

Implementeringsplan for it-sikkerhedsregulativet

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	Kapitel 1 Regulativets anvendelsesområde og formål				
Forvaltningerne	§ 1, stk. 2. Det skal aftales med de selvejende og private institutioner mv., der har indgået driftsoverenskomst med kommunen, eller som kommunen udfører behandlinger for, at disse skal efterleve it-sikkerhedsregulativet.	It-sikkerhedslederne	Umiddelbart efter it-sikkerhedsregulativets ikrafttræden.	Eksisterende aftaler gennemgås senest 12 måneder efter it-sikkerhedsregulativets ikrafttræden. Eventuelle rettelser/ ajourføringer foretages ved næste revision eller senest ved udgangen af 2009.	12
	Kapitel 3 Interne organisatoriske forhold				
	Borgerrepræsentationen				
BR	§ 4. Borgerrepræsentationen vedtager kommunens it-sikkerhedsregulativ og it-sikkerhedspolitik.		BR-møde, maj 2008	Ved vedtagelsen	0
BR-Sekr. og ØU	§ 4, stk. 3. It-sikkerhedspolitikken skal revurderes mindst hvert 2. år. Resultatet heraf skal godkendes af Borgerrepræsentationen efter indstilling fra Borgerrepræsentationens Sekretariat og Økonomiudvalget.	BR	Årshjul. Hvert 2. år.	Årshjul. Første gang 24 måneder efter it-sikkerhedsregulativets ikrafttræden.	24

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	Økonomiudvalget				
BR-Sekr.	§ 6, stk. 2. Borgerrepræsentationens Sekretariat fører en fortegnelse over Økonomiudvalgets beslutninger om fravigelser fra it-sikkerhedsregulativet og orienterer årligt udvalget for it-sikkerhed herom.	Udvalget for it-sikkerhed	Umiddelbart efter it-sikkerhedsregulativets ikrafttræden. Årshjul. Hvert år.	1. fortegnelse skal foreligge ved udgangen af 2008 og ellers ved udgangen af hvert år.	7
	Borgerrepræsentationens Sekretariat				
BR-Sekr.	§ 7, stk. 3. Borgerrepræsentationens Sekretariat tilrettelægger informations- og uddannelsesaktiviteter for medarbejdere, der varetager kommunens it-sikkerhedsfunktioner.	Økonomiforvaltningens direktion, som BR-Sekr. hører under	Foregår løbende.	Informations- og uddannelsesplaner udarbejdet 6 måneder efter it-sikkerhedsregulativets ikrafttræden. Uddannelse af centrale roller skal kunne starte hurtigt herefter.	6
	Overborgmesteren og borgmestrene				
Overborgmester -en og de enkelte borgmestre	§ 9. Overborgmesteren og de enkelte borgmestre udpeger inden for eget forvaltningsområde en eller flere it-sikkerhedsledere samt mindst en stedfortræder for hver it-sikkerhedsleder.	BR-Sekr.	Umiddelbart efter it-sikkerhedsregulativets ikrafttræden. Oversigt over alle it-sikkerhedsområder samt it-sikkerhedsledere og stedfortrædere. Paradigme på udpegningsbrev.	4 måneder efter it-sikkerhedsregulativets ikrafttræden.	4
Overborgmester en og de enkelte borgmestre	§ 9, stk. 2. Kompetencen til at udpege it-sikkerhedsledere og stedfortrædere kan delegeres til den administrerende direktør.	BR-Sekr.	Paradigme på delegation.	4 måneder efter it-sikkerhedsregulativets ikrafttræden.	4
	Direktionerne				

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
Direktionerne	§ 10, stk. 5. Direktionen udpeger inden for eget område en systemejer for hvert it-system samt mindst en stedfortræder for hver systemejer. Systemejerskab skal varetages inden for den forvaltning, som i medfør af styrelsesvedtægten skal løse den faglige opgave, som it-systemet skal understøtte.	BR-Sekr.	Umiddelbart efter it-sikkerhedsregulativets ikrafttræden. Paradigme på udpegningsbrev. Oversigt over it-systemer samt systemejere og stedfortrædere.	4 måneder efter it-sikkerhedsregulativets ikrafttræden.	4
Direktionen for Koncernservice	§ 10, stk. 6. Direktionen for Koncernservice skal udpege en systemejer for hvert af de fællessystemer, som Koncernservice er ansvarlig for.	BR-Sekr.	Umiddelbart efter it-sikkerhedsregulativets ikrafttræden. Paradigme på udpegningsbrev. Oversigt over it-systemer samt systemejere og stedfortrædere.	4 måneder efter it-sikkerhedsregulativets ikrafttræden.	4
Direktionen for Koncernservice	§ 10, stk. 7. Direktionen for Koncernservice skal udpege en it-ansvarlig samt mindst en stedfortræder for denne.	BR-Sekr.	Umiddelbart efter it-sikkerhedsregulativets ikrafttræden. Paradigme på udpegningsbrev. Oversigt over it-ansvarlige og stedfortrædere.	4 måneder efter it-sikkerhedsregulativets ikrafttræden.	4
Direktionen for Børne- og Ungdomsforvaltningen	§ 10, stk. 8. Direktionen for Børne- og Ungdomsforvaltningen kan udpege en it-ansvarlig samt en stedfortræder for denne for forvaltningens eget netværk, netværksudstyr og servere m.v.	BR-Sekr.	Umiddelbart efter it-sikkerhedsregulativets ikrafttræden. Paradigme på udpegningsbrev. Oversigt over it-ansvarlige og stedfortrædere.	4 måneder efter it-sikkerhedsregulativets ikrafttræden.	4
Ledelsen for Brandvæsnet	§ 10, stk. 9. Ledelsen for Brandvæsnet kan udpege en it-ansvarlig samt en stedfortræder for denne for Brandvæsnets eget netværk, netværksudstyr og servere	BR-Sekr.	Umiddelbart efter it-sikkerhedsregulativets ikrafttræden. Paradigme på udpegningsbrev.	4 måneder efter it-sikkerhedsregulativets ikrafttræden.	4

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	m.v.		Oversigt over it-ansvarlige og stedfortrædere.		
	It-sikkerhedsledere				
De nuværende it-sikkerhedsledere i samarbejde med BR-Sekr.	§ 13. It-sikkerhedslederens opgaver.	Økonomiforvaltningens direktion, som BR-Sekr. hører under	Opgavebeskrivelse for it-sikkerhedsledere.	3 måneder efter it-sikkerhedsregulativets ikrafttræden.	3
It-sikkerhedslederne	§ 13, stk. 5. It-sikkerhedslederen rådgiver inden for eget område om it-sikkerhedsmæssige forhold og tilrettelægger informations- og uddannelsesaktiviteter om it-sikkerhed for områdets medarbejdere.	BR-Sekr.	Efter udpegning.	Plan for informations- og uddannelsesaktiviteter klar 12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
It-sikkerhedslederne, BR-Sekr.	§ 13, stk. 6. It-sikkerhedslederen vurderer inden for eget område, om der er behov for at fastsætte regler i en it-sikkerhedsinstruks, som supplerer it-sikkerhedsregulativet. It-sikkerhedslederen udarbejder i givet fald en it-sikkerhedsinstruks, som godkendes af vedkommende borgmester, og som skal revideres mindst hvert 2. år.	BR-Sekr.	Årshjul. Vurdering af behov årligt. Revurdering hvert 2. år.	Vurdering skal være foretaget 8 måneder efter it-sikkerhedsregulativets ikrafttræden. Eventuel instruks skal være udarbejdet og godkendt 11 måneder efter it-sikkerhedsregulativets ikrafttræden.	8 11
			Paradigme på it-sikkerhedsinstruks (indholdsfortegnelse med mulige emner).	Paradigme skal være udarbejdet 6 måneder efter it-sikkerhedsregulativets ikrafttræden.	6
	Systemejere				
De nuværende systemejere i samarbejde med BR-Sekr.	§ 14. Systemejernes opgaver	BR-Sekr	Opgavebeskrivelse.	3 måneder efter it-sikkerhedsregulativets ikrafttræden.	3
Systemejerne	§ 14, stk. 2. Systemejeren skal godkende den it-ansvarliges	BR-Sekr.	Årshjul. Godkendelse af procedurer og driftsplaner når	Procedurer og driftsplaner skal være udarbejdet 12	12

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	<p>procedurer for driftsafviklingen, herunder driftsplanen. Driftsplaner udarbejdet af eksterne samarbejdspartnere skal tillige godkendes af systemejereren. Driftsafviklingsprocedurer for it-systemer, der er væsentlige informationsaktiver, skal være dokumenterede, ajourførte og tilgængelige for driftsafviklingspersonalet og andre med et arbejdsbetinget behov herfor. Systemejereren skal endvidere sikre, at den it-ansvarlige indgår aftale om it-beredskab for så vidt angår det it-system, som henhører under systemejereren.</p>		<p>disse foreligger.</p> <p>Oversigt over emner, der skal indgå i aftale om it-beredskabet.</p>	<p>måneder efter it-sikkerhedsregulativets ikrafttræden.</p> <p>Oversigten foreligger 9 måneder efter it-sikkerhedsregulativets ikrafttræden.</p>	9
Systemejerne	<p>§ 14, stk. 3. Ved brug af eksterne samarbejdspartnere er systemejereren ansvarlig for, at der i forhold til det pågældende it-system træffes de nødvendige it-sikkerhedsforanstaltninger, herunder at der i nødvendigt omfang indgås aftaler om de nærmere vilkår og it-sikkerhedskrav i forbindelse med samarbejdet.</p>	It-sikkerhedslederne	Allerede indgåede aftaler skal gennemgås.	Aftaler skal være gennemgået og ajourført i nødvendigt omfang et år efter it-sikkerhedsregulativets ikrafttræden.	12
Systemejerne	<p>§ 14, stk. 4. Udveksling af person- og værdioplysninger i form af udtræk fra et it-system til et andet (dataudveksling) skal uanset udtræksmediet ske i henhold til retningslinier udarbejdet af systemejereren for det it-system, som er genstand for udtrækket.</p>	It-sikkerhedslederne	Retningslinier for udtræk.	Retningslinier pr. system skal være udarbejdet 12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
	It-ansvarlige				

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsregulativets ikrafttræden
De nuværende it-ansvarlige i samarbejde med BR-Sekr.	§ 15. Opgavebeskrivelse for de it-ansvarlige	BR-Sekr.	Opgavebeskrivelse.	3 måneder efter it-sikkerhedsregulativets ikrafttræden.	3
De it-ansvarlige	§ 15, stk. 2. Den it-ansvarlige udarbejder it-sikkerhedsforskrifter for it-installationer, såfremt det skønnes nødvendigt. It-sikkerhedsforskrifterne skal revideres mindst hvert 2. år.	It-sikkerhedslederne	Årshjul. Revurdering hvert 2. år.	Vurdering skal være foretaget 9 måneder efter it-sikkerhedsregulativets ikrafttræden. Eventuel it-sikkerhedsforskrift skal være udarbejdet 12 måneder efter it-sikkerhedsregulativets ikrafttræden.	9 12
De it-ansvarlige	§ 15, stk. 5. Den it-ansvarlige sikrer, at udviklings-, test- og uddannelsesmiljøer holdes adskilt fra produktionsmiljøet.	It-sikkerhedslederne	I kraft ved it-sikkerhedsregulativets ikrafttræden.	9 måneder efter it-sikkerhedsregulativets ikrafttræden skal der være foretaget en vurdering af, hvor yderligere adskillelse af miljøer er påkrævet. Nødvendig adskillelse skal være implementeret 18 måneder efter it-sikkerhedsregulativets ikrafttræden.	9 18
	Koncernservice				
Koncernservice/ bestillerenhederne i de respektive forvaltninger, BR-Sekr.	§ 16, stk. 3. Ved bestilling af ydelser hos Koncernservice er bestillerenheden ansvarlig for, at der træffes de nødvendige it-sikkerhedsforanstaltninger, herunder at der i nødvendigt omfang indgås aftale om de nærmere vilkår og it-sikkerhedskrav i forbindelse med bestilling af ydelsen.	It-sikkerhedsfunktionerne, Økonomiforvaltningens direktion, som BR-Sekr. hører under	De allerede indgåede aftaler skal gennemgås mhp. at sikre, at der er taget højde for it-sikkerhedskravene. Eventuelt manglende it-sikkerhedskrav skal indarbejdes og aftalerne justeres i overensstemmelse hermed. Vejledning om hvordan de nødvendige it-sikkerhedsforanstaltninger	10 måneder efter it-sikkerhedsregulativets ikrafttræden skal aftalerne være gennemgåede. 12 måneder efter it-sikkerhedsregulativets ikrafttræden skal aftalerne være justerede. 8 måneder efter it-sikkerhedsregulativets ikrafttræden.	10 12 8

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
			træffes.		
	Organisering af internt samarbejde				
BR-Sekr.	§ 21. Der skal etableres et udvalg for it-sikkerhed og et samarbejdsforum for henholdsvis it-sikkerhedslederne og systemejerne for væsentlige fælles- og fagspecifikke it-systemer.	Økonomiforvaltningens direktion, som BR-Sekr. hører under	6 måneder efter it-sikkerhedsregulativets ikrafttræden skal for etableres. Medlemsoversigt over udvalgene.	6 måneder efter it-sikkerhedsregulativets ikrafttræden skal for etableret og medlemsoversigt være udarbejdet.	6
De respektive samarbejdsfora	§ 21, stk. 6. Møder i samarbejdsforaene skal afholdes mindst en gang hver fjerde måned.	BR-Sekr.	Årshjul. Hver 4. måned.	8 måneder efter it-sikkerhedsregulativets ikrafttræden skal foraene have afholdt deres første møde.	8
Udvalget for it-sikkerhed	§ 22, stk. 5. Udvalget refererer til kredsen af administrerende direktører. Udvalget skal årligt orientere kredsen af administrerende direktører om udvalgets arbejde og kan indstille sager til beslutning.	BR-Sekr.	Årshjul. Årligt.	1. gang 12 måneder efter, at udvalget har afholdt sit første møde.	20
Udvalget for it-sikkerhed	§ 22, stk. 7. Møder i it-sikkerhedsudvalget skal afholdes mindst en gang hver fjerde måned.	BR-Sekr.	Årshjul. Hver 4. måned.	8 måneder efter it-sikkerhedsregulativets ikrafttræden skal udvalget have afholdt dets første møde.	8
	Kapitel 4 Organisering af eksternt samarbejde				
BR-Sekr.	§ 23, stk. 1. Vurdering af sikkerhed hos en eventuel samarbejdspartner.	Økonomiforvaltningens direktion, som BR-Sekr. hører	Vejledning om vurdering af sikkerheden hos samarbejdspartneren.	9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
		under			
Systemejere, eksterne samarbejdspartnere	§ 23, stk. 2. Ved indgåelse af aftaler med eksterne samarbejdspartnere skal samarbejdspartneren underskrive en tavshedspligtserklæring, hvis samarbejdspartneren som led i samarbejdet får adgang til kommunens fortrolige og følsomme personoplysninger og værdioplysninger. Det nærmere indhold af tavshedspligtserklæringen fremgår af et af Borgerrepræsentationens Sekretariat udarbejdet paradigma.	It-sikkerhedsleder -ne	De allerede indgåede aftaler skal gennemgås mhp. at sikre, efterlevelse af kravet om tavshedspligt og aftalerne skal justeres i overensstemmelse hermed. Paradigme på tavshedspligtserklæring.	Gennemgangen og eventuelle justeringer skal være foretaget 9 måneder efter it-sikkerhedsregulativets ikrafttræden eller ved genforhandling/ fornyelse af aftalen. 6 måneder efter it-sikkerhedsregulativets ikrafttræden.	9 6
Systemejere, eksterne samarbejdspartnere	§ 23, stk. 3. Ved indgåelse af aftaler med eksterne samarbejdspartnere, der indebærer, at samarbejdspartneren skal foretage databehandling på kommunens vegne, skal der indgås en databehandleraftale, hvis indhold er i overensstemmelse med et af Borgerrepræsentationens Sekretariat udarbejdet paradigma herom.	It-sikkerhedslederne	De allerede indgåede aftaler skal gennemgås mhp. at sikre, efterlevelse af paradigmet og aftalerne skal justeres i overensstemmelse hermed. Paradigme på databehandlingsaftale. Ekstrakt af de regler samarbejdspartneren skal overholde.	Gennemgangen og eventuelle justeringer skal være foretaget 9 måneder efter it-sikkerhedsregulativets ikrafttræden eller ved genforhandling/ fornyelse af aftalen. 6 måneder efter it-sikkerhedsregulativets ikrafttræden.	9 6
	Kapitel 5 Risikovurdering og - håndtering				
BR-Sekr.	§ 25-27. Udarbejdelse af risikovurderinger.	Økonomiforvaltningens direktion, som	Generel vejledning om udarbejdelse af risikovurderinger.	Skal udsendes 6 måneder før første obligatoriske risikovurdering.	14

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
		BR-Sekr. hører under			
BR-Sekr.	§ 25, stk. 6. Direktionen skal på baggrund af en indstilling fra it-sikkerhedslederen tage stilling til, om it-sikkerhedsniveauet er passende. Hvis it-sikkerhedsniveauet ikke er passende, skal der iværksættes tiltag, så det ønskede it-sikkerhedsniveau opnås. It-sikkerhedslederen skal orientere vedkommende udvalg og Borgerrepræsentationens Sekretariat om direktionens beslutning.	BR-Sekr.	Paradigme på indstilling om it-sikkerhedsniveau. Paradigme på orientering af BR Sekr. og udvalget for it-sikkerhed.	Skal udsendes 6 måneder før første obligatoriske risikovurdering.	14
BR-Sekr.	§ 26, stk. 1. Risikovurderinger skal udarbejdes på grundlag af et af Borgerrepræsentationens Sekretariat udarbejdet paradigma.	Økonomiforvaltningens direktion, som BR-Sekr. hører under	Paradigma (på emner der skal indgå i risikovurderinger) skal udarbejdes.	Skal udsendes 6 måneder før første obligatoriske risikovurdering.	14
Direktionerne	§ 26, stk. 2. Risikovurderinger skal udarbejdes inden udgangen af hvert ulige år og ved væsentlige ændringer i risikobilledet.	BR-Sekr.	Årshjul. Hvert 2. år. Ved udgangen af hvert ulige år og ved væsentlige ændringer i risikobilledet.	Første ordinære vurdering ved udgangen af 2009.	20
BR-Sekr.	§ 27, stk. 1. Borgerrepræsentationens Sekretariat udarbejder på baggrund af de enkelte forvaltningers risikovurderinger en samlet risikovurdering for kommunen.	Økonomiforvaltningens direktion, som BR-Sekr. hører under	Paradigme på en samlet risikovurdering.	Skal udarbejdes 6 måneder før første obligatoriske risikovurdering.	14
BR-Sekr.	§ 27, stk. 2. Den samlede risikovurdering skal udarbejdes	Økonomiforvaltningens	Årshjul. Udgangen af 1. kvartal hvert lige år.	Første gang 1. kvartal 2010.	23

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	inden udgangen af 1. kvartal i hvert lige år.	direktion, som BR-Sekr. hører under			
BR	§ 27, stk. 3. På baggrund af den samlede risikovurdering træffer Borgerrepræsentationen beslutning om fastlæggelse af kommunens overordnede it-sikkerhedsniveau. Det overordnede it-sikkerhedsniveau fremgår af kommunens it-sikkerhedspolitik.	BR-Sekr.	Årshjul. 2. kvartal hvert lige år.	Første gang 2. kvartal 2010.	24
	Liste over behandlinger og anmeldelsespligt				
It-sikkerhedslederne	§ 28. Som led i risikovurderingen skal it-sikkerhedslederen udarbejde en liste over alle anvendte it-systemer samt de databehandlinger, der foretages på it-sikkerhedslederens område, og det skal i den forbindelse også vurderes og dokumenteres, i hvilket omfang der er pligt til at foretage anmeldelse af behandlingen, jf. stk. 3.	BR-Sekr.	Årshjul. Hvert år i takt med risikovurderingerne. Liste over anvendte it-systemer, driftssteder m.v.	Første gang inden udgangen af 2008	7
It-sikkerhedslederne, BR-Sekr.	§ 28, stk. 3. It-sikkerhedslederen skal inden for eget område og efter forudgående at have rådført sig med Borgerrepræsentationens Sekretariat foretage anmeldelse til Datatilsynet af alle anmeldelsespligtige behandlinger før behandlingerne påbegyndes, jf. dog også persondatalovens § 44. Anmeldelser skal i videst muligt omfang ske ved tilslutning til de af KL og Datatilsynet udarbejdede fællesanmeldelser.	BR-Sekr.	It-sikkerhedslederne udarbejder liste over it-systemer og behandlinger i løbet af 2008.	Inden udgangen af 2008 gennemgår it-sikkerhedsledere oversigter over behandlinger med BR-Sekr. for at vurdere, om anmeldelsesregler er overholdt, og om der er behov for at forelægge behandlinger i henhold til § 26.	7

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	Væsentlige informationsaktiver				
It-sikkerhedslederne	§ 30. Som led i risikovurderingen skal it-sikkerhedslederen sikre, at der til enhver tid findes en ajourført fortegnelse over alle væsentlige informationsaktiver inden for it-sikkerhedslederens ansvarsområde med undtagelse af disketter, cd'er, usb-nøgler eller lignende mobile lagringsmedier.	BR-Sekr.	Udarbejdelse af fortegnelse.	Ifm. udarbejdelse af risikovurderingen v. udgangen af 2009.	19
BR-Sekr.	§ 30, stk. 2. Af fortegnelsen over væsentlige informationsaktiver skal for hvert enkelt aktiv fremgå, hvem der er aktivets ejer, og hvilken type af oplysninger aktivet indeholder. Endvidere skal der være taget stilling til arkivering og eventuel sletning af oplysninger. Fortegnelsen skal udarbejdes på grundlag af et af Borgerrepræsentationens Sekretariat udarbejdet paradigma.	Økonomiforvaltningens direktion, som BR-Sekr. hører under	Paradigme på fortegnelse over væsentlige informationsaktiver. Holdes på et generelt niveau	14 måneder efter it-sikkerhedsregulativets ikrafttræden ifm. udarbejdelse af paradigme på risikovurdering	14
	Kapitel 6 It-sikkerhedshandlingsplan				
BR-Sekr.	§ 31. Borgerrepræsentationens Sekretariat udarbejder en it-sikkerhedshandlingsplan, der skal sikre, at it-sikkerhedspolitikken udmøntes i praksis.	Økonomiforvaltningens direktion, som BR-Sekr. hører under	Umiddelbart efter it-sikkerhedsregulativets ikrafttræden.	5 måneder efter it-sikkerhedsregulativets ikrafttræden.	5
BR-Sekr., Økonomiudvalget	§ 31, stk. 2. It-sikkerhedshandlingsplanen skal forelægges for Økonomiudvalget til orientering.	Økonomiudvalget	Årshjul. Hvert 2. år.	Første forelæggelse 5 måneder efter it-sikkerhedsregulativets ikrafttræden.	5

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	Kapitel 7 Adfærdsregler				
	Kommunikation og lagring				
Den it-ansvarlige	§ 32, stk. 2. Når kommunikation mv. ikke foregår via kommunens fælles it-netværk, må der kun anvendes it-systemer, internetservices, programmer, kommunikationsforbindelser, mv., der er godkendt af den it-ansvarlige.	BR-Sekr.	Vejledning om hvilken kommunikation, der kan godkendes af den it-ansvarlige.	9 måneder efter it-sikkerhedsregulativets ikrafttræden skal vejledning være udarbejdet.	9
Den it-ansvarlige	§ 33. Alle oplysninger skal lagres på serverdrev, der er godkendt af den it-ansvarlige.	It-sikkerhedslederne	Liste over godkendte serverdrev skal udarbejdes.	De it-ansvarlige skal senest 6 måneder efter it-sikkerhedsregulativets ikrafttræden have udarbejdet listen og meddele området, hvilke serverdrev, der er godkendt til hvilke data.	6
	Kryptografi				
Den it-ansvarlige	§34. Den it-ansvarlige skal etablere en generel krypteringsløsning og udarbejder et nøglehåndteringssystem, som understøtter anvendelse af kryptografi.	BR-Sekr.	Vejledning om krypteringsløsninger.	9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9
	Brug af Internet				
BR-Sekr.	§ 35-36. Brug af Internet og e-mail.	Økonomiforvaltningens direktion, som BR-Sekr. hører under	Vejledning om anvendelse af Internet og e-mail med nærmere beskrivelser og forklaringer af reglerne i selve it-sikkerhedsregulativet.	12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
Den it-ansvarlige	§ 35, stk. 2. Den it-ansvarlige fastlægger sikkerhedsindstillingerne for	BR-Sekr.	Fastlæggelse af sikkerhedsindstillinger.	9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	webbrowsere og administrerer indstillingerne centralt. Der må kun anvendes godkendte webbrowsere. Medarbejderne må på ingen måde forsøge at omgå eller bryde disse it-sikkerhedsforanstaltninger.				
Den it-ansvarlige	§ 35, stk. 3. Den it-ansvarlige kan i fornødent omfang fastsætte regler om tung og vedvarende trafik.	BR-Sekr.	Eventuelle regler udarbejdes.	Eventuelle regler udarbejdet 9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9
	Kapitel 8 Medarbejderne				
	Ansættelse af medarbejdere				
Ledere, BR-Sekr., HR	§ 38. Alle medarbejdere skal senest på tiltrædelsestidspunktet og som en integreret del af ansættelsesaftalen erklære at være bekendt med, at vedkommende er underlagt reglerne om tavshedspligt, jf. forvaltningslovens § 27 og straffelovens § 152 og §§ 152 c-152 f. Ansvar for påhviler medarbejderens nærmeste overordnede.	It-sikkerhedslederne, økonomiforvaltningens direktion, som BR-Sekr. hører under	Vejledning om hvad man skal huske fsva. it-sikkerhed ved ansættelse og ansættelsesforholdets ophør. Tavshedspligtserklæring udarbejdes af BR-Sekr. Vejledning om undersøgelse af en medarbejders forhold.	8 måneder efter it-sikkerhedsregulativets ikrafttræden.	8
	Under ansættelsesforholdet				
Ledere	§ 39, stk. 2. Alle medarbejdere gennemgår som led i et introduktionsforløb om it-sikkerhed en elektronisk udgave af kommunens it-sikkerhedspolitik og it-sikkerhedsregulativ. Ved afslutningen af dette introduktionsforløb anmodes medarbejderen om at tilkendegive, om reglerne er læst og forstået.	It-sikkerhedslederne	Udarbejdelse af introduktionsforløb.	Introduktionsforløb skal være udarbejdet 8 måneder efter it-sikkerhedsregulativets ikrafttræden.	8

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	Hvis medarbejderen bekræfter dette, gives vedkommende i fornødent omfang adgang til kommunens it-systemer og oplysninger.				
	Ved ansættelsesforholdets ophør				
Ledere, it-sikkerhedslederne BR-Sekr.	§ 40. Medarbejderens nærmeste overordnede sikrer, at medarbejderen senest ved ansættelsesforholdets ophør afleverer it-udstyr og lignende, som tilhører kommunen, og at der sker inddragelse af medarbejderes adgangsrettigheder i henhold til en af it-sikkerhedslederen for det pågældende område nærmere fastlagt procedure.	It-sikkerhedslederne Økonomiforvaltningens direktion, som BR-Sekr. hører under	Procedure for aflevering af it-udstyr og lignende samt for inddragelse af rettigheder. Paradigma udarbejdes af BR-Sekr.	Skal være udarbejdet 8 måneder efter it-sikkerhedsregulativets ikrafttræden.	8 6
	Kapitel 9 Fysisk sikkerhed				
	Beskyttelse af udstyr, herunder ind- og uddata				
BR-Sekr.	§ 43, stk. 4. Tilintetgørelse af ind- og uddata.	Økonomiforvaltningens direktion, som BR-Sekr. hører under	Vejledning om tilintetgørelse af ind- og uddata.	12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
BR-Sekr.	§ 43, stk. 5. Fysisk transport af ind- og uddata	Økonomiforvaltningens direktion, som BR-Sekr. hører under	Vejledning om fysisk transport af ind- og uddata.	12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
It-sikkerhedslederne	§ 45. It-udstyr må kun fjernes fra kommunens ejendomme efter forudgående skriftlig godkendelse fra it-sikkerhedslederen for det	BR-Sekr.	Generelle retningslinier skal udarbejdes.	Retningslinier for fjernelse af udstyr skal være fastlagt senest 12 måneder efter it-	12

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	område, hvor it-udstyret er placeret.			sikkerhedsregulativets ikrafttræden.	
Den it-ansvarlige	§ 45, stk. 2. Servere, netværksudstyr m.v., som ejes af Koncernservice, må kun fjernes fra kommunens ejendomme efter forudgående skriftlig godkendelse fra den it-ansvarlige i Koncernservice.	BR-Sekr.	Generelle retningslinier skal udarbejdes.	Retningslinier for fjernelse af udstyr skal være fastlagt senest 12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
Den it-ansvarlige	§ 46. Den it-ansvarlige i Koncernservice skal fastsætte regler for, hvilket it-udstyr, der skal tyverisikres gennem mærkning.	BR-Sekr.	Regler for mærkning.	Regler for, hvilket it-udstyr, der skal tyverisikres gennem mærkning og hvordan mærkningen skal foregå skal være fastlagt senest 12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
Den it-ansvarlige	§ 48. Personoplysninger eller værdioplysninger skal så vidt muligt slettes effektivt og på en sikker måde fra it-udstyr, der repareres eller vedligeholdes uden for kommunens ejendomme.	BR-Sekr.	Vejledning om effektiv sletning.	Vejledning skal være udarbejdet 9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9
	Sikre og kontrollerede områder				
Den it-ansvarlige	§ 49, stk. 2. Den it-ansvarlige skal fastsætte retningslinier for fysisk sikring herunder om godkendelse af personale med adgang til de i stk. 1 nævnte områder, om eventuel overvågning af personale, om meddelelse af oplysninger herom, om anvendelse af alarmsystemer, beskyttelse mod brand og vandskader, eventuel etablering af køling og ventilation, beskyttelse	BR-Sekr.	Retningslinier skal udarbejdes.	Retningslinier skal være udarbejdet 9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	med nødstrømsanlæg og kapaciteten heraf samt om andre foranstaltninger til beskyttelse af sikre områder. Retningslinierne skal revideres mindst hvert 4. år.				
Den it-ansvarlige	§ 49, stk. 3. Der føres en fortegnelse over de i stk. 1 nævnte områder.	BR-Sekr.	Fortegnelse over krydsfelter, serverrum mv.	Fortegnelse skal foreligge senest 9 måneder efter it-sikkerhedsregulativets ikrafttræden	9
It-sikkerhedslederne	§ 50, stk. 1. Den lokale ledelse skal i samarbejde med it-sikkerhedslederen træffe beslutning om, hvilke andre områder der, udover de i § 49, stk. 1 nævnte, skal være sikre områder. Der føres en fortegnelse over disse områder.	BR-Sekr.	Fortegnelse over sikre områder	Fortegnelse skal foreligge senest 9 måneder efter it-sikkerhedsregulativets ikrafttræden	9
Den lokale ledelse	§ 50, stk. 2. Den lokale ledelse fastsætter i samarbejde med it-sikkerhedslederen retningslinier for fysisk sikring herunder om godkendelse af personale med adgang til sikre områder, om eventuel overvågning af personale, om meddelelse af oplysninger herom, om anvendelse af alarmsystemer, beskyttelse mod brand og vandskader, eventuel etablering af køling og ventilation, beskyttelse med nødstrømsanlæg og kapaciteten heraf samt om andre foranstaltninger til beskyttelse af sikre områder. Retningslinierne skal revideres mindst hvert 4. år.	BR-Sekr.	Retningslinier skal udarbejdes.	Retningslinier skal være udarbejdet 9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9
Den lokale ledelse	§ 51. Den lokale ledelse træffer i samarbejde med it-sikkerhedslederen herudover beslutning om, hvilke områder,	BR-Sekr.	Retningslinier skal udarbejdes.	9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	som offentligheden ikke normalt skal have adgang til, og som dermed skal anses som kontrollerede områder. Den lokale ledelse fastsætter i samarbejde med it-sikkerhedslederen om nødvendigt nærmere retningslinier for sikkerheden på sådanne kontrollerede områder. Eventuelle retningslinier herom skal revideres mindst hvert 4. år.				
	Kapitel 10 Adgangsstyring				
	Adgangsstyring og brugeradgang				
Koncernservice	§ 52, stk. 4. Koncernservice skal udarbejde en eller flere procedurer for adgangsstyring og brugeradgang, jf. §§ 52-55 og § 59, stk.3. Proceduren eller procedurerne skal sendes i høring hos it-sikkerhedslederne. Proceduren eller procedurerne skal forelægges for Borgerrepræsentationens Sekretariat til godkendelse.	BR-Sekr.	Procedurer for adgangsstyring og brugeradgang. udarbejdes af Koncernservice. Skal til høring i forvaltningerne og godkendes af BR-Sekr.	Procedurerne udarbejdet 7 måneder efter it-sikkerhedsregulativets ikrafttræden.	7
It-sikkerhedslederne	§ 52, stk.6. It-sikkerhedslederne opretter og ajourfører inden for eget område en oversigt over, hvilke overordnede, der jf. stk. 5 kan anmode om tildeling af autorisationer til de enkelte medarbejdere.	BR-Sekr.	Oversigter udarbejdes.	7 måneder efter it-sikkerhedsregulativets ikrafttræden.	7
It-sikkerhedslederne	§ 56, stk. 1-3. Kontrol af tildelte autorisationer.	BR-Sekr.	Arbejdsgangsbeskrivelse udarbejdes. Beskrivelsen kan være relativ	Udarbejdet 8 måneder efter it-sikkerhedsregulativets ikrafttræden.	8

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
			enkel.		
Ledere, it-sikkerhedsledere, bruger-administrationen i Koncernservice	§ 57, stk.4. Ophører ansættelsesforholdet, eller er der i en periode ikke den fornødne arbejdsmæssige brug for at kunne udnytte brugerrettigheder, hvilket f.eks. kan være tilfældet ved længerevarende orlov, skal brugerrettighederne inddrages.	BR-Sekr.	Forretningsgangsbeskrivelse skal udarbejdes.	Forretningsgangsbeskrivelse skal være udarbejdet 8 måneder efter it-sikkerhedsregulativets ikrafttræden.	8
Systemejerne	§ 58. Systemejer meddeler de enkelte it-sikkerhedsledere de nærmere retningslinier for adgangsstyring til hvert enkelt system. Retningslinierne skal blandt andet beskrive, hvilke medarbejdergrupper der skal have adgang til it-systemet, samt hvilke oplysninger og funktioner den enkelte medarbejder kan få adgang til. Retningslinierne kan endvidere indeholde en beskrivelse af eventuel mulighed for anvendelse af rolleprofiler.	BR-Sekr.	Umiddelbart efter udpegning af systemejere udarbejdes retningslinier for adgangsstyring.	Retningslinier skal være udarbejdet 8 måneder efter it-sikkerhedsregulativets ikrafttræden.	8
	Styring af netværk				
Den it-ansvarlige	§ 61, stk. 1. Beskyttelse af netværk	BR-Sekr.	Vejledning om beskyttelse af netværk.	12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
Den it-ansvarlige	§ 61, stk. 2. Benyttede internetforbindelser	BR-Sekr.	Vejledning om ansvaret for de benyttede internetforbindelser.	12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
Den it-ansvarlige	§ 61, stk. 3. Brug af trådløse netværk må kun ske efter tilladelse fra den it-ansvarlige.	BR-Sekr.	Retningslinier for brug af trådløse netværk.	12 måneder efter it-sikkerhedsregulativets ikrafttræden skal retningslinier være udarbejdet.	12
Den it-	§ 62. Den it-ansvarlige skal sikre, at	BR-Sekr.	Retningslinier for brugen af	12 måneder efter it-	12

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
ansvarlige	medarbejderne alene får adgang til fælles netværk og dertil knyttede tjenester.		netværkstjenester.	sikkerhedsregulativets ikrafttræden skal retningslinier være udarbejdet.	
Den it-ansvarlige	§ 63. Den it-ansvarlige skal begrænse og styre adgangen til systemværktøjer, der kan påvirke eller omgå systemers eller enheders it-sikkerhed. Unødige systemværktøjer må ikke være installeret eller tilgængelige på medarbejderes computere. Adgangen til systemværktøjer skal begrænses til et minimum af godkendte medarbejdere.	BR-Sekr.	Vejledning om systemværktøjer.	Vejledning udarbejdet 12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
Den it-ansvarlige	§ 64. Den it-ansvarlige skal sikre, at der installeres de nødvendige antivirusprodukter til beskyttelse af systemer og oplysninger. Der skal installeres antivirus på alle it-systemer, hvor dette er muligt. Antivirus skal løbende opdateres.	BR-Sekr.	Vejledning om installation af antivirusprodukter.	Vejledning udarbejdet 6 måneder efter it-sikkerhedsregulativets ikrafttræden.	6
Den it-ansvarlige	§ 65. administrator adgangskoder.	BR-Sekr.	Forretningsgangsbeskrivelse om administrator koder.	6 måneder efter it-sikkerhedsregulativets ikrafttræden.	6
	Mobilt it-udstyr, herunder fjernarbejdspladser				
Den it-ansvarlige	§ 66. Fjernarbejdspladser tillades, når it-sikkerhedspolitikken overholdes.	BR-Sekr.	Vejledning om fjernarbejdspladser	12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
Den it-ansvarlige	§ 68. Anvendelse af mobilt it-udstyr.	BR-Sekr.	Vejledning om anvendelse af mobilt it-udstyr.	12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
	Kapitel 11 Anskaffelse, udvikling og				

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	vedligeholdelse af it-systemer				
	Anskaffelse af it-systemer				
Systemejerne, BR-Sekr.	§ 69. Ved anskaffelse og udvikling af it-systemer skal systemejer sikre, at anskaffelsen og udviklingen lever op til de gældende it-sikkerhedskrav.	BR-Sekr.	Vejledning om it-sikkerhedskrav til it-systemer	Vejledning skal foreligge 9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9
Systemejerne, BR-Sekr.	§ 69, stk. 4. Systemejer skal sikre, at leverandøren indgår en it-sikkerhedsaftale med kommunen og fremlægger en årlig revisorerklæring i henhold til "statsautoriserede revisors revisionsstandard RS3411 om generelle it-kontroller og applikationskontroller".	BR-Sekr.	Årligt. Systemejer fastsætter termin. Paradigme på it-sikkerhedsaftale	Inden udgangen af 2008 skal første erklæring foreligge. 6 måneder efter it-sikkerhedsregulativets ikrafttræden.	8 6
Systemejerne	§ 69, stk. 6. Risikovurdering af nye it-systemer.	BR-Sekr.	Paradigme på risikovurdering af it-systemer.	9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9
	Anskaffelse af it-udstyr				
Den it-ansvarlige	§ 71, stk. 1. Risikovurdering ved anskaffelse af udstyr.	BR-Sekr.	Paradigme på risikovurdering af it-udstyr.	9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9
	Interne kontroller for it-systemer				
Systemejerne	§ 72. Systemejer skal sikre, at der udarbejdes de nødvendige beskrivelser af interne kontroller ved anvendelse af it-systemet så der ved anvendelsen af it-systemerne sker en kontrol af oplysningernes korrekthed.	BR-Sekr.	Kontroller beskrives.	Beskrivelse af kontroller skal foreligge 12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
	Styring af driftsmiljøer				
Den it-ansvarlige	§ 73. Den it-ansvarlige skal sikre, at der sker lagring og backup af	BR-Sekr.	Årshjul. Hvert 4. år. I kraft ved it-sikkerhedsregulativets	Retningslinier for sikkerhedskopiering skal	9

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	oplysninger på serverudstyr. Det skal sikres, at der efter behov og i henhold til aftale tillige opbevares en sikkerhedskopi på en ekstern lokation. Den it-ansvarlige fastsætter nærmere retningslinier for sikkerhedskopieringen. Retningslinierne skal revideres mindst hvert 4. år.		ikrafttræden. Retningslinier skal udarbejdes.	foreligge og verificerede arbejdsgange for opbevaring for sikkerhedskopier på ekstern lokation skal være sat i værk 9 måneder efter it-sikkerhedsregulativets ikrafttræden.	
Systemejerne	§ 74, stk. 3. Kildekode til udviklingsprojekter skal sikres mod uautoriseret adgang og opbevares forsvarligt. Vedligeholdelse og kopiering af kildekode skal følge en dokumenteret procedure for ændringsstyring.	BR-Sekr.	Procedure for ændringsstyring.	Procedure for ændringsstyring skal være udarbejdet 12 måneder efter it-sikkerhedsregulativets ikrafttræden.	12
	Sårbarhedsstyring				
Den it-ansvarlige	§ 78, stk. 2. Den it-ansvarlige skal sikre, at det løbende vurderes, om der er behov for at installere rettelser til operativsystemer i kommunens interne driftsmiljø. Nødvendige rettelser installeres senest en uge efter gennemførelse af en positiv funktions- og kompatibilitetstest.	BR-Sekr.	Årshjul. Løbende. Forretningsgangsbeskrivelse fsva. behovet for at installere rettelser til operativsystemer.	9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9
Den it-ansvarlige	§ 78, stk. 3. Den it-ansvarlige skal sikre, at det løbende vurderes, om større operativsystemopdateringer og programpakkeopdateringer ("service packs") skal installeres i kommunens interne driftsmiljø.	BR-Sekr.	Årshjul. Halvårligt. Forretningsgangsbeskrivelse fsva. installation af service packs.	9 måneder efter it-sikkerhedsregulativets ikrafttræden.	9
	Kapitel 12 Styring af it-sikkerhedshændelser				

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
It-sikkerhedslederne	§ 79, stk. 4. It-sikkerhedslederen orienterer én gang årligt og inden udgangen af 4. kvartal vedkommendes fagudvalg om konstaterede it-sikkerhedsbrud. Såfremt der er flere it-sikkerhedsområder, som hører under det samme fagudvalg, koordinerer it-sikkerhedslederne for disse områder en samlet forelæggelse for fagudvalget.	BR-Sekr.	Årshjul. Årligt, ultimo 4. kvartal. Paradigme for orientering udarbejdes.	Første gang 6 måneder efter it-sikkerhedsregulativets ikrafttræden.	6
BR-Sekr.	§ 79, stk. 5. Borgerrepræsentationens Sekretariat orienterer én gang årligt og inden udgangen af 1. kvartal i det i forhold til stk. 4 efterfølgende år Økonomiudvalget om konstaterede it-sikkerhedsbrud.	ØU	Årshjul. Årligt, 1. kvartal. Paradigme for orientering udarbejdes.	Første gang 1. kvartal 2009.	9
BR-Sekr.	§ 80, stk. 3. Borgerrepræsentationens Sekretariat vurderer mindst en gang om året, om periodens hændelser giver anledning til forbedringer af it-sikkerheden.	ØU	Årshjul. Årligt, 2. kvartal (efter ØU har behandlet BR-Sekr's orientering).	Første gang 2. kvartal 2009.	12
Systemejerne	§ 81. Brugere, der observerer programfejl, som de ikke har oplevet før, skal rapportere dette til systemeieren eller rette vedkommende med henblik på videreformidling til systemeieren.	It-sikkerhedslederne	Oversigt over hvem rette vedkommende er.	Oversigter klar 7 måneder efter it-sikkerhedsregulativets ikrafttræden.	7
Koncernservice, eksterne samarbejdspartnere	§ 82. Koncernservice og eksterne samarbejdspartnere skal mindst en gang om måneden rapportere til relevante it-sikkerhedsledere, hvorvidt der er konstateret hændelser af betydning for it-sikkerheden og i bekræftende fald	BR-Sekr.	Årshjul. Månedligt. Paradigme for rapportering udarbejdes.	5 måneder efter it-sikkerhedsregulativets ikrafttræden.	5

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	beskrive disse hændelser nærmere.				
	Kapitel 13 It-beredskabsstyring				
BR-Sekr.	§ 83. Borgerrepræsentationens Sekretariat har ansvaret for, at der foreligger procedurer, som sikrer en tværorganisatorisk styring af it-beredskabet i tilfælde af større it-nedbrud mv. til uddybning af kommunes beredskabsplan.	Økonomiforvaltningens direktion, som BR-Sekr. hører under	Procedure skal laves.	Procedurer skal foreligge 6 måneder efter it-sikkerhedsregulativets ikrafttræden.	6
BR-Sekr., den it-ansvarlige	§ 83, stk. 2. Borgerrepræsentationens Sekretariat fastlægger i samarbejde med den it-ansvarlige i Koncernservice de overordnede retningslinier for udarbejdelse af it-beredskabsplanerne. It-beredskabsplanerne skal indeholde procedurer for iværksættelse af nødplaner, reetablering af it-systemer og begrænsning af skadevirkninger i tilfælde af større it-nedbrud.	Økonomiforvaltningens direktion, som BR-Sekr. hører under	Retningslinier for udarbejdelse af it-beredskabsplan.	Overordnede retningslinier skal foreligge 6 måneder efter it-sikkerhedsregulativets ikrafttræden.	6
Direktionerne, Borgerrådgiveren, Direktøren for Revisionsdirektoratet	§ 83, stk. 3. Direktionen henholdsvis Borgerrådgiveren og direktøren for Revisionsdirektoratet har inden for eget område ansvaret for, at der bliver udarbejdet en it-beredskabsplan som omfatter alle kritiske it-systemer og processer.	BR-Sekr.	Udarbejdelse af it-beredskabsplaner.	It-beredskabsplaner skal foreligge 10 måneder efter it-sikkerhedsregulativets ikrafttræden.	10
It-sikkerhedslederne	§ 73, stk. 4. It-sikkerhedslederen koordinerer inden for eget område arbejdet med udarbejdelse af it-beredskabsplaner og sikrer, at der foregår en tilstrækkelig uddannelse	BR-Sekr.	Årshjul. Årlig vurdering af uddannelsesbehov. Koordinering starter 6 måneder efter it-sikkerhedsregulativets	Uddannelse iværksættes, når it-beredskabsplaner foreligger 10 måneder efter it-sikkerhedsregulativets ikrafttræden.	10

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	af medarbejdere i de fastlagte it-beredskabsprocedurer.		ikrafttræden (når overordnede retningslinier foreligger).		
Den it-ansvarlige	§ 84. Den it-ansvarlige har inden for eget område ansvaret for at indgå aftale om it-beredskab, herunder den tekniske reetableringsplan med eksterne driftsleverandører og sikre, at disse bliver testet og vedligeholdt. It-sikkerhedslederen for det pågældende område og systemejerne for de it-systemer, som it-beredskabsplanen vedrører skal medvirke ved test af it-beredskabsplanen.	BR-Sekr.	Årshjul (test af planer). Frekvens og termin ikke fastsat for test. Det bør være op til den it-ansvarlige at beslutte dette. Paradigme på indgåelse af aftale om it-beredskab med driftsleverandører.	Beredskabsaftaler skal være indgået et år efter it-sikkerhedsregulativets ikrafttræden (ref. § 14, stk. 2). 9 måneder efter it-sikkerhedsregulativets ikrafttræden.	12 9
Systemejerne	§ 84, stk. 2. Systemejeren skal sikre, at der indgås aftale om it-beredskab for så vidt angår det it-system, som denne er systemejer for. Hvis flere it-systemer driftafvikles hos samme leverandør, skal it-beredskabsplanerne for disse it-systemer koordineres.	BR-Sekr.	Årshjul. (test af planer) Frekvens og termin ikke fastsat for test. Det bør være op til systemejeren at beslutte dette. Paradigme på indgåelse af aftale om it-beredskab fsva. it-systemer.	Beredskabsaftaler skal være indgået et år efter it-sikkerhedsregulativets ikrafttræden. 9 måneder efter it-sikkerhedsregulativets ikrafttræden.	12 9
Direktionerne	§ 85. Direktionen henholdsvis ledelsen har inden for eget område ansvaret for at sikre, at der er tegnet en tilstrækkelig forsikring af det af området anvendte it-udstyr, software, it-systemer og oplysninger. Stk. 2. Direktionen for Koncernservice har, ud over det i stk. 1 nævnte, ansvaret for at sikre, at der er tegnet en tilstrækkelig forsikring for netværksudstyr og	BR-Sekr.	Årshjul. Forsikringsbehov bør genovervejes periodisk.	Forsikringsbehov skal være opgjort 9 måneder efter it-sikkerhedsregulativets ikrafttræden. Forsikringsaftaler skal være indgået 15 måneder efter it-sikkerhedsregulativets ikrafttræden.	9 15

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
	servere m.v., som ejes af Koncernservice.				
	Kapitel 14 Lovbestemte krav				
BR-Sekr.	<p>§ 87, stk. 2. Medarbejdere skal særligt være opmærksomme på følgende forhold:</p> <p>a) om reglerne i persondataloven skal iagttages og i givet fald,</p> <p>b) om behandlingen overholder de grundlæggende krav og er hjemlet efter bestemmelserne i persondatalovens kapitel 4,</p> <p>c) om kommunen har opfyldt en evt. oplysningspligt over for den registrerede,</p> <p>d) om kommunen i fornødent omfang har givet den registrerede indsigt og behandlet evt. indsigelser mv.,</p> <p>e) om der er en eventuel anmeldelsespligt, og i så fald om it-sikkerhedslederen er orienteret herom,</p> <p>f) om it-sikkerhedsbestemmelserne er opfyldt.</p>	Økonomiforvaltningens direktion, som BR-Sekr. hører under	<p>Vejledninger til litra a-f skal udarbejdes.</p> <p>Arbejdsgangsbeskrivelse ift. litra d om indsigt skal udarbejdes.</p>	16 måneder efter it-sikkerhedsregulativets ikrafttræden.	16
	Kapitel 15 Revision af it-sikkerhed				
Den eksterne revision	§ 88. Som led i den almindelige revision af kommunen skal også foretages revision af it-sikkerheden.	ØKF's direktion, BR-Sekr.	Den nye eksterne revision skal klarlægge i hvor høj grad det nuværende it-sikkerhedsregulativ var overholdt. Starter umiddelbart efter	01.07.2009	19

Ansvar for udførelse	Bestemmelse	Ansvar for opfølgning	Aktivitet/ aktivitet start	Aktivitet slut	Status i mdr. regnet fra it-sikkerhedsreg.s ikrafttræden
			etablering af den eksterne revision		
	Kapitel 16 I krafttrædelse og ændringer				
BR-Sekr.	§ 90. Borgerrepræsentationens Sekretariat vurderer hvert år inden udgangen af juni måned, om it-sikkerhedsregulativet er i overensstemmelse med it-sikkerhedspolitikken, og om der er behov for ændringer i it-sikkerhedsregulativet.	Økonomiforvaltningens direktion, som BR-Sekr. hører under	Årshjul. Årligt, inden udgangen af juni måned.	Første gang juni 2009	14