Myndigheten för samhällsskydd och beredskaps författningssamling

Utgivare: Key Hedström, Myndigheten för samhällsskydd och beredskap
ISSN 2000-1886

MSBFS 2009:10
Utkom från trycket den 8 januari 2010

Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet;

beslutade den 22 december 2009.

Myndigheten för samhällsskydd och beredskap föreskriver följande med stöd av 34 § förordningen (2006:942) om krisberedskap och höjd beredskap.

Tillämpningsområde

1 § Denna författning innehåller bestämmelser om myndigheternas arbete med informationssäkerhet och deras tillämpning av standarder i sådant arbete.

2 § Författningen gäller för myndigheter under regeringen med undantag för Regeringskansliet, kommittéväsendet och Försvarsmakten. För utlandsmyndigheterna tillämpas bestämmelserna endast i den utsträckning som bestäms i föreskrifter som meddelas av Regeringskansliet.

3 § Om det i någon annan författning finns bestämmelser om statliga myndigheters arbete med informationssäkerhet gäller dessa framför bestämmelserna i denna författning.

Arbete med informationssäkerhet

4 § En myndighet ska i sitt arbete med att upprätthålla säkerhet i sin informationshantering tillämpa ett ledningssystem för informationssäkerhet. Det innebär att myndigheten ska

1. upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet,

2. utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet,

3. klassificera sin information med utgångspunkt i krav på konfidentialitet, riktighet och tillgänglighet,

4. utifrån risk- och sårbarhetsanalyser och inträffade incidenter avgöra hur risker ska hanteras, samt besluta om åtgärder för myndighetens informationssäkerhet,

5. dokumentera granskningar och säkerhetsåtgärder av större betydelse som har vidtagits.

5 § Myndighetens ledning ska löpande informera sig om arbetet med informationssäkerhet samt minst en gång per år följa upp och utvärdera informationssäkerhetsarbetet på myndigheten.

Tillämpning av standarder

6 § En myndighets arbete enligt 4 och 5 §§ ska bedrivas i former enligt följande etablerade svenska standarder för informationssäkerhet;

- Ledningssystem för informationssäkerhet – Krav (SS-ISO/IEC 27001: 2006 fastställd 2006-01-19), och
- Riktlinjer för styrning av informationssäkerhet (SS-ISO/IEC 27002:2005 fastställd 2005-08-12).

Denna författning träder i kraft den 1 februari 2010.

Myndigheten för samhällsskydd och beredskap

HELENA LINDBERG

Helena Andersson
(Avdelningen för risk- och sårbarhetsreducerande arbete)

MSBFS 2009:10

Myndigheten för samhällsskydd och beredskaps allmänna råd om statliga myndigheters informationssäkerhet

Följande allmänna råd ansluter till 30 a § förordningen (2006:942) om krisberedskap och höjd beredskap samt till Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2009:10) om statliga myndigheters informationssäkerhet.

De termer och uttryck som används i de ovan nämnda författningarna har samma betydelse i dessa allmänna råd.

Allmänna råd har en annan juridisk status än föreskrifter. Allmänna råd är inte tvingande, utan deras funktion är att förtydliga innebörden i en lag, förordning eller myndighetsföreskrifter och att ge generella rekommendationer om tillämpningen av sådana regler.

Allmänna råd är markerade med grå bakgrund.

Myndigheten för samhällsskydd och beredskap

CECILIA NYSTRÖM

Helena Andersson
(Avdelningen för risk- och sårbarhetsreducerande arbete)

Bakgrund

Regeringens ambition att använda informations- och kommunikationsteknik för att förbättra service, främja demokratiprocessen och öka effektiviteten i offentlig förvaltning bygger på att nödvändig tillit kan etableras i relationen mellan offentlig förvaltning å ena sidan och medborgare och företag å andra sidan. Myndigheter som samverkar måste känna förtroende för varandra när det gäller åtkomst till och utbyte av information. Medborgare och företag måste känna tillit till myndigheternas sätt att hantera information.

Bristande informationssäkerhet kan få konsekvenser i form av att verksamheten inte kan bedrivas på ett ändamålsenligt och effektivt sätt, bristande skydd för den personliga integriteten samt störningar i samhällsviktig verksamhet.

En organisations sammantagna informationssäkerhet skapas genom en kombination av tekniska respektive administrativa säkerhetsåtgärder. Informationssäkerhet som begrepp omfattar skydd av information både när den hanteras manuellt av människor och när den behandlas med hjälp av IT. Att åstadkomma god informationssäkerhet är en komplex process som inbegriper hela verksamheten och som därför kräver engagemang och styrning från myndighetens ledning. Utgångspunkten för arbetet med informationssäkerhet är att risk- och sårbarhetsanalyser genomförs för att klarlägga den säkerhetsnivå som ska gälla för skydd av en organisations information.

Dagens samhälle präglas av ett högt beroende av IT. Utveckling av IT-användningen, inte minst den som följer av utvecklingen av e-förvaltningen och digitala kontrollsystem i samhällsviktiga verksamheter, innebär stora möjligheter men kan också medföra en ökad sårbarhet. Grunden för att åstadkomma och vidmakthålla en tillräcklig nivå på informationssäkerheten är att det finns fungerande processer som gör att man kan möta nya situationer och möjligheter. Att åstadkomma säkerhet vid användning av IT är en förutsättning för att kunna utnyttja tekniken på ett effektivt och ändamålsenligt sätt.

Ökad samverkan mellan organisationer, utökat informationsutbyte, flera e-tjänster mot allmänhet och företag ställer krav på att säkerhetsfrågorna behandlas seriöst och kompetent. Detta för att skapa nödvändig kvalitet och säkerhet kring den information som hanteras och för att säkerställa investeringar inom IT-området samt vidmakthålla omvärldens förtroende.

Inom IT-området finns en lång tradition av utveckling av nödvändiga standarder för att bidra till interoperabilitet i produktutbud och till kostnadseffektiv styrning av verksamhetsutvecklingen. Det gäller också på det säkerhetstekniska området, till exempel i fråga om kryptering, elektronisk legitimering och signering. Myndigheten för samhällsskydd och beredskaps föreskrifter (MSBFS 2009:10) om statliga myndigheters

informationssäkerhet anknyter till etablerade svenska och internationella standarder.

Nedan förklaras i korthet innebörden av bestämmelserna i författningen.

Författningens syfte och tillämpningsområde (1-3 §§)

Författningen gäller med vissa angivna undantag de statliga myndigheterna under regeringen. Författningens syfte är att skapa förutsättningar för att myndigheterna i sin informationshantering uppfyller sådana grundläggande och särskilda säkerhetskrav att myndigheternas verksamhet kan utföras på ett tillfredsställande sätt. När myndigheterna tillämpar etablerade standarder för informationssäkerhet ökar förutsättningarna för att upprätthålla informationssäkerhet i myndigheternas verksamhet.

Författningen är avsedd att tillämpas där motsvarande reglering saknas och den har därför gjorts subsidiär till andra författningar om statliga myndigheters arbete med informationssäkerhet. Andra myndigheters föreskriftsrätt på detta område påverkas därför inte. Det är emellertid lämpligt att sådana föreskrifter bygger på samma standarder.

Arbetet med ledningssystem för informationssäkerhet (4-5 §§)

Följande beskrivning utgår från innehållet i angivna standarder. Se ytterligare hänvisningar i slutet av de allmänna råden.

Ledningssystem för informationssäkerhet (LIS)

En organisations process för styrning och ledning av informationssäkerhet brukar benämnas ”Ledningssystem för informationssäkerhet” (LIS). Därmed avses myndighetens process för styrning och ledning av informationssäkerhetsarbetet vilket omfattar bl.a. organisation, resurser samt tekniska respektive administrativa säkerhetsåtgärder. Ledningssystemet för informationssäkerhet utgör en kvalitetsprocess som kontinuerligt ska utvärderas och anpassas till aktuella verksamhets- och omvärldskrav. Föreskrifterna lämnar möjlighet för varje myndighet att utifrån sin storlek, inriktning och andra förhållanden samt genomförd riskanalys besluta om i vilken omfattning kraven enligt bilaga A till SS-ISO/IEC 27001 är tillämpliga. Myndigheterna har möjlighet att anpassa sitt informationssäkerhetsarbete till en för verksamheten motiverad nivå.

Myndighetens beslut om i vilken omfattning standarden är tillämplig bör dokumenteras för att möjliggöra uppföljning och utvärdering av informationssäkerhetsarbetet.

Informationssäkerhetspolicy och andra styrande dokument

Informationssäkerhetspolicyn är det övergripande dokumentet som anger mål och inriktning samt styr organisationens informationssäkerhetsarbete. Informationssäkerhetspolicyn och övriga styrande dokument utgör systemdokumentationen av ledningssystemet för informationssäkerhet. Andra styrande dokument kan exempelvis vara myndighetens riktlinjer och beslut om ansvarsfördelning och risk- och incidenthantering. Myndighetens informationssäkerhetspolicy bygger på verksamhetens inriktning, organisation, intressent- och författningskrav samt identifierade hot och risker. En viktig utgångspunkt för informationssäkerhetsarbetet är att den information som myndigheten hanterar utgör en tillgång i verksamheten. För att verksamheten ska fungera krävs olika grader av konfidentialitet, krav på riktighet och krav på att information är tillgänglig.

Övriga styrande dokument upprättas i den omfattning som krävs för en kontinuerlig ledning och styrning av verksamhetens informationssäkerhet.

Alla styrande dokument bör omfattas av en formell styrning som innebär regelbunden granskning och förändringsåtgärder utifrån av ledningen tidigare fattade och dokumenterade beslut. Med formell styrning menas att det ska framgå vem som beslutat om dokumentet, vem som ansvarar för det, dess giltighet, ändringshistorik etc.

Organisation, roller och ansvarsförhållanden

Myndighetens ledning beslutar om hur uppgifter om informationssäkerhet fördelas i organisationen men har alltid det yttersta ansvaret för verksamhetens informationssäkerhet.

Samordning av informationssäkerhetsfrågor bör utföras av myndighetens ledning eller av en befattningshavare som ledningen direkt har utsett.

Informationssäkerhet bör ses som en integrerad del av myndighetens verksamhet vilket innebär att ansvariga för exempelvis IT-system, information och verksamhet har ett gemensamt ansvar för säkerheten i myndighetens informationstillgångar. Säkerhetskrav vid relationer med utomstående organisationer och personal ska särskilt beaktas (samverkande organisationer, utlokalisering av verksamhet, konsulter etc.)

Ledningen bör säkerställa att man får det underlag som är nödvändigt för att bedöma behovet av åtgärder och beslut om förbättringar av styrningen av informationssäkerhetsarbetet, förbättringar av mål och säkerhetsåtgärder samt om fördelning av resurser och ansvar. En viktig del av ledningens engagemang är att besluta om åtgärder för hantering av identifierade risker.

Personalens medverkan

God informationssäkerhet förutsätter att all berörd personal känner till och medverkar till att gällande regelverk följs. Därför bör säkerhetsfrågor också vara en naturlig del i relationen mellan arbetsgivare och arbetstagare från anställningens början till dess att den upphör. Utbildning och rutiner bör finnas som säkerställer att personalen har tillräcklig kunskap om gällande regler för informationssäkerhet. Utbildningen bör även omfatta etik och moralfrågor i anslutning till informationsbehandling i offentlig verksamhet.

Informationsklassificering

Syftet med informationsklassificering är att informationstillgångarna ska få en lämplig skyddsnivå.

Värdering och/eller klassificering av information bör ske i en omfattning och med den detaljeringsgrad som behövs för att, tillsammans med risk- och sårbarhetsanalyser, fatta relevanta beslut om skyddsnivå. En alltför omfattande klassificering kan innebära omotiverade administrativa kostnader.

Myndigheten för samhällsskydd och beredskap har tillsammans med Swedish Standard Institute (SIS) tagit fram en generell modell för informationsklassificering som behandlar informationens konfidentialitet, riktighet och tillgänglighet. Modellen ger även utrymme för andra aspekter, exempelvis spårbarhet. Myndigheternas arbete med klassificering bör ske på ett sätt som är förenligt med denna modell.

Modellen har publikationsnummer 0040-09 och finns tillgänglig på Myndigheten för samhällsskydd och beredskaps webbplats, www.msb.se.

Risk- och sårbarhetsanalyser

Myndigheten bör tillämpa lämpliga former för att kontinuerligt analysera risker och sårbarheter i verksamheten. Resultatet av genomförda analyser bör leda till beslut om lämpliga säkerhetsåtgärder.

Generella regler om myndigheternas risk- och sårbarhetsanalyser finns i 9 § förordningen (2006:942) om krisberedskap och höjd beredskap.

Säkerhetsåtgärder

Fysiskt skydd

Fysiskt skydd, huvudsakligen omfattande tillträdesskydd och skydd avseende övrig yttre påverkan, bör etableras med utgångspunkt från identifierade hot och risker.

Skydd av drift och datakommunikation

Alla förhållanden för drift av IT-system och datakommunikation bör beaktas från säkerhetssynpunkt. Rutiner bör vara dokumenterade och även innefatta ändringshantering, incidenthantering, skydd av datamedia och skydd mot skadlig programkod. Drifttagande av databehandlingsresurser inklusive resurser för datakommunikation bör ske efter godkännande och överenskommelse mellan aktuell systemägare och driftsansvarig, eller motsvarande.

Åtkomst- och behörighetsstyrning

Åtkomst till information och informationstillgångar bör utgå från av myndigheten beslutade ansvarsförhållanden och från den enskilde handläggarens behov vid genomförandet av tilldelade uppgifter. Vidare bör hänsyn tas till gällande lagstiftning, exempelvis vad som gäller för offentliga handlingar eller verksamhetens sakområde. Övergripande riktlinjer för åtkomst- och behörighetsstyrning bör upprättas som en del av regelverket för informationssäkerhet. Dessa riktlinjer bör även innefatta krav på loggning och uppföljning, både vid intern informationsbehandling och vid samverkan med andra organisationer. Systemägare eller befattningshavare med motsvarande ansvar för information och andra informationstillgångar bör besluta om tilldelning av behörighet. Formella rutiner för tilldelning, förändring, upphörande och uppföljning av åtkomst bör finnas.

Systemutveckling, systemanskaffning och systemavveckling

Särskild uppmärksamhet bör läggas på att verksamhetens säkerhetskrav beaktas vid utveckling, anskaffning och avveckling av informationsbehandlingsresurser. Vid utveckling av e-tjänster bör åtgärder vidtas för att säkerställa att medborgare och samverkande parter inte åsamkas skada. Etablerade säkerhetsåtgärder bör verifieras och godkännas av systemägaren, eller befattningshavare med motsvarande ansvar, innan driftssättning.

Kontinuitetsplanering

Kontinuitetsplaner för informationsförsörjningen bör upprättas och införas för att säkerställa att verksamheten ska kunna bedrivas enligt den nivå av kontinuitet som beslutats efter genomförd riskanalys. Planerna bör hållas uppdaterade och övas så att de blir ett naturligt inslag i ledning av informationssäkerhetsarbetet. Planerna bör ange beslutad krisorganisation och även omfatta återgång till normal drift.

Incidentrapportering och incidenthantering

Rutiner för incidentrapportering och incidenthantering bör finnas för att mildra effekter, säkra elektronisk bevisning, förhindra upprepande och underlätta återgång till normal drift. Rapportering av inträffade incidenter bör regelmässigt ske till verksamhetens chef i enlighet med upprättad rutin för ändamålet. Denna rutin bör säkerställa att incidenter utreds och hanteras.

Sveriges IT-incidentcentrum (SITIC), har till uppgift att samla in uppgifter om IT-incidenter och att ge stöd vid hot mot IT-säkerheten (www.sitic.se).

Granskning och uppföljning

Relevans och nytta av vidtagna åtgärder bör utvärderas genom regelbunden granskning och uppföljning. Intern granskning bör kompletteras med oberoende granskning. Myndighetens chef bör ange i vilken form rapportering av genomförd granskning ska ske.

Uppdrag till andra myndigheter

En myndighet som av olika skäl behöver samverka i fråga om informationssäkerhetsarbetet, kan överlåta till en annan myndighet att helt eller delvis fullgöra de uppgifter som åligger myndigheten enligt 4 § i författningen. Detta ändrar dock inte myndighetens ansvar för den egna informationssäkerheten.

Ledningen för den myndighet som uppdrar till annan myndighet att fullgöra uppgifter i fråga om informationssäkerhet bör löpande följa upp och informera sig om arbetet med informationssäkerhet på samma sätt som om uppgiften utförts av egen personal på myndigheten.

Tillämpliga standarder (6 §)

Arbetet med informationssäkerhet enligt etablerade svenska standarder beskrivs som en process med ett antal delprocesser av både förebyggande och reaktiv karaktär. Syftet med de LIS-standarder som anges i föreskrifterna är att säkerhetsarbetet anpassas till respektive organisations behov i de delar som bedöms vara tillämpliga. Därmed ger standarden en beslutsmodell för ledning och styrning med rimlig frihet till anpassning. Standarden SS-ISO/IEC 27001 anger krav både när det gäller uppbyggnad av ledningssystemet och mera konkreta åtgärdskrav enligt standardens bilaga A. Standarden SS-ISO/IEC 27002 ger riktlinjer och vägledning för en organisations införande och kontinuerliga arbete med informationssäkerhet.

Ytterligare stöd för informationssäkerhetsarbetet

Stöd för att bedriva informationssäkerhet i enlighet med svensk standard och att åstadkomma ett godtagbart skydd för samhällsviktiga IT-system finns i form av

1. MSB:s rekommendationer och vägledningar på området,
2. SIS handbok i informationssäkerhetsarbete (SIS HB 360) – Ge din information rätt säkerhet,
3. Post och Telestyrelsens råd och rapporter,
4. Datainspektionens allmänna råd, Säkerhet för personuppgifter,
5. Riksarkivets föreskrifter och allmänna råd på området, samt
6. övriga standarder i 27000-serien.

MSBFS
2009:10

Beställningsadress:
Norstedts Juridik AB/Fritzes, 106 47 Stockholm
Telefon 08-598 191 90, www.fritzes.se