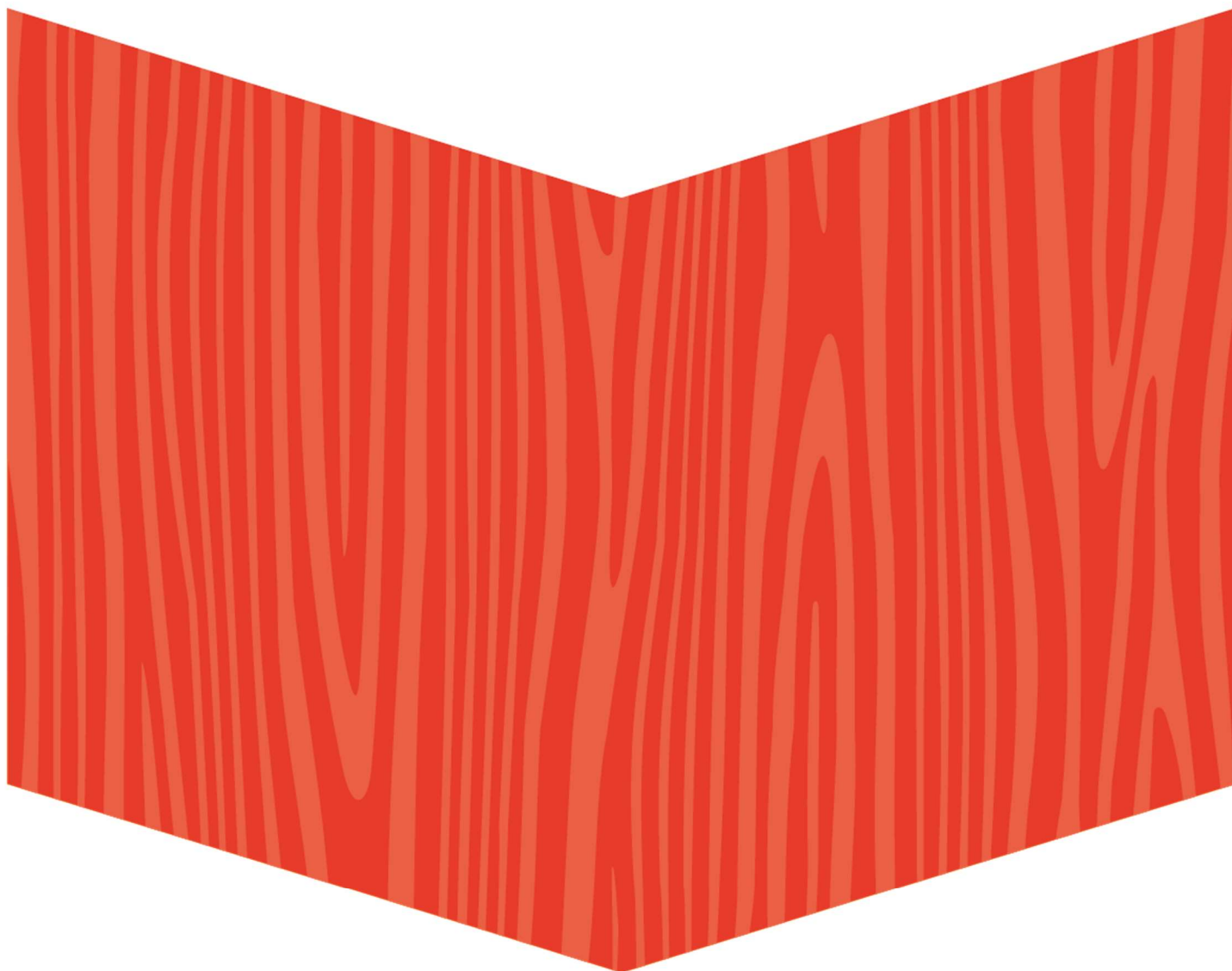




Riktlinjer för informationssäkerhet i Vingåkers kommun

Kommunstyrelsen

Flik 8.34





Dokumenttyp	Riktlinje
Dokumentnamn	Riktlinjer för informationssäkerhet i Vingåkers kommun
Fastställt	2023-11-13, Ks § 207
Beslutande	Kommunstyrelsen
Giltighetstid	Tillsvidare
Processägare	Säkerhetsskyddschef
Senast reviderad	-
Detta dokument gäller för	Vingåkers kommun

Innehållsförteckning

Innehållsförteckning	3
1. Inledning.....	4
2. Begrepp och definitioner.....	5
3. Vad är informationssäkerhet.....	7
4. Organisation, ansvar, roller.....	9
5. Att arbeta systematiskt.....	10
6. Personalsäkerhet.....	11
7. Under anställning/uppdrag.....	11
8. Efter anställning.....	11
9. Hantering av informationstillgångar.....	12
10. Informationssäkerhetsklassning.....	12
11. Styrning av åtkomst.....	13
12. Säkra inloggningsrutiner.....	13
13. Process för att hantera användarkonton.....	14
14. Kryptering.....	14
15. Fysisk säkerhet.....	15
16. Säkra utrymmen.....	15
17. Driftsäkerhet.....	15
18. Ändringshantering.....	16
19. Skydd mot skadlig kod.....	16
20. Säkerhetskopiering.....	16
21. Loggning och övervakning.....	16
22. Hantering av tekniska sårbarheter.....	16
23. Kommunikations- och nätverkssäkerhet.....	16
24. Anskaffning, utveckling och underhåll av system.....	18
25. Leverantörsrelationer.....	19
26. Hantering av informationssäkerhetsincidenter.....	20
27. Informationssäkerhetsaspekter i kontinuitetshanteringen.....	20
28. Efterlevnad/ Uppföljning.....	21

1. Inledning

I dagens komplexa informationssamhälle bearbetar, lagrar, kommunicerar och mångfaldigar vi information i större mängder än någonsin tidigare.

Information är en av kommunens viktigaste tillgångar och hanteringen av den är en viktig och naturlig del i alla verksamheters dagliga arbete, samt en förutsättning för exempelvis digitalisering och för att verksamheterna ska nå sina mål enligt 2 kap. 2 § säkerhetsskyddslagen (2018:585). Offentlighets- och sekretesslagen (2009:400) samt GDPR.

Dessa riktlinjer för informationssäkerhet utgår från allmänt vedertagna säkerhetsstandarder och specifikt standarden SS-EN ISO/IEC 27002:2017 som är utgiven av standardiseringsorganisationerna SIS – Svenska Institutet för Standarder samt CEN (Comité Européen de Normalisation - europeisk standardisering) ISO och riktar in sig på de objekt som ska skyddas. Enligt NIS-direktivet, NIS-direktivet syftar till att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom EU. Det europeiska NIS-direktivet är svensk lag. Information är värdefullt och behöver skyddas efter behov. Ett bra informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering. Detta skapar förtroende både inom och utanför organisationen.

Varje dag arbetar Vingåkers kommuns medarbetare med uppdrag att erbjuda välfärd, service till invånare, föreningar, företag och besökare i Vingåkers kommun.

Hur många av uppdragen är beroende av att medarbetaren har tillgång till behövda uppgifter? Vad händer om uppgifterna inte går att få tag på, inte är korrekta eller sprids till fel personer? Det medför konsekvenser. Hur stora konsekvenserna är för verksamhet och de individerna vars personuppgifter kommunen hanterar varierar stort. Det är viktigt att vi förstår konsekvenser i verksamhet och för utsatta individer för att vi ska kunna anpassa skyddet för uppgifterna till en lämplig nivå. Ansvaret för ledning, genomförande och utvärdering, uppföljning av de olika skyddsåtgärderna med gemensamt syfte att uppnå kommunens mål med informationssäkerhetsarbete. Informationssäkerhet handlar framför allt om att hindra information från att läcka ut, förvanskas och förstöras. Det handlar också om att rätt information ska finnas tillgänglig för rätt personer, och i rätt tid. Information ska inte kunna hamna i orätta händer och missbrukas. Informationssäkerhet gäller såväl hos enskilda personer som hos organisationer, både i näringslivet och i offentlig verksamhet. Informationssäkerhet omfattar därför hela samhället. Arbetet med informationssäkerhet ska vara långsiktigt och kontinuerligt, omfatta alla delar av kommunens verksamheter, bolag, förbund och alla de informationstillgångar som vi äger eller hanterar. Informationssäkerhetsarbete ska vara ett stöd för personal, samverkande partners och kommunens invånare.

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

Vingåkers kommuns verksamhet är omfattande och komplex, med många olika intressenter och med ett stort beroende av information. En effektiv och säker användning av information är en förutsättning för Vingåkers kommuns verksamhet. Informationssäkerhetsarbetet främjar verksamheternas funktionalitet, kvalitet och effektivitet och tillgodoser invånarens rättigheter och personliga integritet. Sammantaget är detta viktiga förutsättningar för att skapa förtroende avseende vår förmåga att leverera service till våra invånare.

Dessutom ställer offentlighetsprincipen krav på Vingåkers kommuns informationshantering, liksom speciallagstiftning inom verksamhetsområden som hälso- och sjukvård. Detta sammantaget gör information till en av Vingåkers kommun mest betydelsefulla resurser.

2. Begrepp och definitioner

Begrepp	Definition
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).
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.
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.
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.
Informationsägare	Individ 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.
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.
Risikanalys	Process för att förstå en risks natur och avgöra sannolikhet för negativa händelser och dess konsekvenser.
IT-säkerhet	IT-relaterade tekniska säkerhetsåtgärder för att upprätthålla informationssäkerhet. Omfattar datasäkerhet och kommunikationssäkerhet
Fysisk säkerhet	Tekniska säkerhetsåtgärder relaterade till skydd av person, lokal och utrustning av betydelse för informationssäkerhet. Tillträdesskydd
Teknisk säkerhet	Säkerhetsåtgärder för att upprätthålla informationens konfidentialitet, riktighet och tillgänglighet. Omfattar områdena IT-säkerhet och fysisk säkerhet. Tillträdesskydd
Riktighet	Skydd mot oönskad förändring.
Konfidentialitet	Skydd mot obehörig insyn
Spårbarhet	Entydig härledning av utförda aktiviteter till en identifierad användare.
Åtkomsträttighet	Användares behörigheter uttrycks i tilldelade åtkomsträttigheter som definierar vad en användare har rätt att utföra inom ansvarsområde läsa, söka, skriva, radera, skapa, exekvera och arkivera.
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.
Redundans	Tillstånd då mer än ett medel finns för att upprätthålla ett givet funktionssätt i syfte till att säkerställa kontinuerlig drift.
Objektstyrning	En modell för styrning av objekt. Objekten består av verksamhetskomponenter (t ex processer, rutiner, manualer) och IT-komponenter (tex IT-system). Det handlar om att stärka samverkan mellan verksamhet och IT för att åstadkomma rättstöd till verksamheten. Gemensamma mål sätts upp och prioriteras. Objekten hanterar vidmakthållande, vidareutveckling, nyutveckling och avveckling.
NIS-direktivet	NIS-direktivet syftar till att uppnå en hög gemensam nivå på säkerhet i nätverk och informationssystem inom EU. Det europeiska NIS-direktivet är svensk lag.

SIGNE	Signalskyddssystem för delgivning och mottagning av säkerhetsklassificerad information upp till Begränsat hemlig.
Konsekvensbedömning	Process för att beskriva en personuppgiftsbehandling och för att hantera risker för den enskilde individen, enligt artikel 35 i dataskyddsförordningen (GDPR).
Informationstillgång	Information, och resurser som hanterar den, som är av värde för en organisation.
Informationsägare Ägarskapet gäller informationen. informationsägaren ansvarar för att informationen hanteras utifrån interna regelverk och externa krav som lagstiftning. Det sker bland annat genom informationssäkerhetsklassificering och riskanalyser. Beslut som fattas för en informationstillgång gäller för alla som hanterar informationen	Objektsägare Ägarskapet gäller systemet/objektet/IT-komponenter. 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 rätt och säkert sätt utifrån lagar och förordningar.

3. Vad är informationssäkerhet

Arbetet med informationssäkerhet omfattar att införa och förvalta administrativa regelverk som policies och riktlinjer, tekniskt skydd med bland annat brandväggar och kryptering samt fysiskt skydd med till exempel skal- och brandskydd. Det handlar om att ta ett helhetsgrepp och skapa ett fungerande långsiktigt arbetssätt för att ge kommunens organisationens information det skydd den behöver.

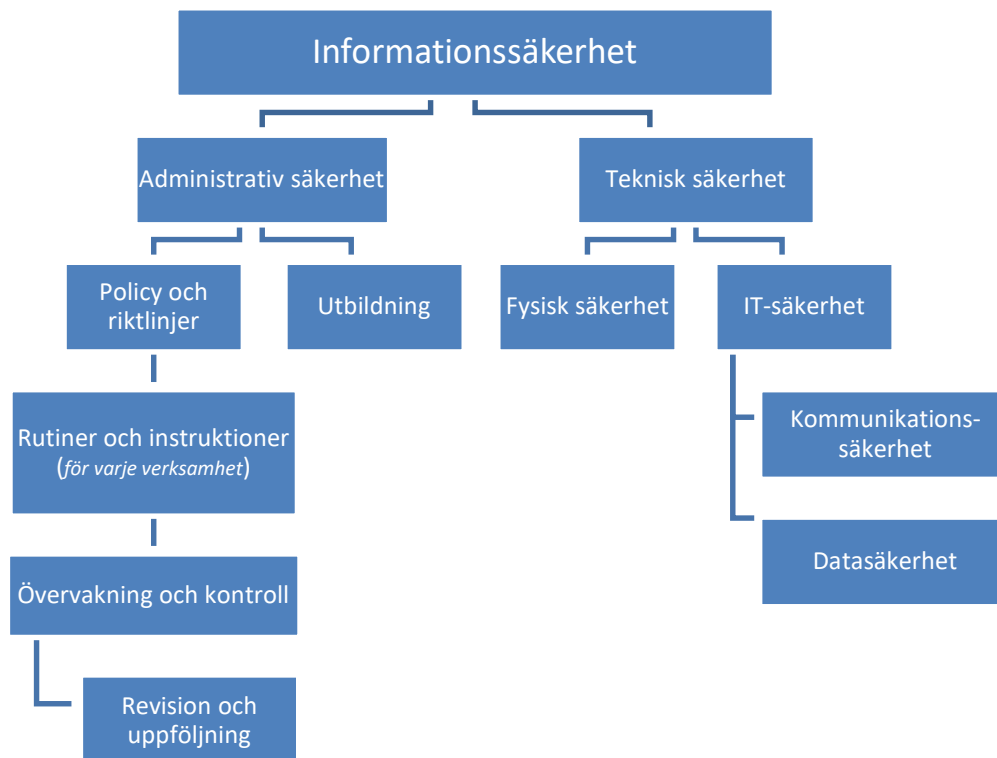
Viss information är känslig och måste skyddas från obehöriga att ta del av. Det handlar ofta om hänsyn till den personliga integriteten och för att undvika att enskilda individer kommer till skada men även annan konfidentiell information. Det finns många lagar och föreskrifter som kommunen måste leva 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 teknisk säkerhet och administrativ säkerhet

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



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 Vingåkers kommun skadas.

Administrativ säkerhet, Informationssäkerhet, IT-säkerhet, Fysisk säkerhet Sammantaget finns stora krav på informationssäkerhet och därför är systematik och en fast styrning nödvändig för att upprätthålla säkerhet och kvalitet inom Vingåkers kommun.

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 skydds krav 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.

4. 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 Informationssäkerhetspolicy för Vingåkers kommun. 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 styrdokumentet och beslutar om de instruktionerna som rör informationssäkerhet.

Kommundirektör/VD har ansvar att utse representanter inom Informationssäkerhetsråd samt ge de förutsättningarna för att bedriva informationssäkerhetsarbete inom förvaltningen.

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 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.

Användare har ett ansvar för säkerheten i informationshanteringen och ansvarar för att följa de styrdokument, rutiner och instruktioner som finns. De ansvarar även för att vara uppmärksam på brister och incidenter rörande informationssäkerhet och att rapportera dessa till närmsta chef, IT-enheten och säkerhetsskyddschef.

Säkerhetsskyddschef är en stödfunktion i organisationen ungefär som andra stödfunktioner inom andra verksamhetsområden som ekonomi-, personal- och kommunikationsfunktioner. Säkerhetsskyddschef samordnar arbete i samråd med utsedda verksamhetsrepresentanter som deltar inom informationssäkerhetsråd, systemförvaltare och GDPR.

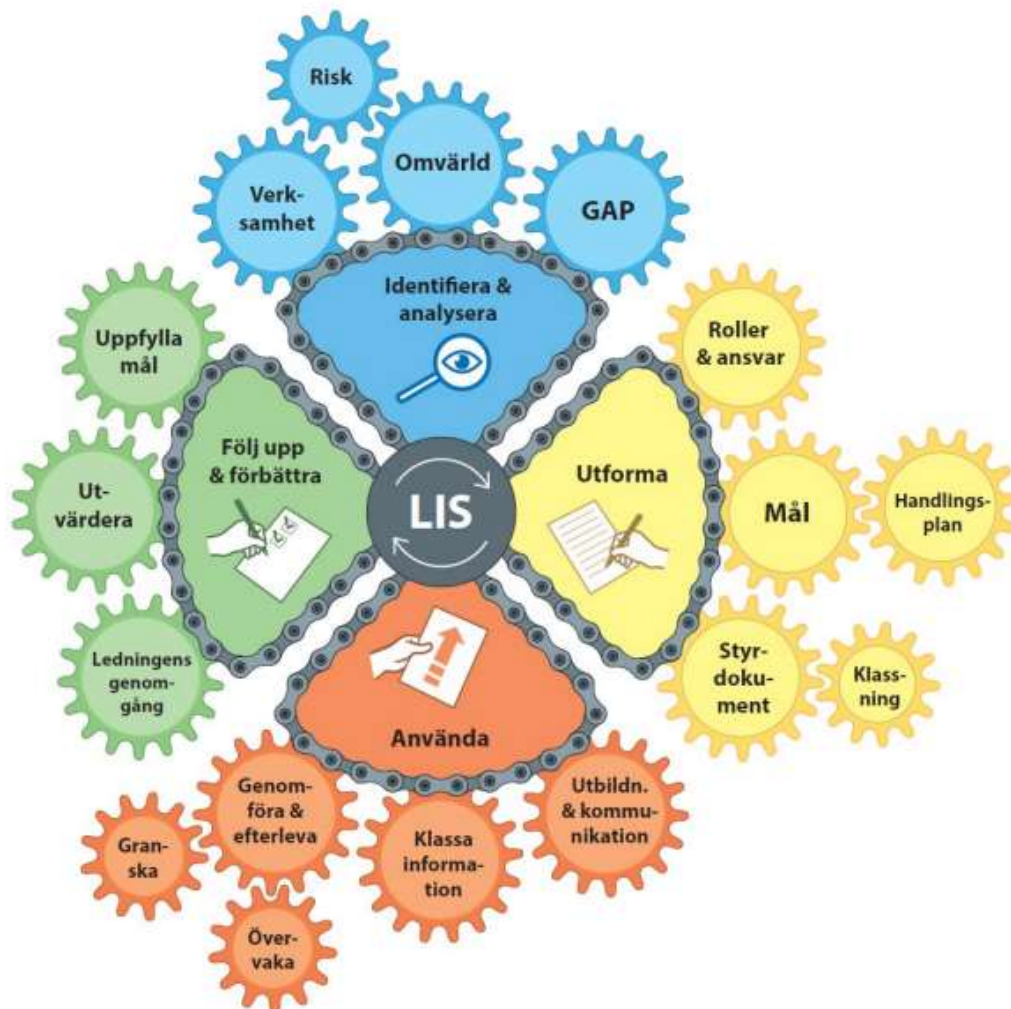
Ansvarsområdet för säkerhetsskyddschef är att ge stöd till ledning, verksamhetschefer och medarbetare så att de kan ta ansvar för informationssäkerheten i sin verksamhet. Säkerhetsskyddschef

ska kontrollera och följa upp informationssäkerheten internt och ansvarar för att förvalta och utveckla ledningssystemet för informationssäkerhet (LIS).

5. Att arbeta systematiskt

Informationssäkerhetspolicy 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.

6. Personalsäkerhet

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

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.

7. 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 se till att medarbetare får utbildning i informationssäkerhet och dataskydd kontinuerligt.

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

8. Efter anställning

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

9. Hantering av informationstillgångar

Ansvar för tillgångar

Mål: Organisationens tillgångar ska identifieras och skyddas ett ägarskap med tillhörande ansvar ska definieras.

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.

10. 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 applicera rätt skydd ska tillgången informationssäkerhetsklassas för egenskaperna konfidentialitet, riktighet och tillgänglighet. Informationsägare ansvarar för att klassificering utförs enligt kommunens modell, VINGSYS som bygger på SKR:s verktyg KLASSA.

Om informationen kommer i orätta händer vilka konsekvenser kan det bli för individen, för verksamheten, för ekonomin och för samhället.

- **Informationen kommer i orätta händer? Konfidentialitet**
- **Informationen inte stämmer? Riktighet**
- **Informationen 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 framtagen.

11. 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 instruktion för IT-säkerhet.

12. Säkra inloggningsrutiner

Tillgång till system och applikationer behöver styras med säkra inloggningsrutiner så att så lite som möjligt avslöjas vid inloggning. Inga hjälpmedelanden 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 rutin för IT-säkerhet.

13. 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 och under övervakning.

14. Kryptering

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

Krypteringssystem Signe hanterar säkerhetsskyddsklassificerat information upp till begränsat hemlig.

Länsstyrelse tillhandahåller godkända krypteringslösningar och instruktioner hur de ska användas. Krypteringslösningar beskrivs i instruktion för signalskyddssystem- Signe.

Rutin för nyckelhantering, inklusive metoder för att hantera skyddet av kryptografiska nycklar och återvinning av krypterad information om nycklar förloras, äventyras eller skadas finns.

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

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

15. Fysisk 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 ska 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 regelverk. Ansvarig för kontroll är ansvarig verksamhet i samråd med kommunens säkerhetsstrateg/säkerhetsskyddschef.

16. 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 ska 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 ska placeras så att inte allmänheten kan få tillgång dit. I förekommande fall ska 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 ska inte tillåtas utan särskilt godkännande av säkerhetsskyddschef/biträdande signalskyddschef.

17. 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 systemhändelse av systemfel, hantering av loggar och rutiner för övervakning.

18. 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.

19. 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.

20. Säkerhetskopiering

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

21. Loggning och övervakning

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

22. 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.

23. 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.

24. 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, skyddsanalyser 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 27 000 efterfrågas och utvärderas vid anbud. Om personuppgifter ska hanteras i systemet tillkommer extra säkerhetsåtgärder rörande personuppgifter att beakta:

- ev konsekvensbedömning
- tredjelandsoverföringar
- personuppgiftsbiträdesavtal
- 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.

25. 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.

26. 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 informationssäkerhet 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 och investeringar i nya säkerhetslösningar eller införande av nya rutiner och kontroller för att förhindra att incidenten sker igen.

Anmälan av informationssäkerhetsincidenter genomförs i samma process som den för IT-säkerhetsincidenter som beskrivs i rutin för incidentrapportering. Det är en konsekvent effektiv process med mottagning, styrning, analys, återkoppling och vidarebefordran till ansvariga och Säkerhetsskyddschef.

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.

27. 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 strömbrott. För att minska brister

i tillgången till information behöver informationssäkerhetsaspekten ingå i RSA-arbete och 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 informationstillgångar och värden går förlorade.

Aktiviteter inom kontinuitetshantering är exempelvis att:

- Kartlägga viktiga processer
- Identifiera beroenden av resurser
- Bestäm acceptabla avbrottstider
- Genomför åtgärder som minskar risk för störning
- Upprätta planer för att hantera störningar som ändå uppstår.

Kontinuitetshantering utförs dels i risk- och sårbarhetsanalysen (RSA:n) som görs enligt lagen om extraordinär händelse, 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 informationssäkerhetsarbetet 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 skydds krav 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-system.
- Övning och testning av avbrottsplaner ska genomföras och utvärderas regelbundet för att ständigt förbättra kontinuiteten.
- Avbrottsplaner ska vara kända för de som ingår inom samhällsviktig verksamhet och samhällsviktiga funktioner, 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.

28. Efterlevnad/ Uppföljning

Mål: Att undvika överträdelser av författningens 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 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 säkerhetsskyddsanalyser 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 lagar och författningar finns
- att de mest kritiska informationstillgångarna har tilldelade informationsägare och är klassade
- att säkerställa behöriga åtkomster
- att alla medarbetare får anpassade utbildningar i deras ansvar
- att rutiner för att rapportera informationssäkerhets-/personuppgiftsincidenter uppdateras, implementeras och följs upp.

Informationssäkerhetschef ska stödja verksamheterna att efterleva styrdokument inom informationssäkerhet och kontrollera och följa upp efterlevnad.

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

Kommunstyrelsen/ledningen ska minst en gång per år informera sig om hur arbetet med informationssäkerhet går. Uppföljningen ska baseras på underlag med rekommendationer som tas fram av informationssäkerhetsansvarig. Underlaget ska innefatta information om:

- Förändringar utanför kommunen som kan påverka informationssäkerheten
- Utbildning (status och behov)
- Inträffade incidenter av större påverkan på verksamheten.
- Resultat från genomförda granskningar
- Aktuella och planerade säkerhetsåtgärder
- Rekommendationer till förbättringar

Resultatet från denna uppföljning ska innefatta beslut om åtgärder för att förbättra informationssäkerheten samt tilldelning av resurser.