ESLÖVS KOMMUN

RUTIN FÖR INFORMATIONSSÄKERHET

Dokumentet är antaget av Kommundirektören 2023-03-31gäller från och med den1 april 2023. Det riktar sig till hela kommunen. Ses över för revidering senast december 2025. Kontaktperson: Kommunledningskontoret, juridiska avdelningen informationssäkerhetssamordnare. (21)

Innehåll

1 Inledning

Syftet med instruktionen är att specificera vilka övergripande säkerhetsåtgärder som ska vidtas inom de områden som standarden för ledningssystem för informationssäkerhet, SS-EN ISO/IEC 27001 och SS-EN ISO/IEC 27002, omfattar.
Standarden anger övergripande vilka skyddsåtgärder som ska finnas men Eslövs kommun har anpassat standarden till sin verksamhet och antagit en lämplig nivå utifrån organisationens förutsättningar. Eslövs kommun är i detta avseende en mycket stor organisation med skiftande verksamhet där kraven på skydd av information skiljer sig åt mellan de olika förvaltningarna.

2 Omfattning

Instruktionen ska efterlevas av samtliga nämnder/förvaltningar.

3 Övergripande informationssäkerhetsåtgärder

Riktlinjen utgår från standarden för informationssäkerhet 27001 samt 27002.

4 Personalsäkerhet

4.1 Före anställning

a) Vid rekrytering till särskilt informationssäkerhetskritiska arbetsuppgifter ska fler och mer detaljerade kontroller övervägas exempelvis bakgrundskontroll.
b) Bakgrundskontroll ska genomföras när behov föreligger till exempel hantering eller tillgång till information som omfattas av NIS direktivet.
c) Innan anställning eller annat deltagande i verksamhet som innebär tillgång till information som är säkerhetsskyddsklassad ska säkerhetsprövning med registerkontroll göras.

4.2 Under anställning

a) Anställda ska i samband med rekrytering samt kontinuerligt under anställningstiden göras medvetna om sitt ansvar för informationssäkerhet och tillämpliga lagkrav, t.ex. beträffande allmänna handlingar och sekretess.

b) Anställda ska göras medvetna om att bristande efterlevnad av gällande regler för informationssäkerhet och sekretess kan utgöra brott, både mot gällande lagstiftning samt mot anställningsavtalet. Ytterst kan detta leda till uppsägning eller avsked.

4.3 Sekretess

a) I det fall information som omfattas av sekretess ska hanteras av anställda ska erinran om sekretess ske där medarbetaren informeras om vilka skyldigheter som följer av lag.
b) Sekretessen omfattar inte enbart den som är anställd av Eslövs kommun eller dess bolag. Vid anlitande av konsult eller annan extern uppdragstagare ska det klargöras om han eller hon deltar i verksamheten på samma sätt som en anställd i Eslövs kommun.
c) Deltar personen inte i verksamheten på sådant sätt att offentlighets- och sekretesslagen blir tillämplig, ska tystnadsplikten regleras civilrättsligt, det vill säga i avtal samt informeras om konsekvenser av bristande efterlevnad. Samt genom Lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.

4.4 Utbildning

a) Anställda ska erbjudas den utbildning i informationssäkerhet som krävs för att de ska kunna utföra sina arbetsuppgifter på ett säkert sätt. Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen. Detsamma gäller även vid förflyttning och omplacering av redan anställda och när tillfällig personal och externa konsulter anlitas.

4.5 Avslut eller ändring av anställning

a) Det ska finnas en fastställd rutin för hantering av personal som avslutar sin anställning. Rutinen ska säkerställa att ansvarsuppgifter överlämnas och att åtkomsträttigheter/behörigheter upphör vid anställningens slut.

5 Hantering av tillgångar

5.1 Förteckning över viktiga informationstillgångar

a) Respektive chef ska ha en förteckning över viktiga informationstillgångar inom sin verksamhet.

5.2 Klassning av information

a) Respektive informationstillgång ska tilldelas en informationssäkerhetsklass som motsvarar dess betydelse för den aktuella verksamheten och de legala krav som finns.

b) Vid informationsklassificering ska gällande rutin/instruktion samt informationsklassificeringsmodell användas.

c) Informationsklassificering ska baseras på säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet. Nivåbestämningen ska utgå från de konsekvenser som obehörig åtkomst, bristande riktighet och bristande tillgänglighet till informationstillgång ger upphov till.

5.3 Märkning av information

a) Märkning av information är en förutsättning för att information ska hanteras rätt vid informationsdelning. Märkning av information ska ske med utgångspunkt från resultatet av genomförd informationsklassning. Detta ska gälla för information i såväl fysisk som elektronisk form.

5.4 Hantering av information som omfattas av sekretess

a) En offentlig verksamhets informationshantering styrs av ett omfattande regelverk, däribland grundlagarna. Alla handlingar som upprättas eller inkommer till en myndighet är i princip allmänna och normalt offentliga och ska vara tillgängliga för allmänheten. Det finns dock allmänna handlingar där uppgifter sekretessmarkerats och som behöver hanteras på säkert sätt.

b) Det ska finnas styrande dokument för utlämnande av information. I dessa ska det framgå vem eller vilka som har rätt att fatta beslut om ett utlämnande och vem som fattar beslut om att inte lämna ut en allmän handling.

c) Det ska finnas styrande dokument som reglerar på vilket sätt säkerhetsskyddsklassificerade uppgifter och handlingar som omfattas av säkerhetsskyddslagen praktiskt ska hanteras.

5.5 Personuppgifter

a) Om personuppgifter behandlas omfattas behandlingen av dataskyddsförordningen. Innan behandling av personuppgifter får ske kan särskilda skyddskrav behöva vidtas. Vilka kraven är ska

avgöras med stöd av underlag från informationsklassificering, riskanalys och genomförande av konsekvensbedömning (DPIA).

5.5.1 Skyddade personuppgifter

a) Skyddade personuppgifter innebär att personer som lever under hot får ett ökat skydd. Det finns tre typer av skyddsåtgärder i folkbokföringen; sekretessmarkering, skyddad folkbokföring och fingerade personuppgifter.
b) Alla personer ska kunna känna sig trygga med att deras personuppgifter inte kommer i orätta händer. Informationsutbyte, elektronisk eller icke-elektronisk, får inte leda till att skyddade uppgifter röjs.
   Det ska finnas styrande dokument som reglerar hur skyddade personuppgifter ska hanteras. Personuppgifter som är skyddade ska vara tydligt märkta så att detta framgår för personer som hanterar dem.
c) Vid utveckling och förvaltning av informationssystem ska hantering av skyddade personuppgifter beaktas särskilt. Informationssystem ska utformas så att endast de som har behov får tillgång till sådana uppgifter.

5.6 Sammanställning och analys

a) Vid sammanställning och analys av stora mängder personuppgifter ska informationsklassificering och riskanalys alltid genomföras och dokumenteras. Den information som sammanställs och analyseras liksom den information som blir resultat av den ska ha tillräckligt skydd från insamling till färdigt resultat. Informationsägare fattar beslut om hur informationen ska hanteras. Beslutet ska dokumenteras.

5.7 Hantering av lagringsmedia

a) Med lagringsmedia avses media där information finns. Det kan röra sig om hårddiskar, papper, USB-minnen, minneskort m.m. Vid förvaring och transport av lagringsmedia ska skyddet motsvara det skyddsvärde som informationen har utifrån den informationsklassificering som genomförts.
b) Lagringsmedia som innehåller skyddsvärd information ska skyddas mot obehörig åtkomst, missbruk eller förvanskning under transport.
c) Om transport av lagringsmedia sker med transportföretag ska sådana åtgärder vidtas som skyddar informationen och som säkerställer att endast rätt mottagare kan ta emot lagringsmediet.

d) När fasta eller löstagbara lagringsmedier som innehåller eller kan innehålla personuppgifter, information som omfattas av sekretess eller av andra anledningar kan vara känslig ska gallras, utrangeras, kasseras, säljas eller på annat sätt lämna verksamheten ska lagringsmedierna förstöras alternativt raderas på ett sådant sätt att uppgifterna inte kan återskapas. Detta gäller även om informationen är krypterad.
e) För hantering av lagringsmedia som innehåller säkerhetsskyddsklassificerade uppgifter finns särskilda hanteringsregler som ska följas.

5.8 Generella regler för användning av informationssystem

a) Med godkänd utrustning och godkända tjänster nedan avses sådan utrustning och sådana tjänster som godkänts av informationsägare och/eller systemägare.
b) Eslövs kommuns resurser (datorer, mobila enheter, nätverk och kringutrustning) är avsedda att användas som arbetsredskap vid tjänsteutövning.
c) Information ska sparas på anvisad plats. För information som omfattas av sekretess finns särskilda krav på skydd och endast godkända tjänster och lagringsytor får användas. Detta gäller även säkerhetskopior.
d) Till Eslövs kommuns nätverk, datorer, mobila enheter får medarbetare endast ansluta utrustning som godkänts.
e) Information som rör Eslövs kommuns verksamhet ska som regel bearbetas och lagras med hjälp av informationssystem som godkänts av kommunen.
f) Vilken slags information som får bearbetas, lagras, eller kommuniceras i ett system ska framgå av systemdokumentationen för systemet.
g) Informationssystemens skyddsmekanismer och säkerhetsprogramvaror ska hållas uppdaterade och får inte kringgås eller inaktiveras.
h) Användare ska hantera utrustning på ett sätt som minimerar risken för att obehöriga får tillgång till utrustningen, att den stjäls eller går förlorad på annat sätt.
i) Användare får endast installera och använda programvaror eller system som godkänts av Eslövs kommun.
j) Privata e-postadresser får inte användas i yrkesutövningen. I yrkesutövningen ska e-postadress som tilldelats i tjänsten användas. Det är inte tillåtet att vidarebefordra yrkes e-post till enhet som inte är tillhandahållen av Eslövs kommun, t.ex. privat mobil.

k) Patientuppgifter, känsliga personuppgifter och annan information som omfattas av sekretess eller i övrigt är skyddsvärd får inte skickas via e-post, internt eller externt, utan godkänd kryptering.

5.9 Användaridentitet, lösenord, legitimation eller e-Tjänstekort

a) Användaridentiteter, lösenord och e-tjänstekort är personliga och får inte lånas ut.
b) Användare ansvarar för att användaruppgifter (till exempel lösenord och PIN-kod) inte blir kända för andra. I de fall användaruppgifter blir kända för andra ansvarar användaren för att de utan dröjsmål byts i aktuellt system.
c) Vid misstanke om att ett lösenord eller PIN-kod blivit känd för andra ska lösenordet eller PIN-koden ändras. Om ett e-tjänstekort tappats bort ska det omgående rapporteras så att det kan spärras och bytas ut.

5.10 Kontrollåtgärder

a) Information om vad som sker i IT-system och på användares dator loggas. Loggning görs för driftövervakning och felsökning men kan även göras för uppföljning av att interna styrande dokument följs samt för att identifiera hot (t.ex. intrångsförsök och skadlig kod) som kan utgöra en fara för Eslövs kommuns informationstillgångar.
b) För e-post finns loggar om bland annat mottagare, avsändare, tidpunkt och ämnesrad. För internetanvändning loggas interna och externa IP-adresser samt tidpunkt.
c) Kontroller kan ske av tekniska och säkerhetsmässiga skäl för att ta fram statistik eller för att utreda misstanke om brott, misstanke om att användaren brutit mot interna styrande dokument samt misstanke om att arbetstagaren allvarligt missbrukat arbetsgivarens förtroende. Verksamhetschef beslutar i enskilda ärenden om kontroll. Vid behov kan samråd ske med kommunens jurist och/eller HR.
d) Under vissa omständigheter kan arbetsgivaren behöva komma åt innehållet i en enskild medarbetares hemmakatalog. Dessa tillfällen kan vara att medarbetaren slutat och inte överlämnat handlingar som Eslövs kommun behöver, handling begärs ut och handlingen finns i medarbetarens hemmakatalog och medarbetaren är otillgänglig eller det finns misstanke om brott, både mot lagstiftning och interna styrande dokument som gör att arbetsgivaren behöver åtkomst till hemmakatalogen. Förvaltningschef beslutar i enskilda ärenden om

kontroll. Vid behov kan samråd ske med kommunens jurist och/eller HR.

e) Anslutning till Eslövs kommuns nätverk kan stängas av om anslutningen utgör hot mot kommunens informationstillgångar, exempelvis olaga dataintrång, skadlig kod, överbelastningsattack m.m. Innan beslut om avstängning fattas ska riskerna med avstängningen ha analyserats. Beslut om avstängning fattas av Kommundirektör eller den som Kommundirektören delegerat ansvaret till. I ett akut läge kan beslut tas av It chef i samråd med informationssäkerhetssamordnare.

6 Åtkomst till information

6.1 Åtkomst till elektronisk information

a) All tillgång till elektronisk information inom Eslövs kommun ska styras med hjälp av administrativa och tekniska skyddsåtgärder så att endast behöriga, det vill säga de som behöver informationen för sitt arbete, får tillgång till informationen.
b) Behörigheter ska vid varje tillfälle baseras på aktuella arbetsuppgifter.
c) Innan en användare tilldelas åtkomsträttighet ska en behovs- och riskbedömning göras.
d) Tilldelning av åtkomsträttigheter ska dokumenteras och regelbundet följas upp. Detta ska även ske efter varje större organisations- eller systemförändring.
e) Åtkomst med utvidgade rättigheter, så kallade administratörsrättigheter, ska begränsas till så få personer som möjligt och baseras på aktuella arbetsuppgifter.
f) Varje användares identitet ska verifieras. Detta sker genom autentisering, det vill säga verifiering av användarens identitet. Alla användare ska ha en unik identitet. Det grundläggande kravet på utformningen av identiteter är att de ska vara spårbara till en fysisk person.
g) e-Tjänstekort med PIN-kod eller annan godkänd autentisering ska användas för att fastställa en användares identitet. För information med lägre skyddskrav och när det inte är möjligt att använda tvåfaktorsautentisering kan andra metoder användas om riskerna analyserats och bedömts vara acceptabla.

h) Åtkomst ska loggas och tilldelade rättigheter följas upp för att säkerställa att endast behöriga användare har åtkomst till information.
i) Loggar ska vara skyddade mot obehörig åtkomst och manipulation. Loggarna ska omfattas av fastställda rutiner för säkerhetskopiering och arkivering.
j) Systematiska och regelbundna stickprovskontroller av loggar ska göras enligt fastställda styrande dokument. Av dessa ska framgå vad som ska loggas, hur ofta loggarna ska granskas, vem som ska utföra granskningen samt vad som är att betrakta som överträdelse. Vidare ska det finnas regler för hur överträdelser hanteras.
k) För system som innehåller personuppgifter eller uppgifter som omfattas av sekretess, bör loggarna analyseras med hjälp av automatiserade verktyg med koppling till larm när gränsvärden överskrids. Om detta inte är möjligt ska manuella kontroller göras. Extra vikt ska läggas vid uppföljning av konton med höga behörigheter.

6.2 Extern informationsanvändning

a) För informationsanvändare som ges åtkomst till Eslövs kommuns icke-publika informationstillgångar från miljöer utanför Eslövs kommuns kontroll, ska särskilda krav ställas på autentisering av användare och utrustning, liksom på kryptering.
b) Personuppgifter i hälso- och sjukvård (patientuppgifter) eller andra uppgifter med höga skyddskrav ska krypteras med relevant metod och endast vara tillgängliga genom stark autentisering. Undantag kan under vissa förutsättningar göras för kallelser och påminnelser via sms och e-post.

6.3 Styrning av åtkomst till icke digital information

a) Skyddsvärd icke digital information ska omgärdas av skyddsåtgärder vid all hantering, det vill säga kopiering, distribution, förändring, läsning, makulering, förvaring och arkivering.

7 Fysisk och miljörelaterad säkerhet

7.1 Generella regler fysisk säkerhet

c) Nivån på det fysiska skyddet av tillgångar ska baseras på genomförda riskanalyser och stå i proportion till identifierade risker. Grundregeln är att information aldrig ska lämnas oskyddad.

d) System och utrustning som är känslig i sig själv eller behandlar information som omfattas av sekretess eller av andra skäl är känslig, ska placeras så att tillträde minimeras och utformningen av lämpliga skyddsåtgärder underlättas.
e) Kritiska informationstillgångar ska inrymmas i säkra utrymmen.
f) Tillträdeskontroll till viktiga byggnader och lokaler ska finnas, för att säkerställa att endast behörig personal ges tillträde.

7.2 Säkra utrymmen

Med säkra utrymmen avses utrymmen som är speciellt planerade och uppbyggda för att uppfylla höga krav på otillåten åtkomst, skada och störning. Skydd av sådana utrymmen ska utformas i proportion till förekommande risker och ska omfatta skal- och brandskydd, säkerhetsspärrar och tillträdeskontroller.

a) Skalskyddet ska anpassas till säkerhetskrav för tillgångarna inom skalskyddet och resultatet av en riskbedömning/säkerhetsskyddsanalys. Branschnormer ska följas.
b) För att säkerställa att endast behörig personal ges tillträde till säkrade utrymmen, ska dessa skyddas med lämpligt skalskydd och tillträdesbegränsningar.
c) För att möjliggöra loggning av in- och utpasserande ska kontrollsystemen vara kopplade till individuella passagekort eller koder.
d) Elektronisk utrustning är känslig för brand, annan temperaturhöjning och rök. Det är viktigt att ett ändamålsenligt skydd finns i de utrymmen där sådan utrustning finns.
e) Rör, där vatten står under tryck, bör inte finnas i säkra utrymmen. Vätskelarm ska finnas, om det i utrymmet finns rördragningar innehållande vatten, eller om det av andra orsaker finns risk för vattenskada.

7.3 Reservkraft och avbrottsfri kraft

f) System för samhällsviktig verksamhet, verksamhetskritiska system och verksamhetsställen med starkt beroende av elförsörjning ska vara försedda med reservkraft.
g) System och annan elektronisk utrustning bör skyddas mot elavbrott och andra störningar i elförsörjningen. Strömförsörjning av verksamhetskritiska system och utrustningar bör ske via avbrottsfri kraft (UPS), som i sin tur bör anslutas till reservkraft.

h) Tester ska göras regelbundet för att säkerställa att övergången till reservkraft fungerar. Risker rörande den elektromagnetiska miljön bör beaktas.

7.4 Säkerhet för tillgångar utanför egna lokaler

a) Risker i samband med hantering av system och utrustning och andra tillgångar utanför de egna lokalerna ska beaktas och nödvändiga skyddsåtgärder vidtas. Styrande dokument ska fastställas för sådan hantering.

8 Driftsäkerhet

8.1 Generella krav på systemmiljö

a) Eslövs kommun ska som regel ha en systemmiljö med åtskilda produktions-, utvecklings-, test-, acceptanstest-, och utbildningsmiljöer. Säkerhetsreglerna för produktionsmiljöer ska i relevanta delar även gälla för utvecklings- och acceptanstestmiljöer.
b) Systemmiljö för industriella informations- och styrsystem, t.ex. SCADA-system. Dessa system och anslutningar ska vara kartlagda.

8.2 Systemförvaltning

a) För att upprätthålla säker och tillförlitlig tillgång till information, ska administration, drift och underhåll av system ske på ett strukturerat och systematiskt sätt, enligt en fastställd modell för systemförvaltning.
b) System ska ha fastställda och aktuella rutiner för administration, drift och underhåll, dokumenterade i en systemförvaltningsplan. Planen ska säkerställa att systemen hanteras på ett enhetligt och informationssäkerhetsmässigt korrekt sätt och att beroendet av enskilda personers kunskaper minskas.
c) Beskrivning av systemets ändamål och kraven utifrån informationssäkerhetsklass ska finnas i systemdokumentationen, hållas aktuella och uppdateras om informationssäkerhetsklassningen ändras.
d) Informationsklassificering och riskhantering ska genomföras regelbundet och innan viktiga förändringar genomförs, för att utvärdera kraven på skydd. Utifrån dessa analyser ska lämpliga skyddsåtgärder vidtas för att fastställd skyddsnivå ska få avsedd effekt. I analyserna ska ingå kontroll av att systemen följer interna och juridiska krav.

8.3 Systemdokumentation

a) Det ska finnas systemdokumentation för varje system. Dokumentationen ska normalt bestå av system-, drift- och användardokumentation.
b) Systemdokumentation ska vara fullständig och aktuell. Ändring i dokumentationen ska ske enligt fastställda rutiner.
c) Det ska finnas en kopia av systemdokumentationen, liksom av andra, för systemets användning och drift, viktiga dokument. Dessa kopior ska förvaras skilda från originalen i annan brandcell eller annan byggnad och de ska vara åtkomliga även om systemet de normalt sett förvaras på är otillgängligt.
d) Delar av systemdokumentationen som innehåller känslig information, till exempel om systemets säkerhetsfunktioner, ska förvaras så att den endast är åtkomlig för behörig personal.
e) I systemdokumentationen ska det framgå hur informationen ska bevaras och gallras samt vilken bevarande- och gallringsplan som gäller för systemet.

8.4 Säkerhetsuppdateringar

a) Leverantörers säkerhetsuppdateringar ska installeras skyndsamt. För att säkerställa att driften inte påverkas negativt ska säkerhetsuppdateringarna testas och analyseras innan de installeras i produktionsmiljön.

8.5 Skydd mot skadlig kod

a) System och utrustning som kan drabbas av skadlig kod, ska skyddas. Kontrollen ska ske obligatoriskt och automatiskt. Skyddsmekanismerna ska automatiskt uppdateras löpande, för att garantera generellt och aktuellt skydd.
b) Förekomst av skadlig kod är att beteckna som informationssäkerhetsincident och ska rapporteras enligt intern rutin.

8.6 Styrning av ändringar i system

a) Ändringar i eller kring ett system ska planeras. Innan ändringsbeslut fattas ska riskbedömning ske.
b) Beslut om ändringar i eller kring ett system ska fattas av systemägaren i enlighet med informationsägarens fastställda krav gällande ändamål och krav på informationssäkerhet. Beslut om ändringar som väsentligen avviker från fastställt ändamål för ett system eller på annat sätt kan påverka informationssäkerheten ska fattas av informationsägaren.
c) Samtliga ändringar ska kunna härledas till en ansvarig beställare.

d) Rutiner ska fastställas för ändringshantering och testning, och ska vara kända av berörda personer. Rutinerna ska även säkerställa att det är möjligt att återgå till läget före ändringen.
e) Ändringar, som bedöms kunna påverka informationssäkerheten, ska testas i separat testmiljö innan de införs i produktionsmiljö.

8.7 Felhantering

a) Allvarliga störningar i produktionsmiljö kräver ofta att åtgärder genomförs omgående och att fastställda rutiner för ändringshantering inte kan följas. Sådana akuta ändringar ska dokumenteras och i efterhand följas upp enligt rutinen för ändringshantering.

8.8 Kapacitetsplanering

a) Kapacitetsplanering som syftar till att förutse och förebygga kapacitets- eller prestandaproblem ska ske. Regelbunden mätning och uppföljning av kapaciteten ska genomföras. Detta är särskilt viktigt för de system som stödjer samhällsviktig eller verksamhetskritisk verksamhet.

8.9 Säkerhetskopiering och återläsning av data

a) Säkerhetskopiering av information och programvara ska utföras regelbundet, med frekvens och omfattning anpassad till verksamhetskrav respektive legala krav.
b) Tester för att återskapa information från säkerhetskopior ska genomföras regelbundet och resultatet ska dokumenteras.
c) Säkerhetskopior och original ska förvaras i olika byggnader eller brandceller och med skyddsåtgärder som överensstämmer med informationens klassificering.

8.10 Driftövervakning

a) System som stödjer samhällsviktig eller verksamhetskritisk verksamhet ska driftövervakas kontinuerligt och händelser ska loggas för att minimera avbrott och andra informationssäkerhetsincidenter. Loggar ska skyddas mot radering, manipulation och obehörig åtkomst.
b) Behovet av och rutiner för loggning och uppföljning av loggar (analys) ska fastställas av informationsägaren. Lagkrav som är tillämpliga på övervakningsaktiviteterna ska följas. Områden som ska övervägas är till exempel behörig åtkomst, privilegierade aktiviteter, obehöriga åtkomstförsök, systemlarm, ändringar eller försök till ändringar av säkerhetsinställningar.

8.11 Drift hos extern part

Innan lagring eller behandling av känsliga personuppgifter eller information som omfattas av sekretess sker hos extern leverantör ska informationsklassificering och riskanalys genomföras. Om personuppgifter ska behandlas som kan leda till en hög risk för de registrerade ska även konsekvensbedömning (DPIA) avseende dataskydd genomföras. Resultatet utgör underlag för beslut av informationsägare om vilka krav som ska ställas på informationshanteringen.

a) När en verksamhet köper en tjänst hos extern part eller förlägger drift av system hos en sådan, ska minst samma regler för informationssäkerhet gälla som när driften hanteras i egen regi.
b) Kraven på informationssäkerhet ska regleras i avtalet mellan parterna och uppföljning av avtalad säkerhetsnivå ska ske. Detta ska göras möjligt genom att i avtalet specificera att Eslövs kommun har rättighet att genomföra revision av informationssäkerheten eller ta del av revisioner som utförs av godkänd tredje part.
c) I en upphandlingsprocess där det i förfrågningsunderlaget eller under uppdragets utförande förekommer säkerhetsskyddsklassificerade uppgifter eller där leverantören kommer att delta i verksamhet med betydelse för Sveriges säkerhet, ska det träffas ett skriftligt säkerhetsskyddsavtal med anbudsgivaren eller leverantören om det säkerhetsskydd som behövs.
d) Risker som följer av beroendet av en viss leverantör ska minimeras och åtgärder vidtas för att hantera konsekvenserna av att en leverantör inte kan fullfölja sitt uppdrag.
e) I avtalet med tjänsteleverantör ska det regleras i vilka format data ska hämtas ut vid avslutande av tjänst.

8.12 Gallring av information och avveckling av informationssystem

a) Gallring av information och avveckling av informationssystem ska ske på ett säkert sätt och i enlighet med dokumenthanteringsplan.
b) I samband med kravställning av informationssystem ska det, i den mån det är möjligt, ingå delar som reglerar hur en framtida avveckling ska hanteras.

9 Kommunikationssäkerhet

a) Om privata verksamheter med egen internetkoppling ska anslutas till Eslövs kommuns nätverk fordras att riskbedömning utförs och att avtal tecknas som reglerar det gemensamma trafikskyddet.
b) Eslövs kommuns nätverk ska vara uppdelat i nätverkssegment för att minimera risken för obehörig åtkomst samt möjliggöra uppdelning i t.ex. åtskilda produktions-, utvecklings- och testmiljöer etc. Utvecklings- och testarbete ska inte kunna störa produktionen.
c) Publika nätverk ska vara logiskt separerade från produktionsnätverk.
d) Sammankoppling av nätverk får endast ske efter genomförd riskanalys och sedan nödvändiga skyddsåtgärder vidtagits av respektive nätverks systemägare. Sammankoppling av nätverk får ske först efter skriftligt beslut.
e) Respektive nätverksägare ansvarar för de skyddsåtgärder som krävs för att motverka avlyssning och förändring av överförd information. Skyddsåtgärderna ska ha sin grund i aktuell informationsklassificering och riskanalys och motsvara det skyddsvärde som informationen har.
f) Respektive nätverksägare ska utifrån informationsägarnas krav på tillgänglighet besluta om nätverksinfrastruktur och val av aktiva nätkomponenter.
g) Respektive nätverksägare ska se till att det finns styrande dokument för anslutning mot nätverket.
h) Nätverk, dess komponenter och systemsamband ska vara dokumenterade och det ska finnas tydliga instruktioner hur dokumentation ska utformas.
i) Fjärranslutningar till system för till exempel fjärrdiagnostik eller fjärrövervakning m.m. ska ske genom Eslövs kommuns nätverk underkontrollerade och säkra former fastställda av respektive systemägare.

10 Anskaffning, utveckling och underhåll av system

10.1 Generella regler

Informationssäkerhetskraven, vid upphandling, ny- och vidareutveckling av system, i egen regi eller i samverkan med samarbetspartner, ska analyseras och definieras utifrån en dokumenterad informationsklassificering och riskbedömning.

a) Vid utveckling och anskaffning av system ska det analyseras vilket skydd systemet kräver och vilka åtgärder som måste vidtas för att skyddet ska få avsedd effekt. Kraven på systemet ska tydligt framgå i kravspecifikationen.
b) Innan ett system tas i drift ska informationen som ska hanteras i systemet vara klassificerad enligt gällande rutin för informationsklassning samt klassificeringsmodell.
c) Ett system ska, innan det tas i drift, ha godkänts av den eller de informationsägare vars information ska hanteras i systemet.
d) All anskaffning, utveckling, förändring och avveckling av IT-system ska ske i enlighet med beslutad förvaltningsmodell

10.2 Systemutveckling

a) Det ska i systemutvecklingsarbete tillses att dokumenterade modeller för systemutveckling och projektstyrning finns och tillämpas.
b) I systemutvecklingsarbete ska system, programvara och informationstillgångar skyddas på motsvarande sätt som de färdiga produkterna. Produktionsmiljöer ska skyddas.
c) Information i samband med systemutveckling ska skyddas enligt samma principer som övrig verksamhetsinformation. Testmiljö ska, om inte särskilda skäl föreligger, inte innehålla produktionsdata.
d) Styrande dokument för acceptanstest, driftgodkännande och produktionssättning ska finnas och tillämpas. System ska genomgå acceptanstest före godkännande. I godkännandet ska det ingå en uppföljning av säkerhetskraven. Ett beslut ska fattas om eventuella avvikelser hindrar en produktionssättning och inom vilken tidsram de ska åtgärdas. Är systemet godkänt kan det därefter överlämnas för driftsättning. Driftgodkännande ska ske av respektive informationsägare.

10.3 Upphandling av system och systemutveckling

a) För upphandling som innefattar hantering av säkerhetsskyddsklassificerade uppgifter finns krav utifrån lagstiftning (säkerhetsskyddslagen) som ska följas.
b) Avtal ska utformas så att Eslövs kommun erhåller fullständig förfoganderätt till allt kundunikt arbete och material som leverantören tar fram särskilt för beställaren i samband med uppdrag.
c) För att möjliggöra och bibehålla kontinuitet och fortsatt utveckling av viktiga tjänster ska Eslövs kommun, vid behov, avtala om att få tillgång till källkoden om vissa förutsättningar är uppfyllda som exempelvis att

leverantören går i konkurs, om nyckelpersoner som utvecklat programmet lämnar leverantören eller om leverantören missköter sitt utvecklings- eller underhållsåtagande. I ett sådant Källkodsdepositionsavtal ska leverantören åta sig att deponera aktuell källkod hos en oberoende tredje part som under vissa förutsättningar ger kommunen tillgång till källkoden. Eslövs kommun ges då möjlighet att själv underhålla och uppdatera det aktuella IT-systemet.

11 Informationssäkerhetsincidenter

11.1 Hantering av informationssäkerhetsincidenter

a) Informationssäkerhetsincidenter ska hanteras enligt fastställda rutiner.
b) Incidenter som kräver rapportering till tillsynsmyndighet ska rapporteras till dessa inom givna tidsramar.
c) Medarbetare ska rapportera avvikelser som kan utgöra ett hot mot Eslövs kommuns informationstillgångar.
d) Vid utredning av en incident ska information samlas in på ett sådant sätt att det inte finns risk att bevis förstörs.

11.2 NIS incidenter

Hanteras enligt rutin för rapportering av NIS incidenter. Gäller verksamheter som omfattas av NIS direktivet.

12 Verksamhetens kontinuitet

12.1 Generella regler

a) Informationssäkerhet ska vara en integrerad del av den överordnade processen för verksamhetens kontinuitetsplanering. Processen ska behandla nödvändiga informationssäkerhetskrav som behövs för verksamheten i kontinuitet.
b) I verksamhetens kontinuitetsplan ska det behandlas hur verksamheten ska bedrivas vid avsaknad av kritiska funktioner och informationstillgångar samt hur återgång till normalläge ska ske.
c) Kontinuitetsplaner och återstartsplaner skall finnas för all information och alla system som klassats i tillgänglighetsklass T2 eller högre enligt Eslövs kommuns rutin för klassning samt informationsklassificeringsmodell. Planer kan vara gemensamma för flera verksamheter och flera system och ska innehålla fastställda prioriteringsordningar för återgång till normalläge.

d) Målet med kontinuitetsplaneringen ska vara att kritiska verksamheter ska kunna upprätthållas, på rimlig nivå, vid olika typer av katastrofsituationer, störningar och oplanerade avbrott. De delar av kontinuitetsplaneringen som berör katastrof- och beredskapssituationer ska ingå i verksamhetens övriga katastrofplanering.
e) Det ska finnas fastställda och aktuella reservrutiner för katastrofsituationer, störningar eller oplanerade avbrott. Rutinerna kan vara såväl manuella som IT-baserade.
f) Kontinuitetsplanerna ska testas regelbundet, enligt fastställd plan samt efter större organisationsförändringar. Planerna ska underhållas genom regelbundna granskningar och övningar, för att säkerställa att de är aktuella och ändamålsenliga.

13 Uppföljning och efterlevnad

a) Förvaltningar ska löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.
b) Förvaltningar ska regelbundet granska sin informationssäkerhet. Baserat på genomförda granskningar och identifierade avvikelser ska skyddsåtgärder vidtas.
c) Informationssäkerhetssamordnaren ska årligen, enligt årshjul följa upp informationssäkerhetsarbetet.