Skapat av (Efternamn, Förnamn, org)	DokumentID	Skapad, uppdaterad
Katarina Olsson		2017-01-25
Fastställt av	**Datum för godkännande**	**Version**
Helena Ekroth	Åååå-mm-dd	0.1
Dokumenttitel		
Riktlinjer för informationssäkerhet		

Innehållsförteckning

Skapat av (Efternamn, Förnamn, org)	DokumentID	Skapad, uppdaterad
Katarina Olsson		2017-01-25
Fastställt av	**Datum för godkännande**	**Version**
Helena Ekroth	Åååå-mm-dd	0.1
Dokumenttitel		
Riktlinjer för informationssäkerhet		

1. Övergripande information

Riktlinjerna för informationssäkerhet utgår från Informationssäkerhetspolicy för Kommunalförbundet Sörmlands Kollektivtrafikmyndighet.

Enligt policyn är målet för informationssäkerheten att tillförsäkra att informationstillgångarna omfattas av säkerhetsaspekterna tillgänglighet, konfidentialitet, riktighet och spårbarhet, det vill säga att rätt information är tillgänglig för rätt person när den behövs och på ett spårbart sätt, och att informationen är och förblir rätt och riktig.

Myndighetens informationstillgångar omfattar såväl själva informationen (kunddatabas, metodik, dokument etc.), som myndighetens program (applikation, operativsystem etc.), tjänster (internetförbindelse, elförsörjning etc.) och fysiska tillgångar (dator, telefon etc.).

En stor del av vår information är mycket värdefull för oss. Tänk till exempel på informationen i bokningssystemet för färdtjänst och sjukresor. Är informationen förlorad eller felaktig kan det få allvarliga följder.

Därför måste vi skydda vår information så att:

- den alltid finns när vi behöver den (tillgänglighet)
- vi kan lita på att den är korrekt och inte manipulerad eller förstörd (riktighet)
- endast behöriga personer får ta del av och använda den (konfidentialitet)
- det går att följa hur och av vem informationen har hanterats (spårbarhet)

Bild 1. Schematisk bild över det som ska skyddas samt skyddsåtgärder.

Skapat av (Efternamn, Förnamn, org)	DokumentID	Skapad, uppdaterad
Katarina Olsson		2017-01-25
Fastställt av	**Datum för godkännande**	**Version**
Helena Ekroth	Åååå-mm-dd	0.1

Dokumenttitel

Riktlinjer för informationssäkerhet

Informationssäkerhet är teknikneutral och omfattar skydd av såväl muntlig, pappersbunden som digital information. Riktlinjernas fokus ligger på informationshantering med IS/IT-stöd, men berör också manuell hantering.

1.1 Giltighet

Dessa riktlinjer är beslutade av Kommunalförbundet Sörmlands Kollektivtrafikmyndighets myndighetschef och är utformade med stöd av Informationssäkerhetspolicyn. De gäller således hela myndigheten, samt avtalsparter där det i avtalet anges att myndighetens regelverk ska följas.

1.2 Dokumentstruktur

Policy är beslutad på politisk nivå. Till dessa finns riktlinjer och rutiner som är beslutade av myndighetschef. Inom ramen för dessa kan respektive verksamhetsansvarig ta fram och besluta om specifika instruktioner. Alla styrdokument ingår i myndighetens ledningssystem och finns samlade på myndighetens G.

Riktlinjer för informationssäkerhet kommer att utvecklas och implementeras löpande för att slutligen omfatta följande:

1. Övergripande information
2. Organisation av informationssäkerhetsarbetet
3. Styrning av informationstillgångar
4. Riskhantering
5. Medarbetare och informationssäkerhet
6. Fysisk säkerhet
7. Utveckling av IS/IT-tjänster
8. Leverantörsrelationer
9. Kommunikationssäkerhet
10. Driftsäkerhet
11. Åtkomst till information
12. Hantering av avvikelser och incidenter
13. Kontinuitetshantering
14. Uppföljning

Skapat av (Efternamn, Förnamn, org)	DokumentID	Skapad, uppdaterad
Katarina Olsson		2017-01-25
Fastställt av	**Datum för godkännande**	**Version**
Helena Ekroth	Åååå-mm-dd	0.1
Dokumenttitel		
Riktlinjer för informationssäkerhet		

2. Organisation av informationssäkerhetsarbetet

SYFTE: Organisationen ska ha ett högt riskmedvetande och informationssäkerhetsarbetet ska vara organiserat så att det finns ett tydligt ansvar och väl fungerande beredningsprocesser.

Ansvaret för genomförande och tillsyn av informationssäkerheten följer det delegerade verksamhetsansvaret. Det innebär att den som är ansvarig för en verksamhet också är ansvarig för genomförande och tillsyn av dess informationssäkerhet.

2.1 Särskilda och uttalade roller och ansvar

Ansvar för informationssäkerhet följer ordinarie linjeansvar, och alla informationstillgångar ska ha en utsedd ägare.

Myndighetschef
Har det övergripande ansvaret för verkställigheten av informationssäkerhetsarbetet och ett kontrollansvar att utförandet följer det delegerade ansvaret.

Personuppgiftsombud
Personuppgiftsombud ska se till att personuppgifter behandlas på ett lagligt och korrekt sätt. Personuppgiftsombudet ska bland annat påpeka eventuella brister i behandlingen. Om inte brister åtgärdas efter påpekande ska ombudet anmäla missförhållanden till Datainspektionen som är tillsynsmyndighet när det gäller behandling av personuppgifter.

Personuppgiftsombudet ska föra en förteckning över de behandlingar av personuppgifter, som skulle ha omfattats av anmälningsskyldighet, om ombudet inte funnits.

Informationssäkerhetsansvarig
Ansvarar för samordning och utveckling av informationssäkerhetsarbetet och ska förvalta generella styrdokument. Ansvarar också för samordning och utveckling av att tillräcklig teknisk säkerhet möjliggörs i IS/IT-system[1] (IT-säkerhet). I korthet omfattar ansvaret för informationssäkerhetsansvarig att:

- Ansvara för myndighetens färdriktning i långsiktiga, strategiska IS/IT-frågor.
- Utforma regelverk för informationssäkerhet och uppdatera dessa vid behov.
- Upprätta former för kontinuitetshantering.

[1] Med IS/IT menas informationssystem (IS), det vill säga system som håller data och information samt informationsteknologi (IT), det vill säga teknologin som håller systemen. Se även Bilaga 1. Termer och definitioner.

Skapat av (Efternamn, Förnamn, org)	DokumentID	Skapad, uppdaterad
Katarina Olsson		2017-01-25
Fastställt av	**Datum för godkännande**	**Version**
Helena Ekroth	Åååå-mm-dd	0.1

Dokumenttitel

Riktlinjer för informationssäkerhet

- Hantera allvarliga säkerhetsincidenter.

Samordnare för informationssäkerhet
Ansvarar för att samordna och följa upp informationssäkerhetsarbetet och rapportera till informationssäkerhetsansvarig. Informationssäkerhetssamordnaren ska:

- Utforma förslag till lokala styrdokument för informationssäkerhet med utgångspunkt från den egna organisationens specifika behov
- Sprida kunskap om regler, metoder och tekniker avseende informationssäkerheten
- Samordna det för organisationen och verksamheten gemensamma informationssäkerhetsarbetet
- Koordinera arbetet med att identifiera och klassificera informationstillgångar och IS/IT-system, genomföra riskanalyser och hantera avvikelser och incidenter.
- Säkerställa att krav på informationssäkerhet och funktionalitet beaktas i samband med anskaffning och utveckling av IS/IT-system.

Chefer inom myndigheten
Ansvarar för att information om informationssäkerhetsarbetet sprids, att resurser avsätts för arbetet efter behov, att personal ges tillräcklig kunskap, samt att arbetsmetoder som används bidrar till god informationssäkerhet.

Medarbetare inom myndigheten
Alla medarbetare är skyldiga att följa policy, riktlinjer, rutiner m.m. Avvikelser, brister, risker och incidenter rapporteras till närmaste chef.

Informationsägare
Informationsägaren ansvarar för den information som skapas och hanteras inom den egna verksamheten. Informationsägaren har det övergripande och yttersta ansvaret för den information som används av ett eller flera system. Grunden i informationsägarens arbete är klassificering av informationen och tilldelning av informationsklass som motsvarar kraven på säkerhet och skyddsnivå (arbetet med detta koordineras av samordnaren). Informationsägare fattar det avgörande besluten om informationen, om det behövs nyutveckling, vidareutveckling, förvaltning och avveckling av informationen. I korthet omfattar informationsägarens ansvar att:

- Informationen i systemen följer lagkrav.
- Delta i och stödja informationssäkerhetsarbetet.
- Anmäla till personuppgiftsombudet om information innehåller personuppgifter. I de fall personuppgifter hanteras på uppdrag utanför den egna organisationen ska avtal om personuppgiftsbiträde upprättas i enlighet med PuL, Personuppgiftslagen

Skapat av (Efternamn, Förnamn, org)	DokumentID	Skapad, uppdaterad
Katarina Olsson		2017-01-25
Fastställt av	**Datum för godkännande**	**Version**
Helena Ekroth	Åååå-mm-dd	0.1
Dokumenttitel		
Riktlinjer för informationssäkerhet		

- Besluta hur, av vem och vilken information som ska registreras.
- Besluta vilka personer inom verksamheten som ska ha tillgång till informationen i systemet.

Systemägare
Systemägare äger IS/IT-systemen. Systemägaren är övergripande ansvarig för IS/IT-systemen och dess användning. I korthet omfattar systemägarens ansvar att:

- IS/IT-system uppfyller verksamhetens behov och att bevaka verksamhetsmässiga faktorer som påverkar systemen
- Upprätta riktlinjer och tillämpningsföreskrifter för systemanvändningen
- IS/IT-systemen uppfyller såväl lagkrav som myndighetens policyer.

Varje IS/IT-system ska ha en systemägare utsedd.

Skapat av (Efternamn, Förnamn, org)	DokumentID	Skapad, uppdaterad
Katarina Olsson		2017-01-25
Fastställt av	**Datum för godkännande**	**Version**
Helena Ekroth	Åååå-mm-dd	0.1
Dokumenttitel		
Riktlinjer för informationssäkerhet		

12. Hantering av avvikelser och incidenter

SYFTE: Process, organisation och resurser för avvikelse- och incidenthantering ska finnas, för att mildra effekter, förhindra upprepande och underlätta återgång till verksamhet på normal nivå, då någon form av säkerhetsincident inträffat.

Avvikelser och incidenter i informationssäkerhetsarbetet måste fångas upp för att kunna användas vid uppföljning och förbättringsarbete. Dessutom innebär processen att rapportera, utreda, analysera, åtgärda och följa upp ett lärande för organisationen. En avvikelse eller incident som innebär en kris ska hanteras enligt *Rutin – Hantering av extern kris* eller *Rutin – Hantering av intern kris*.

12.1 Rapportering av avvikelser och incidenter

Den som upptäcker en avvikelse, incident eller en risk ansvarar för att om möjligt åtgärda och/eller lindra dess verkan, dvs. vidta en första åtgärd. Därefter rapporteras avvikelsen omgående enligt *Rutin för hantering av avvikelser*.

Vid händelse som gäller personuppgifters riktighet och när den enskildes integritet kan ha kränkts, ska personuppgiftsombudet (PuO) informeras.

12.2 Utredning och analys, samt korrigerande åtgärder

Bakomliggande orsaker till avvikelsen måste analyseras och åtgärder för att korrigera måste tas fram och dokumenteras i en handlingsplan. Detta görs enligt *Rutin för hantering av avvikelser*. Verksamhetsansvarig ska se till att det görs tillräckliga åtgärder för att ta bort orsaken till avvikelsen/incidenten.

12.3 Uppföljning och återrapportering

För att ständigt förbättra verksamhetens rutiner och arbetssätt och för att arbeta som en lärande organisation så behövs uppföljning av avvikelserna göras. Uppföljning är också nödvändigt för att upptäcka om likartade avvikelser eller händelser har upprepats, vilket kan tyda på att det finns en gemensam grundorsak som ska åtgärdas. Uppföljning av avvikelser och incidenter ska ske enligt *Rutin för hantering av avvikelser*.

Skapat av (Efternamn, Förnamn, org)	DokumentID	Skapad, uppdaterad
Katarina Olsson		2017-01-25
Fastställt av	**Datum för godkännande**	**Version**
Helena Ekroth	Åååå-mm-dd	0.1
Dokumenttitel		
Riktlinjer för informationssäkerhet		

14. Uppföljning

SYFTE: Informationssäkerheten ska regelbundet följas upp på central nivå som en del i den ordinarie verksamhetsredovisningen.

Enligt myndighetens informationssäkerhetspolicy ska arbetet regelbundet följas upp. Resultat av uppföljningen redovisas årligen till direktionen i årsredovisningen.

Samordnare för informationssäkerhet ska kontinuerligt följa upp informationssäkerhetsarbetet och säkerställa att informationssäkerhet ingår i verksamhetens interna kontroll och revision och att resultatet redovisas i direktionens årsredovisning.

14.1 Uppföljning av efterlevnad

14.1.1 Intern kontroll

Kontroll av efterlevnad av informationssäkerhetspolicyn med tillhörande riktlinjer och rutiner är en del av myndighetens interna kontroll. Kontrollerna syftar till att identifiera områden där det finns brister i efterlevnaden och där förändringar i rutiner eller ökade utbildningsinsatser är nödvändiga. Intern kontroll görs enligt *Rutin för intern kontroll*.

14.1.2 Internrevision

Informationssäkerhetsarbetet ska följas upp inom ramen för myndighetens internrevision enligt *Rutin för internrevision*.

14.1.3 Personuppgiftsombudets granskningar

Skyddet för den personliga integriteten och efterlevnad av personuppgiftslagen granskas särskilt av personuppgiftsombudet inom ramen för arbetet med intern kontroll.

Skapat av (Efternamn, Förnamn, org)	DokumentID	Skapad, uppdaterad
Katarina Olsson		2017-01-25
Fastställt av	**Datum för godkännande**	**Version**
Helena Ekroth	Åååå-mm-dd	0.1
Dokumenttitel		
Riktlinjer för informationssäkerhet		

Bilaga 1. Termer och definitioner

För användningen av dokument kopplade till informationssäkerhetsarbetet gäller följande termer och definitioner.

Avvikelse

En avvikelse är något som inträffar och som inte överensstämmer med verksamhetens normala rutiner eller kundens krav/förväntningar. Det kan exempelvis vara brister i tjänster och leveranser, kundsynpunkter och klagomål, brister i rutiner och kompetens, olycksfall och tillbud/incidenter, eller bristande lagefterlevnad. En avvikelse kan ge större eller mindre konsekvenser för den drabbade.

Behandling av personuppgifter

Varje åtgärd eller serie av åtgärder som någon vidtar med personuppgifter, vare sig det görs på automatiserad väg eller inte.

Behörighet

En persons tilldelade rättighet att komma åt information i IS/IT-system.

Hot

Möjlig, oönskad händelse med negativa konsekvenser för verksamheten.

Information

Ett vitt begrepp som inkluderar allt från kunskap som enskilda medarbetare har till information som är lagrad i IS/IT-system.

Informationssäkerhet

Säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad konfidentialitet (sekretess), riktighet, tillgänglighet och spårbarhet. Begreppet innefattar både fysisk säkerhet, IT-säkerhet samt administrativ säkerhet.

Informationssäkerhetsincident

En eller flera händelser som kan tänkas få allvarliga konsekvenser för verksamheten och hota informationssäkerheten (till exempel brott mot sekretess, integritetsförlust, driftavbrott eller brist på tillgång till information). Jämför med **Avvikelse**, där något faktiskt har inträffat.

Skapat av (Efternamn, Förnamn, org)	DokumentID	Skapad, uppdaterad
Katarina Olsson		2017-01-25
Fastställt av	**Datum för godkännande**	**Version**
Helena Ekroth	Åååå-mm-dd	0.1

Dokumenttitel

Riktlinjer för informationssäkerhet

Informationstillgång
En organisations information och de resurser som används för att hantera informationen. Exempel på informationstillgång är: Information (kunddatabas, metodik, dokument etc.), program (applikation, operativsystem etc.), tjänster (Internetförbindelse, elförsörjning etc.), fysiska tillgångar (dator, bildskärm, telefon etc.). Informationstillgång kan vara av fysisk eller logisk karaktär, eller bådadera.

Informationsägare
Informationsägaren ansvarar för den information som skapas och hanteras inom den egna verksamheten.

IS/IT-system
Med IS/IT menas informationssystem (IS), det vill säga system som håller data och information samt informationsteknologi (IT), det vill säga teknologin som håller systemen. Exempel på IS är Alfa, Mina sidor och Hållplatsappen. Exempel på IT-system är datorer och telefoni, men också kommunikationsutrustning, servrar, skrivare och övrig teknisk utrustning.

IS/IT-säkerhet
Säkerhet beträffande IS/IT-system med förmåga att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring eller störning vid databehandling samt dator- och telekommunikation.

Konfidentialitet (sekretess)
Avsikten att innehållet i informationen (eller ibland även informationen ska finnas överhuvudtaget) inte bör göras tillgängligt eller avslöjas för obehöriga.

Kontinuitetsplan
Dokument som beskriver hur verksamheten ska bedrivas och återställas när identifierade, kritiska verksamhetsprocesser allvarligt påverkas under en längre, specificerad tidsperiod.

Planen visar hur man går tillväga för att upprätta driften hos ett system efter en allvarlig händelse. Kan ibland benämnas avbrottsplan.

Personuppgift
All slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet. Bild- och ljuduppgifter om en identifierbar fysisk person räknas som personuppgifter, även om inga namn nämns. Krypterade uppgifter och olika slag av elektroniska identiteter är också personuppgifter om de direkt eller indirekt kan kopplas till fysiska personer som är i livet.

Skapat av (Efternamn, Förnamn, org)	DokumentID	Skapad, uppdaterad
Katarina Olsson		2017-01-25
Fastställt av	**Datum för godkännande**	**Version**
Helena Ekroth	Åååå-mm-dd	0.1

Dokumenttitel

Riktlinjer för informationssäkerhet

Personuppgiftsansvarig

Den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandling av personuppgifter.

Personuppgiftsombud

Den fysiska person som, efter förordnande av personuppgiftsansvarig, självständigt ska se till att personuppgifter behandlas på ett korrekt och lagligt sätt och i enlighet med god sed.

Riktighet

Egenskapen att vi kan lita på att informationen är korrekt och inte manipulerad eller förstörd.

Risk

Kombination av sannolikheten för att en incident ska inträffa och konsekvenserna av en denna.

Riskanalys

Process som identifierar säkerhetsrisker, bestämmer deras betydelse och identifierar skyddsåtgärder.

Samtycke

Varje slag av otvetydig viljeyttring genom vilken den registrerade godtar att personuppgifter som rör honom eller henne behandlas.

Spårbarhet

Möjligheten att entydigt kunna härleda utförda aktiviteter i systemet och/eller processen till en identifierad användare eller resurs.

Systemägare

Systemägare är den som äger teknik, infrastruktur eller IS/IT-systemen och är övergripande ansvarig för systemet och dess användning.

Säkerhetsåtgärd

Medel för hantering av risk, innefattandes policyer, riktlinjer, rutiner, förfaranden eller organisationsstrukturer vilka kan vara av administrativ, teknisk, ledningsmässig eller juridisk karaktär.

Skapat av (Efternamn, Förnamn, org)	DokumentID	Skapad, uppdaterad
Katarina Olsson		2017-01-25
Fastställt av	**Datum för godkännande**	**Version**
Helena Ekroth	Åååå-mm-dd	0.1
Dokumenttitel		
Riktlinjer för informationssäkerhet		

Tillgång

Allt som är av värde för organisationen. Med informationstillgångar menas både informationen i sig och de resurser som används för att hantera den, till exempel programvaror, tjänster och fysiska tillgångar.

Tillgänglighet

Skyddsmål där informationstillgångar ska kunna utnyttjas när vi behöver den.

Yttre sekretess

Innan uppgifter lämnas till mottagare utanför myndigheten görs sekretessprövning enligt offentlighets- och sekretesslagen.

Dokumentändringar

Ändringshistorik

Version	Datum	Ändring	Handläggare
0.1	2017-01-19	Första utkast	Katarina Olsson
1.0	Åååå-mm-dd	Beslut	