Nuvarande MSBFS 2009:10	Förslag till ny föreskrift
Tillämpningsområde	**Tillämpningsområde**
1 § Denna författning innehåller bestämmelser om myndigheternas arbete med informationssäkerhet och deras tillämpning av standarder i sådant arbete.	**1 § första stycket** Denna författning innehåller föreskrifter som ansluter till bestämmelserna om statliga myndigheters informations-säkerhet i 30 a § förordningen om krisberedskap och höjd beredskap.
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.	**1 § andra stycket** Författningen gäller för myndigheter under regeringen med undantag av 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.	**2 § första stycket** Om det i en annan författning finns någon bestämmelse om statliga myndigheters informationssäkerhet som avviker från denna författning, gäller den bestämmelsen.
	2 § andra stycket Kraven i denna författning gäller endast i tillämpliga delar en sådan myndighet vars informationshantering eller informationssäkerhetsarbete helt eller delvis administreras av en annan myndighet. I de fall en myndighet anlitar en annan myndighet för att fullgöra uppgifter som specificeras i denna författning ska de berörda myndigheterna tydligt dokumentera sitt samarbete.
	Begreppsförklaring
	3 § I denna författning avses med informationssäkerhet Ett tillstånd som innebär skydd med avseende på konfidentialitet, riktighet, tillgänglighet och spårbarhet hos information.
Arbete med informationssäkerhet	**Ledningssystem för informationssäkerhet**

Nuvarande MSBFS 2009:10	Förslag till ny föreskrift
	4 § första stycket I 30 a § förordningen om krisberedskap och höjd beredskap finns föreskrifter om varje myndighets ansvar för sitt informationssäkerhetsarbete.
	4 § andra stycket Ansvaret gäller även när myndighetens information hanteras av en extern aktör eller när myndigheten erbjuder andra aktörer tjänster för informationshantering inom e-förvaltning eller motsvarande.
4 § En myndighet ska i sitt arbete med att upprätthålla säkerhet i sin informationshantering tillämpa ett ledningssystem för informationssäkerhet. Det innebär att	**5 §** Varje myndighet ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete med stöd av ett ledningssystem för informationssäkerhet. Det ska säkerställas att det sker en adekvat resurstilldelning för informationssäkerhetsarbetet samt att löpande och regelbunden information lämnas till myndighetsledningen.
	6 § första stycket Ledningssystemet ska utformas utifrån verksamhetens behov och vara styrande för all hantering av information som myndigheten ansvarar för.

Nuvarande MSBFS 2009:10	Förslag till ny föreskrift
	6 § andra stycket Ledningssystemet ska 1. säkerställa att informationssäkerhetsarbetet bedrivs samordnat samt att det regelbundet utvärderas och löpande utvecklas, 2. tydliggöra myndighetsledningens och den övriga organisationens ansvar för myndighetens informationssäkerhetsarbete, 3. precisera och tilldela nödvändiga befogenheter för de roller som arbetet med informationssäkerhet kräver och särskilt för den eller de befattningshavare som behöver utses för att leda och samordna arbetet.
	Närmare krav på myndigheternas informationssäkerhetsarbete
1. upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för myndighetens informationssäkerhet,	**7 §** Myndigheten ska upprätta en informationssäkerhetspolicy, andra styrande dokument samt den dokumentation som i övrigt krävs för att kunna bedriva ett ändamålsenligt arbete med myndighetens informationssäkerhet.
	8 § I syfte att underlätta identifiering av egna krav på informationssäkerhet ska myndigheten kartlägga sina verksamhetsprocesser och den information som stödjer dessa, samt utse informationsägare.
	9 § Myndigheten ska eftersträva en god säkerhetskultur där alla i organisationen har kunskap om och förståelse för behoven av säker informationshantering, genom att
	1. informera medarbetare om krav på säker informationshantering och relevanta regler inom området,

Nuvarande MSBFS 2009:10	Förslag till ny föreskrift
	2. regelbundet, och minst vartannat år, genomföra utbildningar rörande informationssäkerhet som är anpassade till medarbetarnas uppgifter, samt,
	3. regelbundet, och minst vartannat år, genomföra övningar med berörd del av organisationen för att pröva och utveckla myndighetens säkerhetsåtgärder för kontinuitetshantering avseende informationssäkerhet.
	10 § I syfte att hantera hot och risker som rör informationssäkerheten i verksamheten ska myndigheten med stöd av modeller som myndigheten beslutar
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,myndigheten ska	1. klassa information med utgångspunkt i konfidentialitet, riktighet, tillgänglighet och spårbarhet i olika nivåer utifrån vilka konsekvenser som kan uppstå av ett bristande skydd,
4. utifrån risk- och sårbarhetsanalyser och inträffade incidenter avgöra hur risker ska hanteras, samt besluta om åtgärder för myndighetens informationssäkerhet,	2. identifiera, analysera och bedöma hot och risker för verksamhetens information, system och tjänster,
	3. utifrån informationsklassningens resultat identifiera och införa åtgärder (skyddsnivå) som motsvarar informationens krav på skydd,
	4. följa upp och utvärdera införda åtgärder och gjorda bedömningar av hot och risker,
	5. kontinuerligt utveckla skyddet för att över tid upprätthålla informationens behov av säkerhet, samt
5. dokumentera granskningar och säkerhetsåtgärder av större betydelse som har vidtagits.	6. fortlöpande dokumentera genomförda åtgärder enligt denna paragraf.

Nuvarande MSBFS 2009:10	Förslag till ny föreskrift
	10 § andra stycket Av de beslutade modellerna ska det bland annat framgå vid vilka tidpunkter och i vilka situationer som myndigheten genomför informationsklassning och analys av hot och risker samt vem som ansvarar för åtgärderna. De beslutade modellerna ska vara kända av de som berörs i organisationen.
	Särskilt om incidenthantering och kontinuitetshantering
	11 § första stycket Myndigheten ska ha rutiner för att identifiera, rapportera, bedöma, hantera och dokumentera informationssäkerhets-incidenter. Myndigheten ska ha processer för att lära av inträffade informationssäkerhetsincidenter och utförda åtgärder.
	11 § andra stycket Myndigheten ska ha processer för kontinuitetshantering som tydliggör hur verksamhetens informationshantering upprätthålls vid större störningar och avbrott. Förhållanden som kan uppstå i samband med fredstida kriser och under höjd beredskap ska beaktas. I kontinuitetshanteringen ingår att definiera roller med tillhörande ansvar och befogenheter.
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	

Nuvarande MSBFS 2009:10	Förslag till ny föreskrift
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).	