KS § 51 Dnr KS/2021:251 – 003

Riktlinje för informationssäkerhet i Strängnäs kommun

Beslut

Kommunstyrelsen föreslår kommunfullmäktige besluta att

1. anta riktlinje för informationssäkerhet i Strängnäs kommun enligt förslag daterat 2024-02-21.

Beslutsgång

Ordföranden finner att det endast finns ett förslag till beslut och att detta blir kommunstyrelsens beslut.

Beskrivning av ärendet

Information är en av Strängnäs kommuns viktigaste tillgångar och en förutsättning för att verksamhet ska kunna bedrivas. Riktlinje för informationssäkerhet i Strängnäs kommun ska skapa förutsättningar för kommunens systematiska och riskbaserade arbete och ska vara en del av LIS (Ledningssystem för informationssäkerhet) och tillhöra kommunens ledningssystem. Den är en övergripande ram för området och utgår från standarden för informationssäkerhet SS-EN ISO/IEC 27001/27002. Nämnda standard är detsamma som ligger till grund för det metodstöd MSB har och mot vilket myndigheter, regioner och kommuner lutar sitt informationssäkerhetsarbete.

Arbetet med att öka förståelsen och skyddet av kommunens information som pågått under några år har eskalerats med anledning av omvärldsläget. Förslag till kommande lagstiftning (SOU 2024:18) pekar på utökat kommunalt ansvar då kommunen som helhet med hög sannolikhet kommer att omfattas av lagstiftningen som kommer att kallas för ”Cybersäkerhetslagen”. Strängnäs kommun kommer då att räknas som ”väsentlig entitet” vilket bland annat innebär att tillsynen kommer att vara proaktiv varför delarna från ISO-standarden enligt ovan, kommer behöva vara implementerade till det föreslagna datumet för lagens införande 2025-01-01.

En riktlinje för informationssäkerhet måste finnas för att stötta arbetet med informationssäkerhet till att vara en del av verksamhetens ledningssystem. För uppföljning av status behövs systemstöd för riskhantering, klassning, säkerhetsåtgärder med mera.

Ekonomiska konsekvenser för kommunen

För att Strängnäs kommun ska kunna hantera risker i samtliga ledningssystem och för hela organisationens livscykel, behövs stöd i form av

standarddokumentation (Svensk standard ISO). Utöver systemet Klassa (SKR) som kan komma att omfattas av LOU med anledning av att det blir avgiftsbelagt, kommer även systemstöd för utbildningsinsatser att krävas. Här förespråkas extern hjälp med utbildningar och material som är kopplat till aktuell omvärldsbevakning inom informations- och cybersäkerhet. Vidare medför ISO-standarden krav om bland annat rutiner för hot- och logganalys. Det senare kan hanteras med hjälp av systemstöd vilka måste innehålla möjlighet till uppföljning.

Kostnad för införande av systemstöd enligt kravbild är ca 2,5–3,5 miljoner kronor. Vidare tillkommer en årlig kostnad som uppskattas till ca 500 000 – 800 000 kronor.

Övriga konsekvenser
Beslutet medför inga övriga konsekvenser.

Uppföljning
Uppföljning sker årligen och nytt beslut fattas vid behov.

Beslutsunderlag
Tjänsteutlåtande, Antagande av riktlinje för informationssäkerhet, 2024-02-21
Styrdokument, Riktlinje för informationssäkerhet i Strängnäs kommun, förslag, 2024-02-21

Beslutet skickas till
Kommunfullmäktige
Barn- och utbildningsnämnden för kännedom
Kulturnämnden för kännedom
Miljö- och samhällsbyggnadsnämnden för kännedom
Socialnämnden för kännedom
Teknik- och fritidsnämnden för kännedom
Valnämnden för kännedom
Strängnäs kommunföretag AB
SEVAB Strängnäs Energi AB
Strängnäs Fastighets AB
Kommunrevisionen för kännedom

Beslutad:	åååå-mm-dd § xx
Myndighet:	Kommunfullmäktige
Diarienummer:	KS/2021:251 - 003
Ersätter:	-
Gäller för:	Alla nämnder och förvaltningen
Gäller fr o m:	20xx-xx-xx
Gäller t o m:	Tills vidare
Dokumentansvarig:	Kansliavdelningen/Säkerhetsenheten
Uppföljning:	Årligen/Vid behov

Riktlinje för informationssäkerhet i Strängnäs kommun

1. Inledning

1.1
Dessa riktlinjer konkretiserar Strängnäs kommuns policy för Informationssäkerhet och är styrande för skyddet av informationstillgångar[1] som hanteras inom Strängnäs kommun.

1.1.2 Syfte och omfattning
Syftet med riktlinjen är att skapa förutsättningar för hur ett systematiskt och integrerat arbete med informationssäkerhet ska ske inom Strängnäs kommun, nämnder och kontor.

1.1.3 Tillämpning av regelverket
För att underlätta tillämpning av regelverket ska kommunstyrelsen ge ut tillämpningsanvisningar som förtydligar hur, det praktiska arbetet med att följa riktlinjerna, ska gå till. Arbetet med framtagande av tillämpningsanvisningar för informationssäkerhet delegeras till säkerhetsavdelningen.

Detta dokument ska utvärderas och revideras varje år och redovisas vid ledningens genomgång[2].

1.1.4 Baseras på internationell standard
Riktlinjerna utgår från internationell standard (SS-EN ISO/IEC 27001/27002) för styrning och implementering av informationssäkerhet i form av ett s.k. Ledningssystem för Informationssäkerhet[3]. MSB (Myndigheten för samhällsskydd och beredskap) har tagit fram ett metodstöd som bygger på denna ISO-standard som myndigheter, regioner och kommuner använder i sina ledningssystem.

1.2 Strängnäs kommuns styrande dokument för informationssäkerhet

1.2.1 Styrande dokument
Varje nämnd, bolag och kontor ska, inom ramen för Strängnäs kommuns övergripande ledningssystem för informationssäkerhet, styra och leda sitt informationssäkerhetsarbete i ett ledningssystem inom sitt verksamhetsområde.

---

[1] Informationstillgångar innefattar enligt MSB information och resurser som hanterar information.

[2] Se 16.1.

[3] I MSB:s metodstöd förkortas Ledningssystem för Informationssäkerhet till LIS. Med risk för sammanblandning av kommunens ledningsinformationssystem för beslutstöd och verksamhetsstyrning som nu förkortas LIS väljer vi att inte förkorta Ledningssystem för Informationssäkerhet utan vi skriver ut det i sin helhet. På engelska benämns detta som ”ISMS” och står för Information Security Management System.

Det lokala ledningssystemet ska säkra ett systematiskt informationssäkerhetsarbete och en riskavvägd skyddsnivå i verksamheten, och vara en integrerad del i verksamheternas ordinarie ledningsarbete.

1.2.1 Styrande dokument på övergripande nivå

Styrdokumenten består av Strängnäs kommuns informationssäkerhetspolicy, Riktlinje för informationssäkerhet och tillämpningsanvisningar för informationssäkerhet.

1.3 Styrning

1.3.1 Efterlevnad

Riktlinjerna är bindande och ska efterlevas av samtliga nämnder och kontor inom Strängnäs kommun.

1.3.2 Ansvar

Ansvaret för informationssäkerheten är kopplat till verksamhetsansvaret i alla led. Det betyder att varje nämnd eller kontor och varje medarbetare som är ansvarig för en verksamhet också har att ansvara för informationssäkerheten i respektive verksamhet.

1.3.3 Informationshantering som läggs ut på extern part

I de fall nämnder uppdrar åt andra att hantera information ska avtalet om denna hantering omfatta sådana krav att informationen hanteras i enlighet med dessa riktlinjer. Den nämnd som avtalar med annan part om hantering av information ansvarar också för en uppföljning av utförandet och de avtal som ligger till grund för utförandet, så att informationen ges ett avtalsenligt skydd.

1.3.4 Förvaltningschefens ansvar

Förvaltningschefen (kommundirektören) ansvarar inför nämnden eller styrelsen för arbetet med informationssäkerhet. Det löpande arbetet samordnas och följs upp av informationssäkerhetssamordnaren.

1.3.5 Säkerhetsåtgärder

Utformning av säkerhetsåtgärder i enlighet med dessa riktlinjer ska anpassas utifrån organisation, uppdrag, hotbild och sårbarheter.

1.4 Planering

1.4.1 Systematisk arbete

Inom Strängnäs kommun ska ett riskbaserat systematiskt och långsiktigt arbete bedrivas för att skydda informationstillgångar.

1.4.2 Lokal handlingsplan för informationssäkerhet

En lokal handlingsplan för informationssäkerhet ska finnas vid varje nämnd. Av handlingsplanen ska framgå vilka prioriteringar och initiativ som görs avseende informationssäkerhet under innevarande år, med en inriktning för följande tre år. Planen ska årligen uppdateras med utgångspunkt i den systematiska uppföljningen med aktuella hot och sårbarheter.

2. Informationssäkerhetsråd

2.1 Samordning av informationssäkerhetsarbetet

För att samordning och uppföljning av informationssäkerhetsarbetet ska kunna bedrivas effektivt ska det finnas ett informationssäkerhetsråd[4] inom Strängnäs kommun. Rådet leds av informationssäkerhetssamordnaren. Utöver denne ska rådet bestå av informationssäkerhetsansvariga/kontakter inom varje kontor, avdelning och nämnd.

2.2 Rådets uppgift

Rådet ska vara stödjande i arbetet med informationssäkerhetsfrågor. Rådet ska främja erfarenhets- och kunskapsutbyte, bevaka vilket behov av stöd som finns i verksamheterna och föreslå förbättringar samt förankra och samordna informationssäkerhetsaktiviteter.

[4] Kan med fördel vara nuvarande GDPR-samordnare eftersom dataskydd (GDPR) är en del av informationssäkerheten.

3. Bedömning och hantering av risker

Strängnäs kommuns informationstillgångar ska skyddas oavsett vilken form de *har. Om det visar sig att skyddet kan kringgås är det viktigt att verksamheten har* en förmåga att upptäcka detta. Därför ska medarbetare inom Strängnäs kommuns nämnder, kontor och avdelningar ha den kunskap som behövs om hur de kan agera för att förebygga och hantera risker i den dagliga verksamheten. Denna kunskap uppnås bland annat genom ett systematiskt arbete med riskanalyser – ett så kallat ”strukturerat riskbaserat arbetssätt”.

3.1 Riskbedömning och riskhantering

3.1.1 Bedömning av risker som kan påverka informationstillgångar

Nämnder, kontor och avdelningar ansvarar för att analyser genomförs för verksamheter samt IT-system/IT-miljö och infrastruktur avseende vilka risker som kan påverka deras informationstillgångar. Med utgångspunkt i denna bedömning ska beslutas hur riskerna ska hanteras och nödvändiga åtgärder vidtas för att upprätthålla rätt skyddsnivå för informationen. En gemensam metod och mallar för riskanalys kommer att finnas tillgängliga centralt på intranät (länk i fotnot[5]).

3.1.2 Kontinuerlig process

Riskbedömning och riskhantering ska vara en kontinuerlig process och stödja informationssäkerhetsarbetet. Riskbedömningar ska revideras regelbundet (årligen) eller när förutsättningarna förändras.

3.1.3 Internkontroll

Riskbedömning och riskhantering ska genomföras i enlighet med vad som anges i Strängnäs kommuns ”Riktlinjer för internkontroll[6]”.

3.1.4 Riskanalys

Varje nämnd, kontor och avdelning ska minst årligen genomföra en riskanalys för att identifiera de största riskerna mot de informationstillgångar som hanteras. Dessa analyser ska dokumenteras. Eventuella förändringar av säkerhetsåtgärder ska dokumenteras för uppföljning.

---

[5] Länk till intranätsida - Informationssäkerhet | Intranät - Strängnäs kommun (strangnas.se)

[6] Diarienummer KS/2019:680-003.

4. Organisation och ansvar för informationssäkerhet

4.1 Roller och ansvar på övergripande nivå i Strängnäs kommun

Kommunstyrelsen ansvarar för uppsikt över nämndernas och bolagens arbete med informationssäkerhet samt för analys, ledning och samordning inom området.

Kommunstyrelsen har mandat att fatta beslut om åtgärder för att skydda kommunens informationstillgångar vid misstanke om eller vid informationssäkerhetsincident som bedöms kunna leda till allvarlig skada.

Under kommunstyrelsen ska det finnas en säkerhetschef för Strängnäs kommun som samordnar och följer upp kommunens informationssäkerhetsarbete. Säkerhetschefen ska ha möjlighet att rapportera större avvikelser i arbetet med informationssäkerhet till kommunstyrelsen. Säkerhetschefen svarar för utbildning och stöd till informationssäkerhetssamordnaren.

4.1.1 Informationssäkerhet för medarbetare med flera

Det operativa arbetet med kommunens informationssäkerhet ska genomföras i alla verksamheter. Samtliga medarbetare och förtroendevalda ska följa riktlinjen. Leverantörer och konsulter ska i berörda delar också följa riktlinjen.

5. Hantering av informationstillgångar

5.1 Värdering och skydd av information

Nämnder, kontor och avdelningar ansvarar för att informationstillgångar identifieras och värderas utifrån sitt skyddsbehov (vilken skada som kan uppstå) genom ett riskbaserat arbetssätt.

5.2 Skydd av informationstillgångar

Informationstillgångarna ska klassas utifrån gemensamt framtagen klassningsmodell med hänsyn till att informationen ska finnas tillgänglig när den behövs (tillgänglighet), att den är skyddad mot obehörig förändring (riktighet) och att obehöriga inte kan få tillgång till informationen (konfidentialitet). Skyddet av informationstillgångarna ska utformas så att efterlevnad av styrande regelverk uppnås samt med hänsyn till verksamheternas riskacceptans.

5.3 Information om skyddsvärde

Innan informationstillgångar överlämnas till behörig ska mottagaren informeras om informationstillgångarnas skyddsvärde avseende konfidentialitet.

6. Åtkomst till informationstillgångar

6.1 Autentisering (identifiering av personer och system)

Alla utställda identiteter i ett IT-system ska vara unika över tid. Åtkomsten ska vara spårbar till en fysisk person eller ett IT-system.

6.2 Åtkomstkontroll till informationstillgångar

Behörighet till informationstillgångar ska baseras på användarens aktuella arbetsuppgifter och organisatoriska tillhörighet. Användaren ska endast ges åtkomst till de informationstillgångar som behövs för att kunna utföra arbetet.

7. Kryptering[7]

Kryptering ska användas för att skydda information från att kunna läsas om den kommer i orätta händer. Kryptering kan också användas för att skydda information från obehörig förändring.

7.1 Etablerade algoritmer och nyckellängder

Vid kryptering av information ska etablerade och pålitliga algoritmer samt nyckellängder användas.

7.2 Etablerade kryptografiska protokoll

Vid kryptering vid informationsöverföring ska etablerade kryptografiska protokoll användas och konfigureras enligt god standard.

7.3 Skyddsåtgärder för kryptonycklar

Vid kryptering ska det finnas administrativa och tekniska skyddsåtgärder som säkerställer att krypteringsnycklar hanteras säkert över sin livscykel.

---

[7] För mer och utförligare information kring kryptering och godkända algoritmer se dokumentet ”Anvisning för kryptering - IT”. För användare som behöver bedöma om information ska krypteras – se ”Anvisning för kryptering – medarbetare”.

8. Fysisk säkerhet

Tillträdeskontroll, skalskydd och brandskydd handlar om hur informationstillgångar (inklusive IT-system) ska skyddas, både i egna lokaler och vid inhyrning i andras lokaler.

8.1 Generellt om fysisk säkerhet

Utrymmen som innehåller informationstillgångar ska ha ett fysiskt skydd som utformas och dimensioneras utifrån tillgångarnas värde, identifierade risker (riskbaserat systematiskt arbetssätt) och styrande regelverk.

8.2 Skalskydd och tillträdeskontroll

Utrymmen som innehåller informationstillgångar ska skyddas genom åtgärder som säkerställer att endast behöriga får tillträde till tillgångarna.

8.3 Skydd mot angrepp, olyckor och naturkatastrofer

Utrymmen som innehåller informationstillgångar (och informationsbehandlingsresurser) ska ha ett fysiskt skydd mot naturkatastrofer, angrepp från hotaktörer eller olyckor som är anpassat till tillgångarnas värde.

9. Driftsäkerhet

För att undvika störningar och driftstopp i Strängnäs kommuns IT-system krävs en förvaltning och drift med etablerade rutiner för till exempel driftsättning, säkerhetskopiering, proaktiv hotanalys och loggning.

9.1 Rutiner för drift och förvaltning

Ägare av IT-system och nätverk ansvarar för att administration, drift och underhåll av IT-system sker på ett strukturerat och spårbart sätt. Ägare av IT-system som innehåller information där förlust av konfidentialitet, riktighet eller tillgänglighet med allvarlig skada riskerar att ske ska tillse att det finns en kontinuerlig övervakning under systemets driftstid/öppettid för att proaktivt upptäcka och åtgärda fel, minimera avbrott och förebygga IT-incidenter. Detta styrs med krav på säkerhet i enlighet med informationens nivå samt prioritering av verksamhet.

9.2 Systemdokumentation

Ägaren av IT-system ansvarar för att IT-systemet är dokumenterat i en centralt för kommunen placerad konfigurationsdatabas[8] (engelska CMDB Configuration Management Database). Dokumentationen ska ge tillräckligt stöd för strukturerad och säker drift och förvaltning. Ägaren av IT-system (systemägare) och informationsägare ska säkerställa att användarna får kunskap om vilken typ av information som får hanteras i ett IT-system och eventuella regler kring denna hantering. En CMDB är även en nödvändighet att tillgå vid incidenthantering för att spåra och förstå vilka system som påverkas. En CMDB måste därför förvaltas och alltid vara uppdaterad.

9.3 Säkerhetsloggning

Ägaren av IT-system ansvarar för att händelser som kan ha betydelse för säkerheten i IT-systemet eller IT-miljön i Strängnäs kommun loggas i enlighet med säkerhetskrav för klassningsnivå på informationen. Av denna säkerhetslogg ska tidpunkt och annan för händelsen relevant information framgå.

9.4 Säkerhetsloggar för hotanalys

Ägare av IT-system ska, då Strängnäs kommun efterfrågar detta, tillgängliggöra sådana säkerhetsloggar som behövs för att kunna upptäcka och utreda hot mot och sårbarheter i skyddet av Strängnäs kommuns IT-infrastruktur.

---

[8] Dokumentation av konfigurationer är en teknisk säkerhetsåtgärd och ett krav i ISO 27001, 8.9.

9.5 Klocksynkronisering
Samtliga IT-system ska ha korrekt tidsangivelse genom klocksynkronisering. Detta bland annat för en snabbare hantering vid logganalyser.

9.6 Information om loggning till medarbetarna
Samtliga medarbetare ska informeras av sina respektive arbetsställen om att användning av IT-system loggas och att loggarna kan granskas för att undersöka IT- och cybersäkerhetsrelaterade sårbarheter och hot riktade mot Strängnäs kommuns informationstillgångar och IT-miljö.

9.7 Säkerhetsuppdateringar
Leverantörers säkerhetsuppdateringar ska installeras skyndsamt i IT-system.

9.8 Supporterade delkomponenter
Ägare av IT-system ska säkerställa att endast IT-system används där alla delkomponenter fortfarande supporteras av respektive leverantör. Om detta inte är möjligt ska riskerna reduceras till en fördefinierad acceptabel nivå.

9.9 Skydd mot skadlig kod
Ägaren av IT-system ska säkerställa att behovet av skydd mot skadlig kod i IT-systemet är analyserat. I de fall behov av skydd mot skadlig kod finns ska ägaren av IT-systemet säkerställa att sådant skydd implementeras.

9.10 Styrning av ändringar i IT-system
Det ska finnas rutiner för ändringshantering och testning av IT-system.

9.11 Säkerhetskopiering och återläsning av data
Säkerhetskopiering av informationstillgångar (inklusive programvara) ska utföras regelbundet, med frekvens och omfattning anpassad till verksamhetskrav respektive legala krav, enligt fastställd instruktion.

9.12 Återskapa information från säkerhetskopia
Tester för att återskapa information från säkerhetskopior ska genomföras regelbundet och resultatet ska dokumenteras. För information som behövs för verksamhets förmåga att utföra sitt uppdrag ska kontroll ske minst en gång per år att uppgifterna på säkerhetskopiorna går att återskapa inom den tidsrymd som verksamheten kontinuitetsplanering kräver.

9.13 Förvaring

Säkerhetskopior och original ska alltid förvaras fysiskt åtskilda.

9.14 Härdning av IT-system

Härdning (säkerhetskonfigurering av IT-system) ska ske genom att det som inte behövs för IT-systemets definierade funktion ska vara begränsat avseende åtkomst, avstängt eller borttaget ur IT-systemet.

10. Kommunikationssäkerhet

En viktig förutsättning för att skydda Strängnäs kommuns IT-system är att det finns bra skyddsåtgärder i nätverken samt kontroll över vilken kommunikation som sker i nätverken.

10.1 Generella skyddsåtgärder i nätverk

Ägaren av nätverk ansvarar för att nätverk förses med skyddsåtgärder för att motverka obehörig åtkomst.

10.2 Fysisk eller logisk separation

Ägaren av nätverk ansvarar för att nätverk delas upp genom fysisk eller logisk separation. Avgränsningen ska vara tydlig och dokumenterad.

10.3 Gästnätverk

Användare med IT-utrustning som inte är kontrollerad eller godkänd av Strängnäs kommun får endast anslutas till kommunens gästnätverk.

10.4 Skyddsåtgärder i trådlösa nätverk

Trafik i trådlösa nätverk ska krypteras.

11. Utveckling, anskaffning och underhåll av IT-system

Informationssäkerhet ska hanteras under ett IT-systems hela livscykel. Därför är det viktigt att dessa frågor hanteras i ett tidigt skede. Hur kravställning och avtalsskrivning ska gå till i samband med upphandling beskrivs i nästa kapitel.

11.1 Anskaffning av IT

När en verksamhet köper IT som tjänst hos extern part (exempelvis en SaaS-, IaaS- eller PaaS-tjänst[9]) eller förlägger drift av IT-system hos en sådan part, ska minst samma regler för informationssäkerhet gälla som när driften hanteras i egen regi.

11.2 Systemutvecklingsprojekt

Informationssäkerhet ska hanteras i systemutvecklingsprojekt genom dokumenterade modeller för systemutveckling och projektstyrning.

11.3 Test

Instruktioner för acceptanstest, driftgodkännande och produktionssättning ska finnas och tillämpas inom Strängnäs kommun.

[9] SaaS står för Software as a Service, IaaS - Infrastructure as a Service och PaaS – Platform as a Service..

12. Leverantörsrelationer

Det är viktigt att Strängnäs kommuns informationstillgångar har samma skydd även då de hanteras av en leverantör eller underleverantör.

12.1 Kravställning

Innan anskaffning ska analys ske av vilka krav avseende informationssäkerhet som ska ställas.

12.2 Säkerställa skydd

Kraven som ställs i samband med anskaffning ska säkerställa skyddet för de informationstillgångar som leverantören eller leverantörens produkter kommer att hantera.

12.3 Upprättande och förvaltning av avtal

Vid upprättande av avtal med extern leverantör som ska hantera informationstillgångar åt verksamheten ska kraven på informationssäkerhet regleras.

12.4 Hantering av händelser

Avtalet ska specificera hur händelser som rör informationssäkerhet ska hanteras då de uppstår hos leverantören relaterat till de informationstillgångar de hanterar åt kommunen.

12.5 Avvikelser mot krav

Avtalet ska specificera vad som händer om leverantören inte följer de krav som ställts gällande informationssäkerhet.

12.6 Rätt till revision

Avtalet ska specificera att kommunen har rättighet att genomföra revision av informationssäkerheten.

12.7 Minimera risk av beroende

Risker som följer av beroendet av en leverantör ska minimeras och åtgärder vidtas för att hantera konsekvenserna av att leverantören inte kan fullfölja sitt uppdrag.

12.8 Samhällsviktiga tjänster

Vid upphandling av IT-system eller tjänst för samhällsviktiga tjänster ska riskbedömning göras avseende beroenden för hela leverantörskedjan som exempelvis leverantör och underleverantörer.

13. Informationssäkerhetsincidenter

När en allvarlig händelse inträffar som påverkar informationssäkerheten är det viktigt att snabbt agera för att begränsa eller avvärja konsekvenserna av händelsen. Störningar kan ha flera orsaker och kan snabbt komma att påverka många delar av verksamheten men också andra aktörer i samhället.

13.1 Hantering av informationssäkerhetsincidenter

Nämnder och förvaltning ansvarar för att det finns processer och rutiner för att hantera incidenter och sårbarheter som kan utgöra hot mot Strängnäs kommuns informationstillgångar inom respektive verksamhets ansvarsområde.

13.2 Analys av IT-utrustning

Strängnäs kommun ska ha förmåga att genomföra analys av IT-utrustning i de fall då utrustningen misstänks utgöra ett hot mot kommunens IT-miljö eller informationstillgångar.

13.3 Incidentrapportering

Incidentrapportering ska ske till tillsynsmyndighet i enlighet med tillämpliga lagar och dokumenteras. Resultat av kommunens incidenthantering och det totala antalet rapporterade incidenter ska månadsvis rapporteras till säkerhetsavdelningen.

14. Kontinuitetshantering

Verksamhet ska kunna fortsätta även om t.ex. IT-system slås ut, en strömkabel grävs av eller byggnader brinner ner. Därför är det viktigt att planera för hur verksamheten ska fungera om det händer någonting av allvarlig karaktär.

14.1 Generella regler för kontinuitetsplanering

Informationssäkerhet ska vara en integrerad del av den överordnande processen för verksamhetens kontinuitetsplanering. Processen ska behandla nödvändiga informationssäkerhetskrav som behövs för verksamhetens kontinuitet.

15. Spridning

15.1 Information och implementation

Kommunstyrelsen ansvarar för att informera om och implementera riktlinjen. Nämnder och bolagsstyrelser ansvarar för att riktlinjen tillämpas i den egna verksamheten.

16. Uppföljning

16.1 Ledningens genomgång

Varje nämnd ska följa upp att riktlinjen följs och att den är relevant. Eventuella synpunkter ska delges kommunens informationssäkerhetssamordnare. Kommunstyrelsen följer upp arbetet utifrån riktlinjen i samband med den s.k. ledningens genomgång vilken är en obligatorisk årligt återkommande genomgång av kommunens Ledningssystem för Informationssäkerhet.

17. Relaterade dokument

- Informationssäkerhetspolicy
- Tillämpningsanvisningar

18. Begrepp

Tabell 1. Begrepp

Härdning	För att minska exponeringen ska informationssystem ha så få aktiva tjänster, protokoll och nätverkskopplingar som möjligt. De tjänster, protokoll och nätverkskopplingar som inte behövs för informationssystemets funktion ska stängas av, tas bort eller blockeras.
Informationsbehandlingsresurs	Digital eller fysisk resurs för behandling av information. Vanligtvis digital (till exempel IT-system, tjänst, infrastruktur), men kan även vara en fysisk resurs (t.ex. ett säkerhetsskåp eller en människa).
Informationstillgång	MSB:s definition: Information och resurser som hanterar information. Exempel på informationstillgångar: (kunddatabas, metodik, dokument, applikationer, operativsystem, abonnemang, datorer, lokala nätverk, personers kompetens, rykte och image etcetera).
IT-system	Kombination av operativsystem, data-baser, serverbaserade program samt program för datakommunikation, IT--säkerhet och annat som tillsammans är en förutsättning för att man ska kunna utföra arbetsuppgifter med dator på en arbetsplats.