Verket för förvaltningsutvecklings författningssamling

ISSN 1654-0832
Utgivare: Lena Jönsson, Verva, Box 214, 101 24 Stockholm

VERVA VERKET FÖR FÖRVALTNINGS-UTVECKLING

Vervas allmänna råd till föreskrift om statliga myndigheters arbete med säkert elektroniskt informationsutbyte, VERVAFS 2007:2;

VERVAFS 2007:2AR
Utkom från trycket
den 19 november 2007

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 kring e-tjänster måste känna förtroende för varandra när det gäller åtkomst till och utbyte av information. Medborgare och företag måste känna tillit till myndigheternas sätt att tillhandahålla e-tjänster. Detta innebär krav på godtagbar säkerhet så att exempelvis den personliga integriteten skyddas. Brister i informationssäkerhet kan innebära svårigheter att sprida nya e-tjänster och åstadkomma hinder för effektiva processer mellan myndigheter. Att åstadkomma säkerhet vid användning av IT är därmed en nödvändighet för att kunna utnyttja tekniken på bästa sätt.

En organisations sammantagna säkerhet skapas genom en kombination av tekniska respektive administrativa skyddsåtgärder och ger därmed en aggregerad nivå av säkerhet som benämns informationssäkerhet. 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 och informationssystem.

Utveckling av IT-användningen, inte minst den som följer av utvecklingen av e-förvaltningen, 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. 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 av 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 exempelvis kryptering, elektronisk legitimering och signering.

Mot denna bakgrund har Verva beslutat om föreskriften om statliga myndigheters arbete med säkert elektroniskt informationsutbyte (VERVAFS 2007:2) vilken anknyter till etablerade svenska standarder.

Nedan förklaras i korthet innebörden av bestämmelserna i föreskriften.

Föreskriftens syfte och tillämpningsområde (2-4 §§)

Föreskriftens syfte är att åstadkomma nödvändig säkerhet vid utveckling och drift av e-tjänster i offentlig förvaltning genom att skapa likformighet och samsyn på en nivå som ger förutsättningar för säkert och förtroendefullt informationsutbyte mellan myndigheter och i förlängningen mellan myndigheter och medborgare/företag. När alla myndigheter tillämpar de etablerade svenska standarderna för informationssäkerhet ökar förutsättningarna för att åstadkomma och behålla nödvändig och ändamålsenlig informationssäkerhet i förvaltningen.

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

Föreskriften ger även möjlighet för myndigheter som av olika skäl behöver samverka i fråga om informationssäkerhet att besluta om att överlåta till en av myndigheterna att helt eller delvis fullgöra myndigheternas uppgifter enligt denna föreskrift.

Arbetet med ledningssystem för informationssäkerhet (5-6 §§)

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,

skyddsåtgärder och uppföljning. Ledningssystemet för informationssäkerhet utgör en kvalitetsprocess som kontinuerligt ska utvärderas och anpassas till aktuella verksamhets- och omvärldskrav.

Föreskriften lämnar möjlighet för varje organisation att utifrån sin storlek, inriktning och andra unika förhållanden samt genomförd riskanalys besluta om i vilken omfattning skallkrav enligt bilaga A till SS-ISO/IEC 27001 är tillämpliga. Myndigheter har möjlighet att anpassa sitt informationssäkerhetsarbete till en för verksamheten motiverad nivå. Myndighetens beslut i denna del ska dokumenteras för att möjliggöra uppföljning och utvärdering av informationssäkerhetsarbetet.

Upprätta 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. Utgångspunkter för detta synsätt är olika grader av konfidentialitet, krav på riktighet och krav på att information är tillgänglig i den utsträckning som krävs för att verksamheten ska fungera.

Andra styrande dokument, exempelvis riktlinjer för skyddsåtgärder, ska upprättas i den omfattning som krävs för en kontinuerlig ledning och styrning av verksamhetens informationssäkerhet. 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 är ansvarig för dokumentet, dess giltighet, ändringshistorik etc.

Organisation, roller och ansvarsförhållanden

Myndighetens ledning ska besluta om hur ansvar och uppgifter fördelas i organisationen men har alltid det yttersta ansvaret för verksamhetens informationssäkerhet. Samordning av informationssäkerhetsfrågor bör utföras av myndighetens ledning eller av ledningen utsedd befattningshavare.

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, outsourcing, konsulter etc.)

Ansvariga för säkerhetsarbetet ska säkerställa att ledningen 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.

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.

Rutiner bör finnas som säkerställer att all personal känner till gällande regler för informationssäkerhet. Dessa rutiner bör innefatta återkommande utbildning och information som även omfattar gällande författningskrav, exempelvis sekretesslagen, personuppgiftslagen och relevanta registerlagar. Utbildningen bör även omfatta etik och moralfrågor med inriktning på informationsbehandling i offentlig verksamhet.

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 skyddsåtgärder.

Informationsklassificering

Syftet med informationsklassificering är att informationstillgångarna ska få en lämplig skyddsnivå. Information bör därför värderas/ klassificeras med hänsyn till aktuellt skyddsbehov inriktat på aspekterna *sekretess/konfidentialitet, riktighet* och *tillgänglighet* som ett minimum. Klassificering kan också ske med inriktning på andra aspekter som upplevs relevanta, t.ex. *spårbarhet*. Krav och behov med avseende på skydd av personuppgifter, krisberedskap, arkivering och gallring bör ges särskild uppmärksamhet.

Verksamhets- och omvärldskrav utgör grunden för bedömning av hotbild, risker och sårbarhet i samband med användning av all teknik för informationsbehandling och datakommunikation. Värdering och/eller klassificering av information bör ske i en omfattning och med den detaljeringsgrad som behövs för att fatta relevanta beslut om skyddsnivå. En alltför omfattande klassificering kan innebära omotiverade administrativa kostnader. Viss ledning kan sökas i Krisberedskapsmyndighetens rekommendationer 2006:1, Basnivå för informationssäkerhet (BITS) och stödverktyget BITS Plus.

Skyddsåtgärder

- *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 driftansvarig, 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 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*

Avbrottsplan 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 infor-

mationssäkerhetsarbetet. Planen 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, förhindra upprepande och underlätta återgång till normal drift. Rapportering av inträffade incidenter bör regelmässigt ske till verksamhetens chef. Myndighetens chef bör säkerställa att incidenter utreds och hanteras. Sveriges IT-incident centrum (SITIC), som är en del av Post- och telestyrelsen, 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 anger i vilken form rapportering av genomförd granskning ska ske.

Tillämpliga standarder (7 §)

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 föreskriften 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 27001:2006 anger krav både när det gäller uppbyggnad av ledningssystemet och mera konkreta åtgärdskrav enligt standardens bilaga A. Standarden SS-ISO/IEC 27002:2005 ger riktlinjer och vägledning för en organisations införande och kontinuerliga arbete med informationssäkerhet.

Ytterligare vägledning för informationssäkerhetsarbetet

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

- Krisberedskapsmyndighetens rekommendationer BITS 2006:1 och stödverktyget BITS Plus,
- SIS handbok i informationssäkerhetsarbete (SIS HB 360) – Ge din information rätt säkerhet,
- Datainspektionens allmänna råd, Säkerhet för personuppgifter, samt
- Riksarkivets bestämmelser på området.