys, återkoppling och vidarebefordran till ansvariga och berörda personer.

Eftersom vissa incidenter ska rapporteras till tillsynsmyndighet skyndsamt så ska en bedömning av incidenten genast påbörjas. Som exempel kan nämnas incidenter med personuppgifter, enligt dataskyddsförordningen, och incidenter som rör säkerhet i nätverk och informationssystem inom samhällsviktiga tjänster, enligt NIS-direktivet.

För personuppgiftsincidenter finns särskild rutin och stödmaterial för att göra bedömningen om det är en incident som ska rapporteras in till tillsynsmyndigheten. Respektive verksamhets utsedda dataskyddskontaktperson leder arbetet med incidentrapporteringen och tar vid behov kontakt med olika stödfunktioner beskrivna i rutinen.

Informationssäkerhetsaspekter i kontinuitetshanteringen

Mål: Kontinuiteten för informationssäkerhet bör vara integrerad i organisationens ledningssystem för kontinuitetshantering.

Kontinuitetshantering handlar om att planera för att upprätthålla sin verksamhet på en acceptabel nivå oavsett störning. Man kan för enkelhetens skull kalla det att ”ha en plan B” för verksamheten. En störning kan vara att personal inte finns tillgänglig, att lokaler inte kan användas, att leverans av tjänster inte når verksamheten eller att man drabbas av strömavbrott.

För att minska brister i tillgången till information behöver således informationssäkerhets-aspekten ingå i analysen för verksamhetens kontinuitetshantering. Hur länge kan man klara sig utan informationen, finns det en reservplan, behövs det redundans?

Med kontinuitetshantering kan man snabbare återhämta sig eller mildra konsekvenserna av en inträffad händelse. Det blir kortare störningsperioder i verksamheten och man kan förhindra att informationsrelaterade värden går förlorade.

Aktiviteter inom kontinuitetshantering är exempelvis att:

- kartlägga viktiga processer
- identifiera beroenden av resurser
- bestämma vad som är acceptabla avbrottstider
- genomföra åtgärder som minskar risk för störning
- skapa planer för att hantera störningar som ändå uppstår.

Kontinuitetshantering utförs dels i risk- och sårbarhetsanalysen (RSA:n) som görs enligt lagen om extraordinär händelse och dels i informationssäkerhetsklassningar.

Eftersom så mycket av informationen som hanteras idag är digital så är IT-komponenter ett viktigt stöd för verksamhetsprocesser, vilka ibland kan vara helt beroende av tillgänglighet och att allt fungerar som det är tänkt. Kontinuitetshantering för IT är därför en viktig del i informations-säkerhetsarbetet för att minimera negativa konsekvenser vid allvarliga IT-relaterade incidenter eller avbrott. Syftet är att efter ett större avbrott så snabbt som möjligt återgå till normalläge och att konsekvenserna för verksamheten ska vara så små som möjligt, både under och efter avbrottet.

För informationstillgångar med höga skyddskrav avseende tillgänglighet behövs en beredskap för att hantera avbrott. Vid höga tillgänglighetskrav behövs redundanta enheter eller redundant arkitektur. Tester för att säkerställa övergången från enhet till en annan behöver göras.

- Avbrottsplaner ska finnas för alla kritiska IT-resurser.
- Övning och testning av avbrottsplaner ska genomföras och utvärderas regelbundet för att ständigt förbättra kontinuiteten.
- Avbrottsplaner ska vara kända för de som ingår i aktiviteterna samtidigt som de har ett högt skyddsvärde avseende konfidentialitet och ska inte komma obehöriga tillhanda.

Informationsägaren ska ställa krav på leverantör av system, arkitektur och drift som motsvarar klassningsvärdet av informationen.

Efterlevnad

Mål: Att undvika överträdelser av författningsenliga eller avtalsmässiga skyldigheter relaterade till informationssäkerhet, dataskydd och av eventuella säkerhetskrav.

Alla relevanta juridiska och avtalsmässiga krav ska uttryckligen identifieras, dokumenteras och hållas uppdaterade för varje informationstillgång.

I ett LIS ingår granskning, uppföljning och efterlevnad av informationssäkerheten i verksamheten. I praktiken innebär det ett systematiskt förbättringsarbete där sårbarheter och

brister som upptäcks vid granskningar ska åtgärdas. Akuta sårbarheter och brister ska dock åtgärdas genast.

Informationsägare ansvarar för att åtgärder vidtas för brister inom informationssäkerheten och att eventuella risker som accepteras tydligt dokumenteras. Korrekt informationssäkerhet ska säkerställas under hela livscykeln och informationsägare ansvarar därför för att kontroller utförs av att rätt skyddsnivå uppnås. Rätt skyddsnivå avgörs med hjälp av verksamhetsanalyser och juridiska analyser i informationssäkerhetsklassningar.

I internkontrollplanen i organisationen bör moment rörande informationssäkerhet och dataskydd finnas med, till exempel:

- efterlevnad av policy och riktlinje
- att skydd av information enligt gällande författningar finns
- att de mest kritiska informationstillgångarna har tilldelade informationsägare och är klassade
- att säkerställa behöriga åtkomster
- att användare får utbildning i deras ansvar
- att rutin för att rapportera informationssäkerhets-/personuppgiftsincidenter finns.

Informationssäkerhetssamordnaren ska stödja verksamheterna att efterleva styrdokumenten inom informationssäkerhet och kontrollera och följa upp efterlevnad.

Dataskyddsombudet ska kontrollera respektive personuppgiftsansvarigs efterlevnad av gällande dataskyddslagstiftning rörande personuppgifter.

Extern revision av efterlevnad behöver också genomföras, till exempel på uppdrag av den kommunala revisionen.