SALA KOMMUN

VÅRD- OCH OMSORG
Kirsi Kirpislidis

Vård- och omsorgsnämnden

MISSIV

UPPRÄTTADE STYRDOKUMENT – INFORMATIONSSÄKERHETSPOLICY OCH RIKTLINJE FÖR INFORMATIONSSÄKERHET

Sammanfattning av ärendet

För Vård och omsorgsnämndens verksamhet ställs det upp nationella krav i lagstiftning om en Informationssäkerhetspolicy som tydliggör hur verksamheten hanterar informationstillgångar. Det finns även krav på Säkerhetspolicy för hanteringen av personuppgifter både för Vård och omsorgsnämndens och övriga kommunens verksamheter. Upprättad informationspolicy uppfyller de krav som ställs i lagstiftningen på Informationssäkerhetspolicy och Säkerhetspolicy.

Policyn är ett övergripande dokument som beskriver kommunens mål och viljeinriktning, definierar viktiga begrepp samt tydliggör kommunens säkerhetsstrategi. För att förvaltningens olika verksamheter ska kunna arbeta likriktat och effektivt har policyn kompletterats med en riktlinje som mer ingående beskriver hur organisationen bör se ut, hur ansvaret fördelas samt de olika delarna som ska ingå i arbetet med informationssäkerhet.

Vid genomgången visas en film för ledningen som förklarar nyttan med att arbeta för en bra informationssäkerhet från: www.informationssäkerhet.se. Följ länken:

https://www.informationssakerhet.se/sv/kompetensutveckling/Filmer/Kommunledning/

Förslag till beslut

Nämnden föreslås besluta

Att överlämna Informationssäkerhetspolicy och Riktlinjen för informationssäkerhet till kommunfullmäktige för fastställande

Kirsi Kirpislidis
Kvalitetshandläggare

Bilagor: Informationspolicy; Riktlinje för Informationssäkerhet

SALA KOMMUN
Vård- och omsorg
Box 304
733 25 Sala

Besöksadress: Fredsgatan 23, Sala
Växel: 0224-74 70 00
Fax: 0224-192 98
vard.och.omsorgsforvaltningen@sala.se
www.sala.se

Bilaga VON 2015/18/4

SALA KOMMUN

UPPRÄTTAD: 2015-01-16 VERSION/UTGÅVA: 1

DIARIENR: 2015/106 BESLUTAD: 2015-03-

POLICY

KOMMUNFULLMÄKTIGE

INFORMATIONSSÄKERHETSPOLICY

Policyn tydliggör de kraven på informationshantering och informationssäkerhet i Sala kommun. Den gäller för kommunal verksamhet, för kommunala bolag och även för externa utförare enligt avtal. Policyn tydliggör kommunledningens mål, viljeinriktning och ansvaret för informationssäkerhetsarbetet. Här ingår hantering av personuppgifter enligt Personuppgiftslagen, SFS 1998:204 och SFS 1998:1191. Personuppgiftslagen är subsidiär; om det i annan lag eller förordning finns bestämmelser som avviker från denna lag ska den bestämmelsen gälla[1]. Avvikande bestämmelser finns t.ex. inom socialtjänst, sjukvård och för registerhantering.

Verksamheternas informationsförsörjning är en viktig del av kommunens totala informationssäkerhet och arbetet ska bedrivas systematiskt och långsiktigt. Information är en kunskapsbärare och en viktig tillgång. Hantering och arbete med informationssäkerhet utgår från:

- Lagar, förordningar och föreskrifter
- Kommunens egna regler och beslut
- Avtal

Medborgarna ska ha förtroende för att information hanteras säkert, den får inte spriudas till obehöriga.

Vad är informationssäkerhet[2]

Konfidentialitet: information avslöjas inte för och är inte tillgänglig för obehöriga (används ofta i betydelsen sekretess)

Riktighet: information skyddas mot oönskad och obehörig förändring eller förstörelse (primär information är exakt och fullständig)

Tillgänglighet: informationen är tillgänglig i förväntad utsträckning och inom önskad tid (åtkomlig och användbar)

Spårbarhet: att i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt eller användare (vem, vad och när)

MÅL FÖR INFORMATIONSSÄKERHETSARBETET

Information ska behandlas lagligt och all information hanteras säkert. Kommunens verksamheter och medarbetare ska

- ha god kunskap om informationssäkerhet
- använda sig av säkra system med funktionella tekniska lösningar för hantering av information och personuppgifter
- ha fungerande administrativa riktlinjer och tillämpningsrutiner
- rapportera fel och säkerhetsincidenter

[1] 1-2 §§ Personuppgiftslagen (1998:204)
[2] Definition enligt SS-ISO/IEC 27001

- årligen analysera informationssäkerheten i verksamheten

SALAS SÄKERHETSSTRATEGI

En bra informationssäkerhet bygger på säkra system och användare som känner till hur information ska hanteras säkert. Personuppgiftsansvariga nämnder ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda uppgifterna. Vidtagna åtgärder ska åstadkomma en säkerhetsnivå som är lämplig med hänsyn tagen till[3]:

- Tekniska möjligheter
- Kostnader för genomförande
- Särskilda risker som finns med behandling av personuppgifter
- Personuppgifternas känslighet

Förvaltning och säker hantering

Det ska för alla nämnder och i alla verksamheter upprättas styrande dokument för system och hantering av personuppgifter som visar :

- Vad som är tillåtet
- Vilka konsekvenser regelbrott/missbruk kan medföra
- Hur efterlevnad ska följas upp
- Vem användare ska vända sig till vid misstänkt intrång/missbruk
- Ansvaret i de olika delar som ingår

För hantering av information, uppgifter och system ska nämnder och verksamheter

- Genomföra informationsklassning och kontinuitetsanalyser, rapportera incidenter och fel samt analysera informationssäkerheten regelbundet
- Utbilda alla medarbetare i informationssäkerhet
- Utse informationssamordnare för informationssäkerhetsarbetet
- Utse systemansvariga för de system verksamheten äger
- Upprätta riktlinjer och tillämpningsrutiner för användare – för viktiga informationstillgångar (processer och system)
- Upprätta förvaltningsplaner - för system med informationsklassning och hantering: riskanalys, beskrivning samt ansvar och fördelning av uppgifter

Externa samverkansparter – privat verksamhet

Kommunen är personuppgiftsansvarig och ansvaret är fördelat på nämnderna[4]. Där någon del av kommunen, en verksamhet, bolag, enskild (privat) verksamhet eller en anställd självständigt förfogar över personuppgifter ska samråd ske samt hantering och ansvar tydliggöras i ett styrande dokument. Om driften är ett ansvar för annan myndighet eller huvudman t.ex. i privat regi ska ett avtal finnas.

[3] Säkerhet för personuppgifter, 2008, Datainspektionen allmänna råd
[4] Nämndernas reglementen

Bilaga VON 2015/18/5

SALA KOMMUN

UPPRÄTTAD: 2015-01-18 VERSION/UTGÅVA: 1

DIARIENR: 2015/106 BESLUTAD: 2015-03-?

KOMMUNFULLMÄKTIGE RIKTLINJE

Informationssäkerhet

Innehåll

SALA KOMMUN

Kommunfullmäktige

INLEDNING

Verksamheternas informationsförsörjning är en viktig del av kommunens totala informationssäkerhet och arbetet ska bedrivas systematiskt och långsiktigt. Denna riktlinje ska användas av nämnder och verksamheter i Sala kommun samt bolag om bolagen använder sig av stadens gemensamma informationstillgångar.

Informationstillgångar/information- avser all information oavsett om den behandlas manuellt eller automatiserat samt oberoende av dess form och i vilken miljö den förekommer. Exempel på informationstillgångar är:

- Information (databaser, filer, dokument etc.)
- Program (system, operativsystem etc.)
- Tjänster (nätförbindelser och abonnemang)
- Fysiska tillgångar (datorer, lokala nätverk etc.)
- Informationsbärare (pappersdokument, mobiltelefoner, USB etc.)

Informationssäkerhet- omfattar all information och är organisationens förmåga att hantera informationen så att legala, etiska och verksamhetsmässiga intentioner upprätthålls.

Personuppgifter- all slags information som direkt eller indirekt kan kopplas till en fysisk person som är i livet.

Syftet med informationssäkerhetsarbetet

Information ska hanteras säkert så att medborgares personliga integritet inte kränks. Behandling av uppgifter med informationsteknik (IT) kräver att uppgifter skyddas i samband med hantering och i systemen. Vilka säkerhetsåtgärder som behövs är beroende av vilka uppgifter som behandlas[1]. Störningar som medför att uppgifter förstörs, blir felaktiga/missvisande eller sprids till obehöriga ska undvikas[2].

ORGANISATION, ROLLER OCH ANSVAR

Kommunen är personuppgiftsansvarig och ansvaret är fördelat på nämnderna[3]. Ansvaret avgörs sedan av de faktiska omständigheterna i det aktuella fallet d v s vem som faktiskt bestämmer över informationen och behandlingen av uppgifter. En användare som inte självständigt får ändra, komplettera eller radera uppgifter är inte ansvarig. Den ansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda uppgifterna.

Ansvaret för informationssäkerhet

Information och informationssäkerhet ses som en integrerad del av verksamheten.

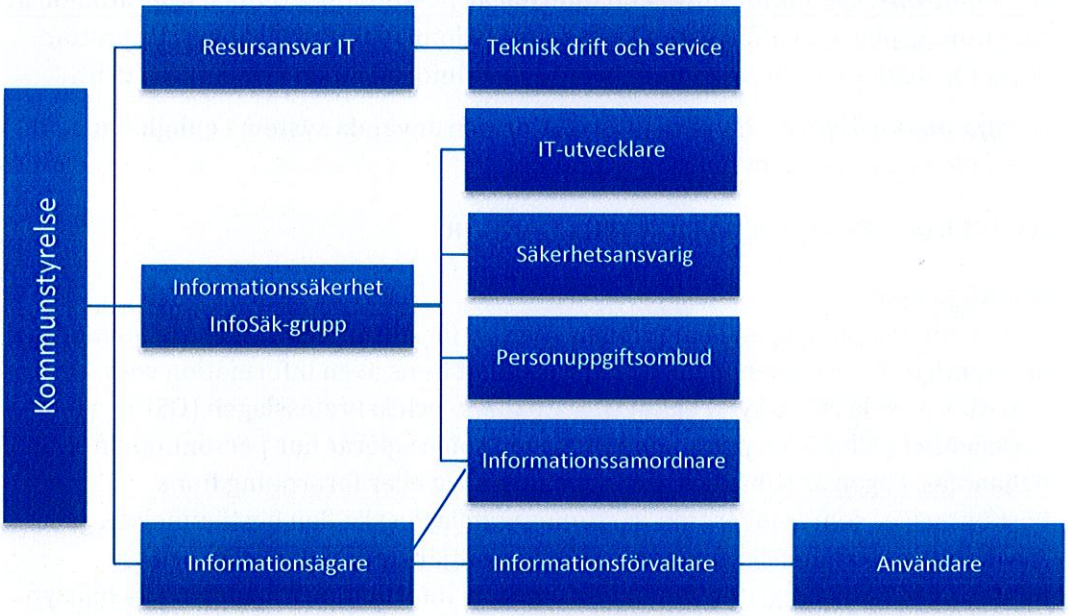
---

[1] Säkerhet för personuppgifter, 2008, Datainspektionen allmänna råd
[2] 48§ Personuppgiftslagen (1998:204)
[3] Nämndernas reglementen

Kommunfullmäktige

Alla användare och medarbetare som hanterar information och system har ett ansvar för att upprätthålla en god informationssäkerhet. Det ingår ett personligt ansvar att ta till sig och följa det regelverk och de styrande dokument som gäller för tjänsten. Verksamheter och system medför olika slag av ansvar. Alla ska vara införstådda med den egna verksamhetens krav och rapportera händelser som påverkar informationssäkerheten.

Det är ett chefsansvar att arbeta för en god informationssäkerhet i den egna verksamheten. När personal anställs och får tillgång till olika system ansvarar anställande chef för att information ges om hur information och system ska hanteras. Informationen ska ingå i introduktionen. Den som använder kommunens informationstillgångar på ett sätt som strider mot denna policy eller lagstiftning kan bli föremål för disciplinära eller rättsliga åtgärder.



Kommunstyrelsen- övergripande ansvar, att uppprätta mål och säkerhetsstrategi samt organisation för och revision av informationssäkerheten. Kommunchef har yttersta ansvaret för genomförande och efterlevnad.

Resursansvar IT –förvaltning och drift av system samt teknisk support. Kommunens IT-avdelning eller annan leverantör enligt avtal.

Referensgrupp InfoSäk- erbjuder stöd och kompetens i tekniska och juridiska frågor. I första hand kontaktas informationsansvarig i egen verksamhet

IT-utvecklare –bedöma vilka tekniska åtgärder som är lämpliga i tänkta system. IT-chef eller av denne utsedd person med teknisk kompetens. Ingår i InfoSäk.

Säkerhetsansvarig - sammanställa inkomna underlag och analysera kommunens totala informationssäkerhet. Vid identifierade väsentliga risker upprättas handlingsplan med förslag på åtgärder till kommunledningen. Ingår i InfoSäk

Personuppgiftsombud- följa upp interna kontroller av behandlingar som görs, påpeka brister och om de inte korrigeras, anmäla till Datainspektionen. Föra förteckning över system och samråda med Datainspektionen. Ingår i InfoSäk.

Informationsägare/systemägare – *Nämnder/verksamheter* ansvar för personregister och system som används. Ska upprätta styrande dokument för säker hantering. Bedöma och vidta organisatoriska åtgärder i samråd med IT-avdelning och personuppgiftsansvarig. Utse säkerhetssamordnare och systemförvaltare.

Informationssamordnare- samordna verksamhetens informationssäkerhetsarbete, göra årlig GAP-analys, koninuitetsplan samt sammanställa rapporterade incidenter och vidtagna förbättringsåtgärder. Delger riskanalyser och incidentdata till personuppgiftsombud. Ingår i InfoSäk.

Informations/systemförvaltare- hantering av personuppgifter och upprättande av förvaltningsplan och informationsklassning av informationstillgångar. Upprättar styrande dokument för systemet. Samråd med InfoSäk innan system tas i drift.

Övriga medarbetare – hantera information och använda system i enlighet med de styrande dokument som finns upprättade.

HANTERING AV INFORMATIONSTILLGÅNGAR

Rättsliga krav

Informationshanteringen i kommunen styrs av lagstiftningen[4], en viktig huvudregel är offentlighetsprincipen men i alla verksamhet finns även information som omfattas av sekretessskydd enligt Offentlighets- och sekretesslagen (OSL). I all verksamhet gäller även personuppgiftslagen som reglerar hur personuppgifter får behandlas. Lagen är subsidiär; Om det i annan lag eller förordning finns bestämmelser som avviker från Personuppgiftslagen ska den bestämmelsen gälla[5]. Avvikande bestämmelser finns t.ex. inom socialtjänsten, sjukvården och för hanteringen i olika register. Vid hanteringen av informationstillgångar ska hänsyn tas till regleringen för aktuellt område och verksamhet. Det ska tydliggöras vilken information som får hanteras och hur.

Integrerat informationssäkerhetsarbete

Informationssäkerhetsarbetet bör ingå som en del i ett integrerat ledningssystem för informationssäkerhet, LIS. Stöd finns på: www.informationssäkerhet.se
Arbetet med informationssäkerhet avser både tekniska åtgärder som brandväggar, krypteringsfunktioner och antivirus samt organisatoriska åtgärder som utbildning, policys, riktlinjer och tillämpningsrutiner.

Utbildning

Användare ska genomgå utbildning och kompetensutveckling i lämplig form[6]. Anställande chef ansvarar för att medarbetare utbildas i informationsäkerhet. Utbildning finns tillgänglig; http://disa.msb.se samt http://isa.msb.se

[4] Tryckfrihetsförordningen och Offentlighets- och sekretesslagen (2009:400)
[5] 1-2 §§ Personuppgiftslagen (1998:204)
[6] Säkerhet för personuppgifter, 2008, Datainspektionen allmänna råd

Styrande dokument
För viktiga informationstillgångar upprättas styrande dokument som beskriver de säkerhetslösningar som används och hur säkerheten ska fungera i de olika systemen. En förvaltningsplan ska finnas för alla viktigare system. Av styrande dokument för hantering och system där personuppgifter behandlas ska framgå:

- Vad som är tillåtet
- Vilka konsekvenser regelbrott/missbruk kan medföra
- Hur efterlevnad ska följas upp
- Vem användare ska vända sig till vid misstänkt intrång/missbruk
- Ansvaret i de olika delar som ingår

För att säkerställa riktighet och spårbarhet ska styrande dokument vara i filformat PDF innan de görs tillgängliga på intranät, hemsida eller annat öppet nät.

Förteckning av system
I alla verksamheter ska viktigare informationstillgångar samt ställda krav på säkerhet identifieras och förtecknas. Förteckningen sammanställs av informationssamordnaren med uppgifter från ledning och systemansvariga.

Förvaltningsplan
De krav som ställs på system och verksamheten ska framgå av en förvaltningsplan som systemförvaltaren upprättar. Förvaltningsplan ska visa vem som är

- systemägare,
- systemansvarig samt
- systemadministratörer och/eller
- support

Förvaltningsplanen kan även innehålla information om säkerhetsåtgärder. De säkerhetsåtgärder som i princip alltid ska finnas med för ett system är följande:

- fysisk säkerhet
- tillträdeskontroll
- behörighetskontroll
- inloggning och lösen
- loggning av system
- åtgärder mot förlust av information
- skydd mot skadliga program

Klassificering av information
Klassificering av information är en grundläggande aktivitet för att kunna skydda information och resurser. Informationsklassning ska göras av alla viktigare informationstillgångar och kan för system dokumenteras i förvaltningsplanen.

Det är informationen som är i fokus för vad som ska skyddas. Klassificeringen fungerar som ett beslutsunderlag för ledningen i arbetet med informationssäkerhet. Klassificeringen revideras vid behov, vid nyanskaffning av system eller förändrad organisation. Klassificeringen som används i Sala utgår från MSB:s rekommendationer för klassificering av information.

Kriterier för informationssäkerhet
All information som hanteras eller lagras i någon form behöver skyddas mot oönskad förändring, påverkan och insyn. Det ska inte vara möjligt för obehöriga att ta del av informationen. Användare med rätt till informationen ska däremot komma åt den efter behov och i rimlig tid. Det är även viktigt att kunna identifiera vem som gjort vad med informationen och i datasystemen.

Salas informationstillgångar ska bedömas utifrån följande 4 egenskaper[7]:

Konfidentialitet: information avslöjas inte för och är inte tillgänglig för obehöriga (används ofta i betydelsen sekretess)

Riktighet: information skyddas mot oönskad och obehörig förändring eller förstörelse (primär information är exakt och fullständig)

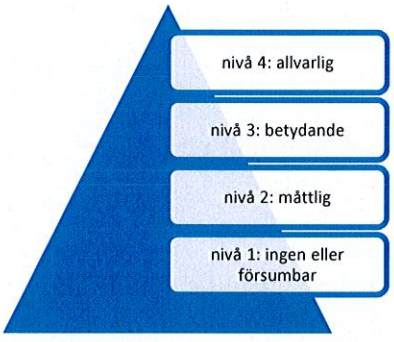
Tillgänglighet: informationen är tillgänglig i förväntad utsträckning och inom önskad tid (åtkomlig och användbar)

Spårbarhet: att i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt eller användare

Bedömning av nivåer och konsekvenser
Vid klassning av informationstillgångar ska informationens värde bedömas utifrån:

- Den funktion och betydelse som den har för verksamheten
- Konsekvenserna för verksamheten om informationen skulle hanteras felaktigt, försvinna, komma i orätta händer etc.

All fyra säkerhetsaspekter ska användas för klassningen av informationstillgången och värderas till någon av nivåerna:



Om informationen bedöms höra till nivå 1, ingen negativ påverkan eller en försumbar negativ påverkan behöver riskanalys inte göras. Inte heller behövs särskilda skyddsåtgärder för denna nivå.

[7] Definition enligt SS-ISO/IEC 27001

SALA KOMMUN

Kommunfullmäktige

Aspekt/ konsekvens	Riktighet	Konfidentialitet	Tillgänglighet	Spårbarhet
Allvarlig -4	Information kan medföra allvarlig negativ konsekvens för egen eller annan organisation eller för enskild person om den är felaktig	Information kan medföra allvarlig negativ konsekvens för egen eller annan organisation eller för enskild person om den röjs för obehörig	Information som kan medföra allvarlig negativ konsekvens för egen eller annan organisation eller för enskild person om den inte är tillgänglig	Information kan medföra allvarlig negativ konsekvens för egen eller annan organisation eller för enskild person om den inte är spårbar
Betydande -3	Information kan medföra betydande negativ konsekvens för egen eller annan organisation eller för enskild person om den är felaktig	Information kan medföra betydande negativ konsekvens för egen eller annan organisation eller för enskild person om den röjs för obehörig	Information som kan medföra betydande negativ konsekvens för egen eller annan organisation eller för enskild person om den inte är tillgänglig	Information som kan medföra betydande negativ konsekvens för egen eller annan organisation eller för enskild person om den inte är spårbar
Måttlig -2	Information kan medföra måttlig negativ konsekvens för egen eller annan organisation eller för enskild person om den är felaktig	Information kan medföra måttlig negativ konsekvens för egen eller annan organisation eller för enskild personom den röjs för obehörig	Information som kan medföra måttlig negativ konsekvens för egen eller annan organisation eller för enskild personom den inte är tillgänglig	Information kan medföra måttlig negativ konsekvens för egen eller annan organisation eller för enskild person om den inte är spårbar
Ingen eller försumbar - 1	Information som inte har krav på riktighet eller inte medför eller medför försumbar negativ konsekvens för egen eller annan organisation eller för enskild person om den är felaktig	Information utan krav på sekretess eller medför försumbar negativ konsekvens för egen eller annan organisation eller för enskild personom den röjs för obehörig	Information som inte har krav på tillgänglighet eller inte medför eller medför försumbar negativ konsekvens för egen eller annan organisation eller för enskild person om den inte är tillgänglig	Information som inte har krav på spårbarhet eller inte medför eller medför försumbar negativ konsekvens för egen eller annan organisation eller för enskild person om den inte kan spåras

Riskanalys och riskhantering
Alla informationstillgångar och verksamheter är utsatta för risker. För alla viktiga verksamhetskritiska informationstillgångar ska därför upprättas riskanalyser. Arbetet med riskanalysen ska identifiera och värdera tänkbara störningar,allvarliga händelser samt extraordinära händelser.

Arbetet ska fokusera på förebyggande åtgärder och syftar till att säkerställa hanteringen och skydda informationstillgångar. Risker som identifieras ska hanteras och åtgärder vidtas. Riskanalysen ska revideras vid förändring av verksamheten, av IT-stödet, av rättsliga krav eller av annan förändring som påverkar säkerheten.

Hantering av incidenter
Incidenter, risker och säkerhetsmässiga svagheter ska rapporteras i verksamhetens avvikelsehanteringssystem och tillställas närmaste chef . Chefen ansvarar sedan för att åtgärder vidtas för att minimera skada, åtgärda brister eller vidta åtgärder så att eventuell brottslighet utreds och anmäls. Om rapporterad risk eller incident avser brister i datasystemet ska även systemägaren informeras.

UPPFÖLJNING OCH REVISION
Säkerhetspolicyn revideras årligen av säkerhetsansvarig. Policyn ingår som styrande dokument och kompletteras av kommunens övriga styrande dokument; policys, handlingsplaner, riktlinjer och tillämpningsrutiner.

Informationssamordnaren gör en årlig analys av informationssäkerheten för nämnden eller den egna verksamheten där rapporterade fel och säkerhetsincidenter för informationshantering samt förteckningen över använda system är en del. Analysen ska, om väsentliga risker identifierats, innehålla en riskanalys och förslag på åtgärder. Förteckning och analys delges styrgruppen för Informationssäkerhet; InfoSäk. Tillsynsrapporter är en bedömning av hur väl verksamheten efterlever lagstiftning och ska om sådan finns ingå i den årliga analysen.

Egenkontroll- internrevision
Uppföljning och inrapportering ska göras av informationssamordnare till nämnd, verksamhetens ledning och säkerhetsansvarig. Uppföljning görs av följande delar:

- Medarbetares kompetens; Andel medarbetare som kan uppvisa intyg på genomförd utbildning i DISA.
- Fungerande administrativa rutiner. Kontroll av att förvaltningsplan och styrande dokument för hanteringen finns upprättade för samtliga verksamhetsområdes system. Jämförs mot förteckning
- Fungerande rapportering av säkerhetsincidenter finns på respektive förvaltning/verksamhet. Kontroll i LISA eller genom inlämning av statistik.
- Analys görs regelbundet minst årligen och åtgärder vidtas vid risker. Kontroll att det ingår i verksamhetens inlämnade dokument

En sammanställning görs för hela kommunen av säkerhetsansvarig och delges kommunchef och kommunstyrelse.

SALA KOMMUN

Kommunfullmäktige

Stödjande dokument

Kontinuitetsplan	Beskriver hur kontinuitetsplan görs. Hämta på www.informationssakerhet.se
Riskanalys	Beskriver hur riskanalys görs. Hämta på www.informationssakerhet.se
Informationsäkerhet	KF:s riktlinje. Beskriver hur arbetet görs och informationsklassning görs (bedömningsmatris)