DEPARTEMENTENE

Strategi

Nasjonal strategi for informasjonssikkerhet

DEPARTEMENTENE

Strategi

Nasjonal strategi for informasjonssikkerhet

Innhold

Forord 6

1 Innledning 8

1.1 Målgruppe 10

1.2 Bakgrunn 11

2 Sikkerhetsutfordringer og trender 12

3 Departementenes roller og ansvar for informasjonssikkerheten 15

4 Overordnede mål og strategiske prioriteringer 17

4.1 Ivareta informasjonssikkerheten på en mer helhetlig og systematisk måte 17

4.2 Styrke IKT-infrastrukturen 18

4.3 Sørge for en felles tilnærming til informasjonssikkerhet i statsforvaltningen 20

4.4 Sikre samfunnets evne til å oppdage, varsle og håndtere alvorlige IKT-hendelser 21

4.5 Sikre samfunnets evne til å forebygge, avdekke og etterforske datakriminalitet 22

4.6 Kontinuerlig innsats for bevisstgjøring og kompetanseheving 23

4.7 Høy kvalitet på nasjonal forskning og utvikling innenfor informasjons-og kommunikasjonssikkerhet 24

5 Ansvar for gjennomføring 26

6 Økonomiske og administrative konsekvenser 27

Vedlegg A: Ord og uttrykk 28

Vedlegg B: Utvalgte nasjonale kontaktpunkter for informasjonssikkerhet 30

Forord

Informasjonsteknologi har skapt store endringer i samfunnet de siste tiårene. Gevinstene har vært betydelige for innbyggere, næringsliv og samfunnet som helhet. IKT-systemene er blitt stadig mer integrert i alle deler av samfunnet. Befolkningen får et bedre og mer mangfoldig tjenestetilbud. Teknologi utgjør nå grunnmuren for all samhandling på tvers av sektorer. IKT har dermed blitt en strategisk sikkerhetsutfordring. Infrastrukturen som ligger til grunn for at tjenestene fungerer, har blitt kritisk for at samfunnet skal fungere normalt.

Økt bruk av IKT gjør at samfunnet blir mer sårbart. Truslene mot IKT-systemene øker, og angrepene blir stadig mer avanserte. God forebyggende informasjonssikkerhet blir derfor stadig viktigere for samfunnssikkerheten. Med *informasjonssikkerhet* mener vi at informasjonen er beskyttet mot uønsket innsyn, at den er tilgjengelig når den trengs, og at den er beskyttet mot uønskede endringer.

Våre nettverk og systemer må være sikre og stabile til enhver tid. Næringslivet, forvaltningen og befolkningen må ha tillit til at de digitale tjenestene i samfunnet fungerer. Gjennom utgivelsen av en nasjonal strategi for informasjonssikkerhet angir regjeringen hvilken retning og hvilke prioriteringer som skal ligge til grunn for myndighetenes informasjons-sikkerhetsarbeid. Strategien beskriver eksisterende sikkerhetsutfordringer og hvilke områder som skal vektlegges for å møte disse og fremtidige utfordringer.

Informasjonssikkerhet krever grenseoverskridende tiltak og spenner over teknologi, retningslinjer, holdninger og kultur. Strategien er utarbeidet i samarbeid mellom Forsvarsdepartementet, Justis- og beredskapsdepartementet, Samferdselsdepartementet og Fornyings-, administrasjons- og kirkedepartementet. En rådgivende gruppe med representanter fra myndighetsorganer og næringslivet har bistått departementene i arbeidet med strategien.

For å få en helhetlig tilnærming til dagens utfordringer har også forslaget til cybersikkerhetsstrategi som Nasjonal sikkerhetsmyndighet utarbeidet i 2009, og innspill fra høringsrunden til denne, inngått som et viktig grunnlagsmateriale for informasjonssikkerhetsstrategien og tilhørende handlingsplan.

IKT er et meget dynamisk fagfelt, og sikkerhets-utfordringene er i stadig endring. Nasjonal strategi for informasjonssikkerhet vil derfor bli revidert i takt med utviklingen.

17. desember 2012

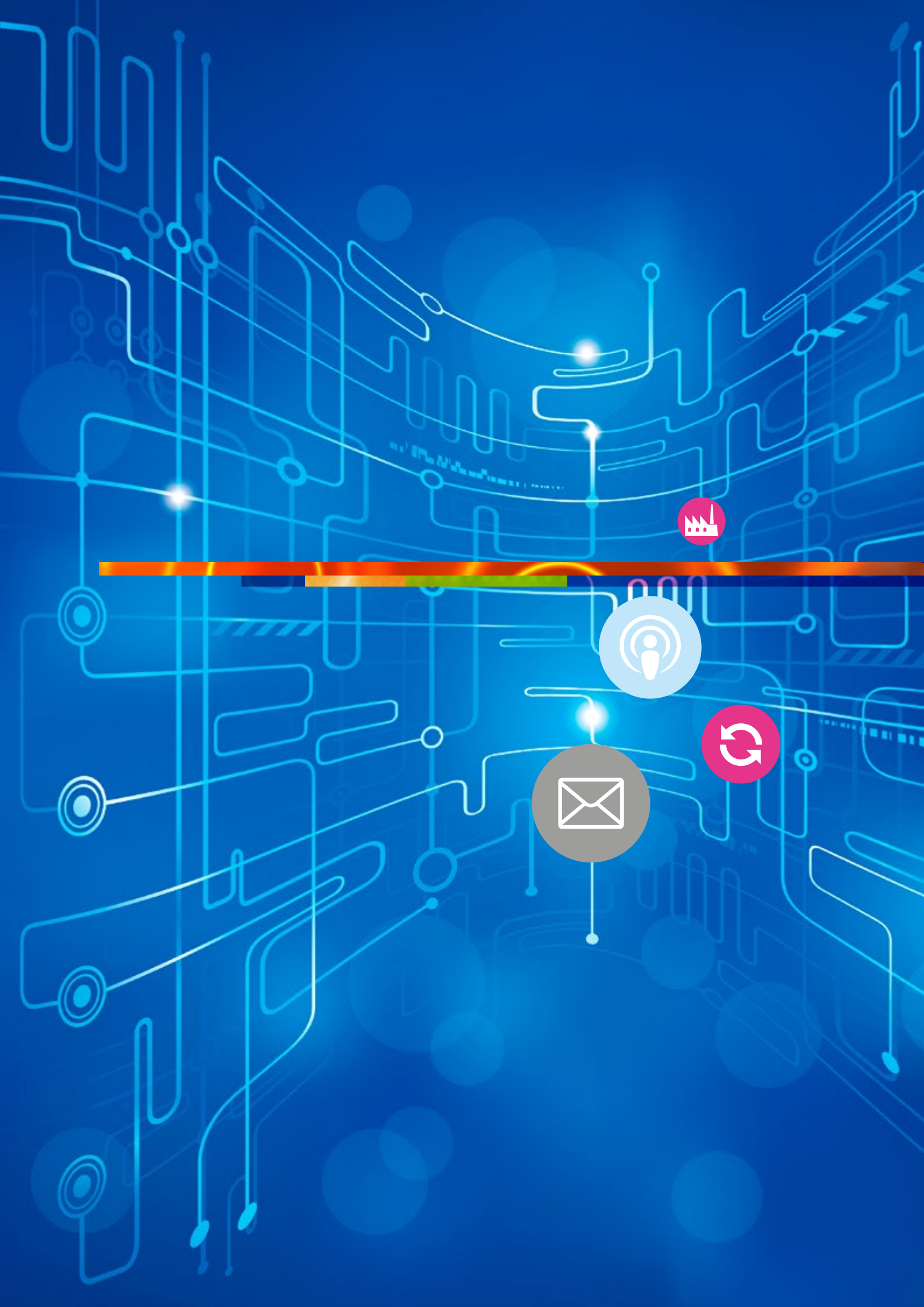
Justis- og beredskapsminster Grete Faremo
Forsvarsminister Anne-Grete Strøm-Erichsen
Samferdselsminister Marit Arnstad
Fornyings-, administrasjons- og kirkeminister
Rigmor Aasrud

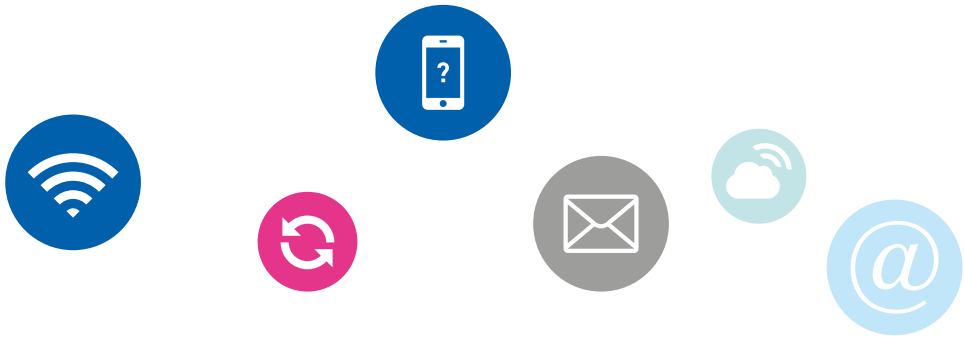
Foto: Torgeir Haugaard

Foto: Torgeir Haugaard

Foto: Olav Heggø

Foto: Johnny Syversen





1 Innledning

Utviklingen innen informasjons- og kommunikasjonsteknologi (IKT) har skapt store endringer i samfunnet de siste tiårene. Internett har skapt store samfunnsmessige fordeler for Norge. Gevinstene har vært betydelige for innbyggere, næringsliv og samfunnet som helhet. IKT-systemer blir stadig viktigere, stadig mer integrert i alle deler av samfunnet og er kritisk for at samfunnet skal fungere normalt. Teknologien er en integrert del av vårt arbeids- og hverdagsliv. Befolkningen er i mange sammenhenger avhengig av IKT for å få utført en tjeneste. IKT utgjør nå grunnmuren for all samhandling på tvers av sektorer, og kan betraktes som en grunnleggende infrastruktur i samfunnet.

De store samfunnsgevinstene har gjort at IKT bevisst har blitt tatt i bruk. Men samtidig har det gjort IKT til en strategisk sikkerhetsutfordring.

Samfunnet vil utvikles videre gjennom stadig mer utstrakt bruk av IKT. Da er det også behov for å beskytte informasjonen og sørge for at våre nettverk og systemer er sikre og stabile til enhver tid. Befolkningen, næringslivet og forvaltningen må ha tillit til at de digitale tjenestene i samfunnet fungerer.

Formålet med sikkerhetsarbeidet innen IKT er at tilstanden i Norge skal preges av at:

- Alle aktører er kjent med risikobildet, og sikrer sine systemer og nett i henhold til dette.
- Myndighetene legger aktivt til rette for at den nasjonale IKT-infrastrukturen er godt sikret, gjennom rett organisering, tilstrekkelig ressursbruk, gode rammevilkår og effektive tiltak.
- Private og offentlige virksomheter bygger sikkerhet og robusthet inn i sin informasjonsinfrastruktur for å sikre egen virksomhet og for å beskytte sine kunder og brukere.
- Den enkelte tar et selvstendig initiativ for å beskytte sin identitet, sitt eget personvern og sine egne økonomiske verdier på nett.

Informasjonssikkerhet handler om hvordan informasjonens konfidensialitet, integritet og tilgjengelighet blir ivaretatt.

Integritet - Sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter.

Konfidensialitet - Sikkerhet for at nærmere angitt informasjon ikke avsløres for uvedkommende, og at kun autoriserte personer får tilgang til denne.

Tilgjengelighet - Sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov.

Integritet, konfidensialitet og tilgjengelighet er alle viktige faktorer når det gjelder å ivareta IKT-sikkerheten i samfunnet. Den enkelte virksomhet vil vekte de ulike faktorene ulikt ut fra hvilket formål virksomheten har eller skal understøtte, og hvilket risikobilde den må forholde seg til.

Informasjonssikkerhet er en kontinuerlig prosess. Det som var god sikkerhet i går, er ikke nødvendigvis godt nok i dag eller i morgen. Vi må vedlikeholde og oppdatere teknisk kunnskap og være sikkerhetsbevisste dersom vi skal oppnå full effekt av innsatsen på området. Den raske teknologiske utviklingen gjør at det stadig dukker opp nye sikkerhetsutfordringer i takt med introduksjon av nye produkter, nye tekniske løsninger, og endrede bruksmønstre.

Regjeringens hovedformål med å utgi en nasjonal strategi for informasjonssikkerhet er å angi hvilken retning og hvilke prioriteringer som skal ligge til grunn for myndighetenes informasjonssikkerhetsarbeid i de nærmeste årene. For hver strategiske prioritering er det angitt en målbeskrivelse for satsingen, statusbeskrivelse og utvalgte områder som skal vektlegges framover. Hvordan regjeringen skal følge opp strategiens utvalgte områder vil framgå av en detaljert handlingsplan. Handlingsplanen utgis separat, og skal revideres ved behov. Oppfølgingen av strategien skal dessuten bidra til at beslutningstakere i offentlig og privat sektor spesielt, og befolkningen generelt, skal få økt bevissthet om hvilke sikkerhetsutfordringer vi står overfor.

1.1 Målgruppe

Myndighetene spiller en sentral rolle når det gjelder å tilrettelegge for og påvirke hvordan IKT utvikles og tas i bruk i samfunnet. Dette omfatter også informasjonssikkerhet. Myndighetene gjør dette blant annet gjennom utforming og håndheving av lover og forskrifter, tilsyn, informasjonsdeling og gjennom råd og veiledning. Den nasjonale strategien for informasjonssikkerhet, med tilhørende handlingsplan, utfyller og viser retning for utviklingen av det eksisterende regelverket og virkemiddelapparatet. Strategien er et uttrykk for regjeringens overordnede prioriteringer på området.

Regjeringen har det overordnede ansvaret for myndighetenes arbeid med informasjonssikkerhet. For å kunne ivareta dette ansvaret må myndighetene ha et tett samarbeid med alle relevante aktører i offentlig og privat sektor. Det finnes også en rekke spesialorganer som har IKT-sikkerhet som et særskilt ansvar jf. vedlegg B.

Det er *departementene* som er ansvarlige for å sørge for at alle relevante aktører i sektorene blir inkludert i gjennomføringen av tiltak innenfor strategiens strategiske prioriteringer.

Ledere i fylkeskommunene, kommunene og næringslivet har et selvstendig ansvar, ut fra sine ulike roller, for å følge opp informasjonssikkerhetsarbeidet i egen sektor eller virksomhet. De må, ut fra eget ansvar og initiativ, gjennomføre nødvendige tiltak som kan bidra til å understøtte strategiens strategiske prioriteringer.

Utover dette har *alle* et selvstendig ansvar for å bidra til å opprettholde og styrke informasjonssikkerheten i samfunnet. En velfungerende hverdagssikkerhet er en grunnforutsetning for å kunne håndtere mer alvorlige hendelser effektivt.

1.2 Bakgrunn

Problemstillingene knyttet til informasjonssikkerhet er ikke nye. Disse utfordringene har vært omtalt og håndtert av skiftende regjeringer i flere tiår. Dette gjelder for eksempel håndtering av personopplysninger, sikring av statshemmeligheter og beskyttelse av samfunnskritisk infrastruktur. Det er lagt ned et stort arbeid både i offentlig og privat sektor for å følge opp de ulike utredningenes anbefalinger om tiltak.

I Sårbarhetsutvalgets rapport, NOU 2000:24 *Et sårbart samfunn,* ble det slått fast at IKT-systemene har blitt en av samfunnets bærebjelker, og at samfunnet har blitt mer sårbart for svikt i disse systemene. Utvalget la i denne sammenheng stor vekt på å formidle betydningen av IKT-sårbarhet som en del av samfunnets totale sårbarhet. Utvalget foreslo en rekke tiltak for å bøte på sikkerhetsutfordringene, herunder utvikling av en nasjonal strategi for å redusere sårbarheten på IKT-området.

Sårbarhetsutvalgets arbeid var en viktig premiss for arbeidet med St. meld. nr. 17 (2001–2002) *Samfunnssikkerhet. Veien til et mindre sårbart samfunn.* Denne meldingen gir blant annet en oversikt over en rekke anbefalte sårbarhetsreduserende tiltak innenfor IKT.

Infrastrukturutvalget startet i 2004 opp en utredning av behovet for sikring av landets kritiske infrastruktur. Utvalgets forslag ble lagt frem i NOU 2006: 6 *Når sikkerheten er viktigst*. Infrastrukturutvalgets anbefalinger ble vurdert og fulgt opp i St.meld. nr. 22 (2007–2008) *Samfunnsikkerhet*. I meldingen blir blant annet den nasjonale CERT-funksjonen (Computer Emergency Response Team) forankret og beskrevet.

I Meld. St. 29 (2011–2012) *Samfunnssikkerhet* konstateres det at utviklingen i blant annet internett, flere mobile tjenester, nye tjenesteplattformer og mer bruk av utenlandske tjenester medfører at IKT har blitt en strategisk sikkerhetsutfordring. Denne utviklingen setter store krav til bevissthet og kompetanse, og forsterker behovet for samarbeid og samordning på tvers av ulike samfunnsområder.

Den første nasjonale strategien for informasjonssikkerhet forelå i juni 2003, og var en felles utgivelse av Nærings- og handelsdepartementet, Forsvarsdepartementet og Justis- og politidepartementet. I løpet av strategiperioden 2003-2006 ble det gjennomført flere konkrete tiltak og aktiviteter. Sikring av kritisk IKT-infrastruktur ble gitt prioritet. Samtidig ble organiseringen av arbeidet styrket i løpet av denne perioden. Strategien ble fulgt opp med utgivelsen av *Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007–2010*.

2 Sikkerhetsutfordringer og trender

Sikkerhetsutfordringene innen IKT omfatter alle nivåer i samfunnet fra beskyttelse av enkeltpersoners mobiltelefoner til beskyttelse av systemer som er avgjørende for samfunnskritiske funksjoner.

Noen av de utfordringene og trendene som kjennetegner dagens situasjon er:

Internett og mobile enheter. Økt utbredelse av internett og bruken av nye datasystemer, styringssystemer for industri, mobiltelefoner, minnepinner, sosiale medier og lesebrett har gjort oss mer effektive, men samtidig mer sårbare.

Driftsavbrudd stadig mer kritisk. Samfunnet har blitt mer sårbart for selv kortere driftsavbrudd i systemer og nett. Betydningen av en sikker og robust IKT-infrastruktur har således blitt større.

Nye tjenesteplattformer og uoversiktlighet. Økt bruk av nye typer tjenesteplattformer, som for eksempel nettbaserte tjenester og bruk av nettskyen, skaper en uoversiktlighet som kan gjøre det mer krevende for brukere av denne teknologien å vurdere risiko og sårbarhet, og dokumentere egen sikkerhet.

Økt bruk av utenlandske tjenesteleverandører. Norske virksomheter setter i økende grad ut drifts- og systemutviklingsoppgaver til leverandører som befinner seg i andre land og på andre kontinent. Dette reiser en rekke sikkerhets- og beredskapsutfordringer. Lokale driftsforhold og andre lands regelverk og praksis på området kan for eksempel avvike fra norske krav til sikker IKT-drift eller regelverk knyttet til personvern og behandling av personopplysninger. Nasjonalt tilsyn og mulighetene til å føre kontroll med hvordan den utkontrakterte virksomheten håndterer data kan bli svekket.

Et marked for kriminalitet. Internett og mobile enheter har ført til en større risiko for å bli utsatt for datakriminalitet. Det eksisterer i dag et undergrunnsmarked, lett tilgjengelig på internett, for kjøp og salg av informasjon og omsetning av verktøy for å utføre datakriminalitet. De som utfører kriminell virksomhet utnytter dette i stadig større grad.

Spionasje og sabotasje – en økende trussel. Tendensen til målrettede og profesjonelle datainnbrudd mot kritiske IKT-systemer er økende. Målrettede spionasjeangrep rettet mot vitale nasjonale sikkerhetsinteresser utgjør nå en betydelig utfordring. Både sivile etater, militære

enheter og private selskaper blir utsatt for spionasje og sabotasje. Mange stater utvikler evne til å drive etterretning og krigføring mot kritisk infrastruktur. Vi må regne med at sofistikerte sabotasje- og påvirkningsangrep vil bli rettet mot samfunnskritiske informasjonsressurser, herunder datasystemer som styrer industriprosesser og kritisk infrastruktur.

Store krav til bevissthet og kompetanse. Nye tjenester og enheter stiller store krav til kompetansen hos vanlige brukere. Det er krevende for eiere av kritisk infrastruktur å ha tilstrekkelig bevissthet og kunnskap om sårbarheter, gjensidige avhengigheter mellom komponenter i infrastrukturen, og hva den enkelte virksomhet må gjøre for å beskytte infrastrukturen.

Økt kompleksitet. De fleste virksomheter har i dag en systemportefølje som er langt mer kompleks enn for bare få år siden. IKT inngår nå tilnærmelsesvis i alle nye produkter og systemer, og det forutsettes at disse skal kunne samspille sømløst med andre systemer, og på tvers av virksomheter og sektorer. Det er en utfordring å holde oversikt over alle gjensidige avhengigheter og potensielle sårbarheter. Den økte kompleksiteten i systemer og nett har også gjort det vanskeligere for bestillere av IKT-systemer å stille klare og presise krav til sikkerhet.

Utro tjenere. Internt skadeverk, tyveri eller misbruk av virksomhetens IKT-ressurser fra egne ansatte kan være vanskelig å avdekke. Dette skyldes blant annet at mange virksomheter har dårlige eller svake drifts- og forvaltningsrutiner, eller at de ansatte har systemrettigheter som virksomhetsledelsen ikke har full kontroll over. Interne angrep mot datanettet kan dessuten være vanskeligere å avdekke enn angrep utenfra.

Personvern og identitetsmisbruk. Personvernet blir også utfordret av nye måter å kommunisere og bruke informasjonssystemer og nett på. Misbruk av identitet er en økende utfordring for både privatpersoner, virksomheter og myndighetene.

Internasjonal oppmerksomhet. Informasjonssikkerhet er et område som mange land og internasjonale organisasjoner framhever som stadig viktigere for økonomisk vekst, samfunnssikkerhet og nasjonal og internasjonal sikkerhetspolitikk. Mange land har utarbeidet egne strategier og retningslinjer for arbeidet med informasjonssikkerhet. De enkelte lands gjensidige forpliktelser overfor fellesskap og allianser har et betydelig fokus i denne sammenheng.

Svakheter i informasjonssikkerheten. Riksrevisjonen har tidligere avdekket store svakheter i informasjonssikkerheten i statsforvaltningen gjennom Dokument 1 (2010-2011). Nasjonal sikkerhetsmyndighet slår fast i *Rapport om sikkerhetstilstanden 2011* at IKT-systemer som er viktige for samfunnet ofte ikke er godt nok sikret, og at truslene som virksomhetene blir utsatt for øker.

Mørketallsundersøkelsen 2012, fra Næringslivets Sikkerhetsråd, har påpekt at gapet mellom trusler og sikkerhetstiltak blant norske virksomheter øker – både i offentlig og privat sektor – parallelt med at virksomhetenes IKT-avhengighet øker.

Sikkerhetsutfordringer og trender er mer utdypende omtalt i regjeringens handlingsplan for informasjonssikkerhet.

3 Departementenes roller og ansvar for informasjons-sikkerheten

Virksomhetenes ansvar

IKT-sikkerhet er først og fremst den enkelte virksomhets ansvar. Dette følger av ansvarsprinsippet, som innebærer at den som har et ansvar for en virksomhet under normale forhold, også har et ansvar i en krisesituasjon. I praksis innebærer dette at ansvaret ligger hos eieren av virksomheten uansett om denne befinner seg i privat eller offentlig sektor.

Større nasjonale IKT-sikkerhetstiltak planlegges og iverksettes i et tett samarbeid mellom myndighetene og den enkelte virksomhet. Den nasjonale sikkerhetstilstanden er summen av alt sikkerhetsarbeidet som foregår i virksomhetene, i den enkelte sektor og på nasjonalt nivå. En god sikkerhetskultur i virksomhetene reduserer sjansen for at ansatte blir det svakeste ledd i våre sikkerhetsbarrierer.

Fagdepartementenes ansvar

Fagdepartementene har et overordnet ansvar for å ivareta sikkerheten i sektorens IKT-infrastruktur, og for at det forebyggende informasjonssikkerhetsarbeidet i sektoren er tilfredsstillende. Dette innebærer at hvert enkelt fagdepartement har ansvar for å:

- identifisere kritisk infrastruktur i egen sektor, og sørge for tilfredsstillende sikring
- vurdere, beslutte og iverksette tiltak av forebyggende karakter i egen sektor
- forberede beredskapstiltak med tanke på forskjellige krisesituasjoner
- planlegge for, og ved behov å iverksette, krisehåndtering innen egen sektor
- føre tilsyn med, og følge opp arbeidet med informasjonssikkerheten i egne underlagte etater

I praksis vil de fleste av disse oppgavene bli utført av etatene eller underlagte virksomheter ettersom det er disse som best kjenner til virksomhetens avhengighet av viktige informasjonssystemer og infrastruktur.

Departementer med et særlig ansvar for IKT-sikkerhet

Basert på ovennevnte ansvarsfordeling foregår hovedtyngden av alt IKT-sikkerhetsarbeid i den enkelte sektor, og da primært i den enkelte virksomhet. Utover dette har enkelte departementer en særskilt rolle knyttet til IKT-sikkerhet.

Justis- og beredskapsdepartementet har samordningsansvar for samfunnets sivile sikkerhet. Ved siden av å initiere, utvikle og gjennomføre tiltak gjennom egne virkemidler, er departementet en pådriver og koordinator overfor andre sektormyndigheter. Justis- og beredskapsdepartementet skal overta og videreutvikle ansvaret for IKT-sikkerhet i samfunnet.

Fornyings-, administrasjons, og kirkedepartementet er ansvarlig for koordinering av regjeringens IKT-politikk. Departementet har også et særskilt ansvar for å arbeide for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen.

Forsvarsdepartementet har ansvar for alt arbeid med forebyggende IKT-sikkerhet knyttet til militær sektor. Forsvarsdepartementet har etatsstyringsansvar for Nasjonal sikkerhetsmyndighet, og forvaltningsansvaret for sikkerhetsloven.

Samferdselsdepartementet har som sektordepartement ansvar for IKT-sikkerheten knyttet til elektroniske kommunikasjonsnett og -tjenester, herunder internett. Dette reguleres gjennom lov om elektronisk kommunikasjon med forskrifter. Post- og teletilsynet har, som myndighetsorgan under Samferdselsdepartementet, et særskilt ansvar knyttet til sikkerhet og beredskap i elektroniske kommunikasjonsnett og -tjenester.

Selv om informasjonssikkerhet først og fremst er et virksomhets- og sektoransvar, krever det stadig mer nettverksbaserte samfunnet en helhetlig tilnærming. IKT-infrastrukturen og sikkerhetsutfordringene går på tvers av etablerte virksomheter og sektorer. En effektiv beskyttelse av IKT-infrastrukturen vil forutsette god samordning mellom myndighetene, næringslivet og den enkelte bruker.

4 Overordnede mål og strategiske prioriteringer

Strategien omhandler i hovedtrekk de utfordringene som samfunnet i fellesskap må bidra til å løse. Med bakgrunn i blant annet de sikkerhetsutfordringer og trender som er omtalt i strategiens kapittel 2, har regjeringen utpekt fire overordnede mål for informasjonssikkerhetsarbeidet:

1. Styrket samordning og felles situasjonsforståelse
2. Robust og sikker IKT-infrastruktur i hele samfunnet
3. Sterk evne til å håndtere uønskede IKT-hendelser
4. Høy kompetanse og sikkerhetsbevissthet

Regjeringens overordnede mål for informasjonssikkerhetsarbeidet er likeverdige, og må virke sammen for å oppnå den ønskede tilstand.

De overordnede målene skal operasjonaliseres gjennom sju strategiske prioriteringer:

- Ivareta informasjonssikkerheten på en mer helhetlig og systematisk måte
- Styrke IKT-infrastrukturen
- Sørge for en felles tilnærming til informasjonssikkerhet i statsforvaltningen
- Sikre samfunnets evne til å oppdage, varsle og håndtere alvorlige IKT-hendelser
- Sikre samfunnets evne til å forebygge, avdekke og etterforske datakriminalitet
- Kontinuerlig innsats for bevisstgjøring og kompetanseheving
- Høy kvalitet på nasjonal forskning og utvikling innenfor informasjons- og kommunikasjonssikkerhet

I strategien gis det også en kort statusbeskrivelse på området, og det pekes på utvalgte områder som skal vektlegges i årene framover. Prosesser for den videre konkretiseringen av de strategiske prioriteringene, og gjennomføring av konkrete tiltak, er beskrevet i strategiens kapittel 5. Hvordan regjeringen skal følge opp strategien gjennom konkrete tiltak vil framgå av en handlingsplan. Denne handlingsplanen utgis separat, og skal revideres ved behov.

4.1 Ivareta informasjonssikkerheten på en mer helhetlig og systematisk måte

Private og offentlige virksomheter skal ivareta informasjonssikkerheten *helhetlig og systematisk*. Dette krever bevisst bruk av styringssystemer for informasjonssikkerhet som en del av virksomhetsstyringen. Anerkjente standarder skal legges til grunn. Kravene må tilpasses den risikoen den enkelte virksomhet må håndtere. Virksomhetens karakter, størrelse og samfunnsmessige betydning må være avgjørende for ambisjonsnivået og ressursinnsatsen på sikkerhetsarbeidet.

Flere regelverk pålegger virksomhetene å ha et styringssystem for informasjonssikkerhet. Dette fremgår blant annet av e-forvaltningsforskriften som gjelder i hele offentlig sektor. Forskrift til personopplysningsloven gjelder både privat og offentlig sektor. I tillegg gjelder sikkerhetsloven i hele offentlig sektor og bestemte deler av privat sektor. I flere av regelverkene er det krav om at sikkerheten skal være tilpasset risikoen. Det er derfor viktig at forvaltningen gjør gode risiko- og sårbarhetsvurderinger. Datatilsynet, Nasjonal sikkerhetsmyndighet og Riksrevisjonen har avdekket svakheter i forvaltningens risikovurderinger. Det er påpekt at eksisterende sikkerhetstiltak ofte er lite systematiske, fragmenterte, og at arbeidet med informasjonssikkerhet verken er tilstrekkelig forankret i virksomhetens ledelse eller godt integrert i virksomhetsstyringen. Det antas at økt bruk av internasjonale sikkerhetsstandarder i

statsforvaltningen vil kunne bidra til bedre helhet og systematikk i sikkerhetsarbeidet. Økt bruk av sertifiserte IKT-produkter og -systemer kan også være med på å styrke tilliten til og bedre sikkerhetsnivået til offentlig sektors systemer og tjenester i Norge.

Dette området skal vektlegges:

- Alle etater og statlige virksomheter skal ha et styringssystem for informasjonssikkerhet. Styringssystemet skal bygge på anerkjente sikkerhetsstandarder. Systemets omfang og detaljeringsgrad skal tilpasses risikoen til den enkelte virksomhet og virksomhetenes omfang og art. Kommunesektoren og private virksomheter skal oppfordres til å etablere tilsvarende styringssystemer.

4.2 Styrke IKT-infrastrukturen

IKT- infrastruktur som understøtter samfunnskritiske funksjoner skal være robust og pålitelig slik at uønskede hendelser og handlinger i størst mulig grad kan unngås. Kraftforsyningen og elektroniske kommunikasjonsnett må ha særlig fokus. Det er en overordnet målsetning å sikre at alle aktører i offentlig sektor og privat næringsliv må forholde seg til klare krav og får nødvendige råd og veiledning, slik at de kan bestille og forvalte elektroniske kommunikasjonstjenester som har et forsvarlig sikkerhetsnivå sett ut fra den risiko som den enkelte virksomhet står overfor. Tilsvarende krav skal stilles til eiere av virksomheter som drifter samfunnsviktige funksjoner.

Den teknologiske utviklingen gjør at IKT-infrastrukturen er i kontinuerlig endring. Deler av den vil stadig fornyes. Det tradisjonelle telenettet som formidlet talekommunikasjon erstattes av elektroniske kommunikasjonsnett som brukes for alle slags tjenester. Det er derfor vanskelig å peke ut enkelte deler av IKT-infrastrukturen som kritisk og andre deler som mindre viktig for samfunnssikkerheten.

Det er viktig å understreke at det finnes flere elektroniske kommunikasjonsnett. Brukere som er avhengig av elektronisk kommunikasjon må være i stand til å bruke alternative kommunikasjonsløsninger. Brukerne må ha tilstrekkelig kompetanse til å velge hensiktsmessige løsninger og stille krav til tilbyderne om tjenestekvalitet og pålitelighet. Dette krever at det finnes gode veiledninger for brukerne.

For å skape økt redundans og en mer robust infrastruktur, må behovet for sikkerhet veies opp mot hensynet til miljø og samfunnsøkonomi når infrastrukturen planlegges og bygges ut. Hensyn til miljø og samfunnsøkonomi blir ofte vektlagt ved etablering av infrastruktur, slik at det eksempelvis legges til rette for at flere aktører følger samme trasé for framføring av kabler, bruker felles master for antenner, og at det tekniske utstyret for flere aktører kan samlokaliseres i bygninger. Erfaringer viser at dette kan gå på bekostning av sikkerhetshensyn. Samtidig vil sikringstiltak for én type infrastruktur kunne gi beskyttelse for annen infrastruktur som følger samme trasé. Et eksempel er at skredsikring av en vei også kan bidra til å sikre kabler som er lagt langs den samme veien.

Iverksettelse av endringene i sikkerhetslovens objektsikkerhetsbestemmelser er et viktig virkemiddel for å få identifisert samfunnskritiske funksjoner og avdekket innbyrdes avhengigheter mellom disse. Slik styrkes den nasjonale IKT- og samfunnssikkerheten.

Utvalgte områder som skal vektlegges:

- Fagmyndighetene skal stille krav til driftskontinuitet i systemer som er nødvendige for å opprettholde viktige samfunnsfunksjoner.

- Sikringstiltak for fysisk infrastruktur skal være koordinert på tvers av sektorer slik at de forskjellige tiltakene virker sammen og ikke kommer i konflikt med hverandre.

- Det skal regelmessig øves på situasjoner der deler av infrastrukturen har redusert kapasitet eller faller ut.

- Fagdepartementene skal følge opp at sektorens virksomheter identifiserer og foreslår IKT-funksjoner og -systemer som kan klassifiseres som samfunnskritiske i henhold til objektsikkerhetsregelverket.

4.3 Sørge for en felles tilnærming til informasjonssikkerhet i statsforvaltningen

Digital kommunikasjon skal være hovedregelen for kommunikasjon i og med forvaltningen. Befolkningen, næringslivet og forvaltningen selv skal ha tillit til at elektroniske tjenester i statlig sektor er sikre og pålitelige og at fagsystemer og elektroniske tjenester også er det. Det skal derfor etableres felles statlige løsninger for sikker kommunikasjon og sikker tilgang til tjenester. Eksempler på slike fellesløsninger er ID-porten og en offentlig utstedt elektronisk ID (eID) på høyt nivå. I tillegg til en sikkerhetsmessig gevinst, vil en sentralisert tilnærming også innebære en økonomisk besparelse i form av mer enhetlig utvikling og drift av systemene. Statlige myndigheter skal sørge for at det tydeliggjøres hvilke generelle rettslige, organisatoriske og tekniske sikkerhetskrav som skal gjelde for departementene med underlagte virksomheter, sentrale infrastruktureiere og eiere av graderte IKT-systemer i statsforvaltningen. En felles tilnærming til informasjonssikkerhet vil også stille større krav til å komme frem til felles måter å uttrykke risiko, skadepotensial og sikkerhetsnivå i statsforvaltningen. Risiko- og sårbarhetsanalyser skal ligge til grunn for iverksetting av alle IKT-sikkerhetstiltak i statsforvaltningen.

Det finnes mange regelverk for informasjonssikkerhet, hvor forskjellige etater har et myndighetsansvar. I dag finnes det ikke ett sett med felles minimumskrav for statlig sektor med hensyn til sikkerhetsprosedyrer eller tekniske tiltak i den enkelte virksomhet, eller hos eiere av samfunnskritisk infrastruktur. Dette kan bidra til at virksomhetenes systemer ikke er kompatible, eller til at virksomhetene ikke har tillit til hverandres sikkerhetsnivå, slik at de ikke kan formidle eller dele informasjon på en trygg måte. Fordi det er et så stort antall nettverk som betjener offentlig sektor, er det krevende å etablere sikre, enhetlige løsninger for informasjonsflyt mellom departementene, og mellom departementer og direktorater. I tillegg kan slike fragmenterte løsninger legge til rette for en lite tilfredsstillende sikkerhetstilstand.

Departementer og direktorater har behov for å kommunisere høyt gradert informasjon med hverandre både i daglig virke og i ulike krisesituasjoner. Praktisk erfaring har avdekket utfordringer knyttet til departementenes evne til både å behandle og å kommunisere slik informasjon. Evalueringer etter forskjellige øvelser peker også på mangelen på felles systemer i statsforvaltningen for kommunikasjon av sensitiv, taushetsbelagt og gradert informasjon.

Flere departementer og underlagte etater har etterlyst et felles kravsett for sikkerhetsarbeidet i statlig sektor. Det er gjort forsøk på å samordne regelsettene, men dette har vist seg vanskelig. Det pågår mye arbeid hos regelverksforvaltere og andre myndigheter, for eksempel Direktoratet for forvaltning og IKT (Difi), men dette arbeidet er ikke samordnet i tilstrekkelig grad. Det er også behov for å sikre elektronisk kommunikasjon mellom offentlige virksomheter på den ene siden og innbyggere og næringsliv på den andre siden.

Utvalgte områder som skal vektlegges:

- Statlige myndigheter skal tydeliggjøre hvilke generelle rettslige, organisatoriske og tekniske sikkerhetskrav som skal gjelde for departementene med underlagte virksomheter, sentrale infrastruktureiere og eiere av graderte IKT-systemer i statlig sektor. Kravene må legges til grunn for all informasjonsutveksling i statsforvaltningen. Det bør også inkludere hvilke generelle krav som skal stilles til leverandører av IKT-produkter og -systemer til statlig sektor.

- Offentlige virksomheter skal kunne sende og motta dokumenter elektronisk på en sikker måte, slik at dokumentenes konfidensialitet, integritet og autentisitet kan garanteres.

- Behovet for særskilte systemer og løsninger som brukes for å sikre eksisterende og nye fagsystemer i statsforvaltningen skal reduseres til et minimum.

- Departementene skal ha IKT-løsninger som gjør det mulig å lagre, behandle og kommunisere sensitiv og gradert elektronisk informasjon på tvers av departementene. Løsningene skal kunne virke sammen med forsvarssektorens tilsvarende systemer.

4.4 Sikre samfunnets evne til å oppdage, varsle og håndtere alvorlige IKT-hendelser

Norge skal ha en døgnkontinuerlig, proaktiv operativ beredskap for å kunne forebygge, oppdage og koordinere håndteringen av alvorlige IKT-hendelser. Det skal i denne sammenheng være et tett samarbeid mellom relevante myndigheter og virksomhetene. Det vil legges særlig vekt på samarbeidet med de deler av privat næringsliv som eier eller drifter infrastruktur. Samarbeidet må omfatte både tilsiktede og utilsiktede hendelser, slik som for eksempel teknisk eller menneskelig svikt, ulykker eller naturkatastrofer.

Alvorlige IKT-hendelser omfatter i denne sammenheng målrettede angrep rettet mot kritisk IKT-infrastruktur samt sensitiv, taushetsbelagt, og gradert informasjon. Det store volumet av mindre alvorlige hendelser kan også i sum få alvorlige konsekvenser (for eksempel lekkasje av bedriftssensitiv informasjon og tap av taushetsbelagte eller sensitive personopplysninger). Ikke alle virksomheter har i dag kunnskap om hva de bør gjøre dersom de blir rammet, eller nødvendige rutiner og deteksjonsmekanismer for å forebygge, oppdage, varsle og håndtere uønskede IKT-hendelser. Det er stor variasjon når det gjelder hvilke hendelser som registreres og rapporteres til sentrale myndigheter. Tiltak som gjør IKT-systemer mer robuste og som reduserer konsekvenser av hendelser, uavhengig av årsak, vil i flere tilfeller være sammenfallende. Det vil ha en samfunnsøkonomisk gevinst om slike tiltak koordineres. Virksomheter som er underlagt sikkerhetsloven, er pålagt å rapportere til Nasjonal sikkerhetsmyndighet dersom de oppdager sikkerhetstruende hendelser, men dette er ikke tilstrekkelig til å danne seg et komplett bilde av situasjonen.

Norwegian Computer Emergency Respons Team (NorCERT) i Nasjonal sikkerhetsmyndighet har ved hjelp av Varslingssystem for digital infrastruktur (VDI) og nasjonalt samarbeid, evne til å forebygge, oppdage og analysere data knyttet til alvorlige hendelser på internett. NorCERT-funksjonen samarbeider tett med andre lands og internasjonale organisasjoners tilsvarende tjenester. NorCERT deltar også i et nordisk CERT-samarbeid. Enkelte viktige samfunnssektorer har etablert sektorvise responsmiljøer i nær kontakt med NorCERT og virksomheter i sektoren, eller er i ferd med å gjøre dette (for eksempel Forsvaret, helse- og omsorgssektoren og justissektoren). Disse bidrar til å styrke den samlede håndteringsevne ved sin kompetanse om sektorene, og sikrer at sektormyndighetenes ansvar blir ivaretatt. Stadig flere enkeltvirksomheter bygger dessuten opp interne responsmiljøer eller kjøper tjenester fra private tilbydere. NorCERT-funksjonen er samfinansiert av myndighetene og private aktører.

Når det gjelder hendelser innenfor elektronisk kommunikasjon, som feil i programvare, bortfall og brudd på internettjenester, mobiltelefonitjenester og andre ekomtjenester, er det rutiner for at tilbydere av denne typen nett og tjenester skal varsle Post- og teletilsynet.

Utvalgte områder som skal vektlegges:

- IKT-varslingsmiljøer med en grunnleggende kapasitet til å koordinere og håndtere uønskede IKT-hendelser skal finnes i alle samfunnssektorer (for eksempel som en sektor-CSIRT), og i de viktigste virksomhetene som understøtter samfunnskritiske funksjoner. Disse varslingsmiljøene skal være strukturert slik at man tar hensyn til sektorens bruk av IKT-infrastruktur, hvordan infrastrukturen i sektoren er bygget opp og hvordan denne styres.

- Den nasjonale CERT-funksjonen (NorCERT) skal aktivt innhente og analysere informasjon knyttet til alvorlige IKT-hendelser. NorCERT skal ivareta det nasjonale ansvaret for å koordinere håndteringen av slike hendelser, og gi relevant og rettidig informasjon og veiledning til sektorvise responsmiljøer og slike miljøer i virksomheter som forvalter IKT-infrastruktur av betydning for samfunnskritiske eller andre viktige samfunnsfunksjoner.

- Samarbeidet med private aktører skal videreutvikles og styrkes. Relevant risikoinformasjon skal analyseres og formidles fra den nasjonale CERT-funksjonen på en hensiktsmessig og forsvarlig måte til de som har ansvar for å iverksette tiltak, enten det dreier seg om virksomheter, sektormyndigheter, politiet, andre nasjonale myndigheter eller politisk nivå.

- Beredskapen for å håndtere tilsiktede hendelser (kriminelle handlinger, spionasje, sabotasje og terror) bør koordineres på alle nivåer med den beredskap som er nødvendig for å håndtere tilfeldige hendelser som skyldes svikt, ulykker, vær og naturkatastrofer.

- Rutinene for varsling og håndtering av feil, brudd og bortfall av elektronisk kommunikasjon skal styrkes. Post- og teletilsynet og NorCERT skal etablere rutiner for rask og effektiv informasjonsutveksling om uønskede hendelser.

- Det skal planlegges og gjennomføres øvelser i virksomhetene og i sektorene som skal bedre evnen til å håndtere hendelser. Videre må det øves på tverrsektoriell samhandling og samhandling på tvers av landegrenser.

4.5 Sikre samfunnets evne til å forebygge, avdekke og etterforske datakriminalitet

De som utøver datakriminalitet skal ikke kunne forberede eller gjennomføre kriminelle handlinger uten betydelig risiko for å bli oppdaget og straffeforfulgt. Samfunnets evne til å forebygge, avdekke og etterforske datakriminalitet må prioriteres. Alle aktører skal, på eget initiativ, iverksette kriminalitetsforebyggende tiltak i egen virksomhet, og søke å begrense tap eller skade som følge av datakriminalitet. På myndighetssiden skal dette skje bl.a. gjennom økt spisskompetanse, styrking av spesialistkompetansen og kompetanseheving blant generalistene i politiet. Politiet må prioritere arbeidet gjennom styrket kapasitet slik at etaten får større evne til å forebygge, avdekke og etterforske datakriminalitet. Myndighetene skal fortsette å bygge opp sin kapasitet på området for å avdekke datakriminalitet som direkte eller indirekte kan få innvirkning på rikets sikkerhet eller vitale nasjonale interesser.

Datakriminalitet omfatter kriminalitet rettet mot datasystemer og datanettverk, og kriminalitet hvor sentrale elementer av handlingsforløpet begås ved hjelp av datautstyr eller datanettverk. De to formene er ikke klart adskilt. Hensikten med å begå et datainnbrudd vil eksempelvis ofte være å skaffe seg tilgang til informasjon som senere kan brukes til å begå tradisjonell kriminalitet. De senere år har datakriminalitet utviklet seg fra «gutteromsstreker» til alvorlig organisert kriminalitet. Kriminelle tar også i økende grad i bruk ny teknologi for å begå tradisjonell kriminalitet.

Enkelte kriminelle handlinger kan få følger som gjør det nødvendig at både tilbydere, sektormyndigheter eller virksomhetene selv (eksempelvis støttet av NorCERT eller en sektor-CSIRT) iverksetter krisehåndtering.

Det er behov for informasjonsinnhenting på nettet og sikring av elektroniske spor under en krise. Politiet må samtidig etterforske hva, og eventuelt konstatere hvem, som forårsaket den straffbare handlingen som utløste krisen.

Via internett anskaffer kriminelle verktøy for å gjennomføre ulike former for kriminalitet, eksempelvis programvare som kan ta kontroll over datamaskiner. Trusselvurderinger og erfaringer viser at spesielt innen den organiserte kriminaliteten utnyttes de mest moderne datatekniske hjelpemidler for å skjule aktiviteten for politiet og vanskeliggjøre etterforskning. I alle trendrapporter forventes det en økning i utøvelse av datakriminalitet som følge av den teknologiske utvikling generelt og økning i mobile enheter som mobiltelefoner og mobile datamaskiner spesielt.

Politiet er i stor grad avhengig av publikums tips eller anmeldelser for å avdekke datakriminalitet. En utfordring i den forbindelse er at det for visse typer av datakriminalitet er et stort gap mellom det aktuelle regelverket og folks oppfatninger og holdninger til hva som er rett og galt. Fildelingsproblematikken er et eksempel på dette.

Næringslivets Sikkerhetsråds mørketallsundersøkelse for 2012 viser at det er et større gap enn tidligere mellom trusler og sikkerhetstiltak blant norske virksomheter parallelt med at IKT-avhengigheten øker. Norske virksomheter, særlig ledere, mangler kunnskap om informasjonssikkerhet og har ikke oversikt over trusler og hendelser. I mange tilfeller vil

heller ikke den angrepne virksomhet være klar over at serveren/nettidentiteten er infisert. Virksomhetene erfarer dessuten at politiet, av ressursmessige årsaker, ikke kan prioritere annet enn svært alvorlige saker.

Forebygging, avdekking, etterforskning og rettsforfølgelse av datakriminalitet er utfordrende. Arbeidet er ofte tidkrevende og krever særlig kompetanse og hensiktsmessige virkemidler. I tillegg er det gjerne store utfordringer knyttet til identifisering av gjerningsperson/opphavssted. Det er i dag få miljøer i politiet som har den nødvendige kompetansen for denne typen etterforskning. Det forholdsvis lave antallet rettskraftige dommer innenfor området datakriminalitet synliggjør dette. Faren er at regelverket på dette feltet kan miste sin allmenn- og individualpreventive effekt siden det er små sjanser for å bli dømt i slike saker.

Utvalgte områder som skal vektlegges:

- Alle aktører skal på eget initiativ bidra til å forebygge og begrense tap eller skade som følge av datakriminalitet, ID-tyveri og misbruk av identitet

- Politiet skal ha tilstrekkelig kompetanse og kapasitet til å avdekke, identifisere og håndtere datakriminalitet.

- Politiet skal være tilstede på internett, både med åpen patruljering og ved skjult tilstedeværelse, for å kunne forebygge, avverge og ved behov etterforske og eventuelt føre denne type kriminalitet for retten.

- Det skal finnes klare samarbeidsrutiner og rutiner for kompetansedeling både innad i politiet, og mellom politi, myndighetsorganer og sentrale sikkerhetsmiljøer.

4.6 Kontinuerlig innsats for bevisstgjøring og kompetanseheving

Innbyggere, ansatte og ledere i norske virksomheter skal være sikkerhetsbevisste, og må få tilført økt kompetanse knyttet til informasjonssikkerhet. Alle skal ha tilgang til informasjon om sikkerhetsutfordringer og mottiltak. Alle skal ha forståelse for at tiltak må iverksettes. Virksomhetene må ha nødvendig bestillerkompetanse for innkjøp av nye IKT-verktøy og -tjenester, bruk av ekstern konsulentbistand og utkontraktering av virksomhetens tjenester. Det skal være tilstrekkelig kunnskap om IKT-sikkerhet, sårbarheter og behovet for redundans i forbindelse med anskaffelse og drift av IKT-systemer. Alle barn og unge skal ha en basiskompetanse innen informasjonssikkerhet.

Sikkerhetshendelser inntreffer daglig. I enkelte tilfeller får disse store menneskelige eller samfunnsmessige konsekvenser. Etablerte bevisstgjøringsaktiviteter i regi av for eksempel Norsk senter for informasjonssikring (NorSIS), Næringslivets Sikkerhetsråd, Datatilsynet, Post- og teletilsynet og Medietilsynet har vist at behovet for bevisstgjøring og opplæring er økende. Data kan komme på avveie, misbrukes og manipuleres uten at dette er et bevisst angrep. Det er i tillegg en økning i målrettede angrep, og angripere utnytter i stadig større grad brukeren for å lykkes med angrepet. Dette tilsier at fokus på opplæring, kompetanseheving og bevisstgjøring må økes.

Myndigheter med ansvar for sikkerhet og beredskap er i dag ansvarlige for å innhente og formidle informasjon om trusselsituasjonen på nasjonalt og overordnet nivå. Det er også mange aktører i offentlig og privat sektor som jobber målbevisst for å øke sikkerhetskompetansen i befolkningen. Disse aktørene samarbeider på ulike nivåer, og jobber mot ulike grupper av befolkningen. Gjennom økt koordinering av aktivitetene, vil en kunne styrke arbeidet ytterligere. Målet med koordineringen er at alle skal ha tilgang til samme informasjon om trusler og tiltak for å redusere sannsynligheten for at angrep blir vellykket.

Utvalgte områder som skal vektlegges:

- Myndigheter og næringslivsorganisasjoner bør ha felles eller koordinerte programmer for bevisstgjøring, opplæring og oppbygging av en god kultur for informasjonssikkerhet. Offentlig deltakelse i relevante nettverk skal sikre utveksling av informasjon nasjonalt og internasjonalt.

- Alle eiere og leverandører av komponenter til kritisk IKT-infrastruktur i offentlig og privat sektor bør inviteres til felles arenaer for informasjonsdeling.

- Myndighetene skal måle kompetansenivået i befolkningen og i virksomheter. Effekten av iverksatte tiltak skal måles for å avdekke om tiltakene har effekt, og om innsatsen kan bli bedre.

4.7 Høy kvalitet på nasjonal forskning og utvikling innenfor informasjons- og kommunikasjonssikkerhet

Norske forskningsmiljøer skal være i forkant innenfor flere aspekter ved informasjons- og kommunikasjonssikkerhet, som for eksempel robusthet og pålitelighet, risikostyring, kryptoteknologi, distribuerte systemer og juss. Dette skal blant annet skje i tett samhandling med universiteter og høyskoler, med næringsliv og andre brukermiljøer og Forskningsrådet. Det skal stimuleres til norsk deltakelse på internasjonale arenaer.

Forskning i tilknytning til informasjons- og kommunikasjonssikkerhet skjer på en rekke institusjoner i Norge. IKT-sikkerhet inngår også som et sentralt satsningsområde i Forskningsrådets store program for IKT – VERDIKT (Kjernekompetanse og verdiskaping i IKT) – som har pågått i perioden 2005-2014.

IKT-sikkerhet er også et prioritert område innenfor EUs forskningsprogrammer (blant annet 7. rammeprogram for forskning og teknologisk utvikling og Horizon 2020). EUs forsknings- og innovasjonsbudsjett vil utløse koordinerte satsinger med medlemslandene og de landene som ønsker å delta gjennom egne avtaler, deriblant Norge.

Utvalgte områder som skal vektlegges:

- Det er viktig at forskningen på informasjonssikkerhet holder et høyt internasjonalt nivå, og at den tidlig fanger opp endringer i teknologi, infrastruktur og metoder. Tildeling av forskningsmidler bør baseres på internasjonalt samarbeid, og et tett samarbeid mellom akademia, infrastruktureiere, aktuelle brukermiljøer og myndigheter. IKT-sikkerhet bør også være integrert i andre relevante forskningsprogram. Informasjonssikkerhet bør inngå som et prioritert fagområde i Forskningsrådets portefølje av virkemidler.

- Berørte parter skal legge til rette for at forskningsmiljøene innen grunnforskning og anvendt forskning har god samhandling med ledende IKT-bedrifter og fagmiljøer på tvers av sektorer. Offentlig og privat sektor bør legge til rette for at studenter av informasjonssikkerhet på masternivå eller høyere får anledning til å arbeide med aktuelle sikkerhetsproblemstillinger innen en sektor, eller i en enkelt virksomhet, gjennom å foreslå konkrete anvendelige temaer for master- og doktorgradsoppgaver innen informasjonssikkerhet.

- Myndighetene bør bruke FoU-miljøene aktivt i sin rolle som kunde og bestiller av ulike produkter, utviklingsprosjekter og tjenester. Myndighetene skal legge til rette for informasjonsdeling med forskningsmiljøene.

- Norske forskningsmiljøer for IKT-sikkerhet og berørte virksomheter i offentlig og privat sektor skal oppfordres til å delta aktivt i prosjekter innenfor EUs ulike forskningsprogrammer og andre internasjonale forskningsprogrammer av nasjonal interesse.

5 Ansvar for gjennomføring

Selv om informasjonssikkerhet først og fremst er et virksomhetsansvar, vil en vellykket oppfølging av strategien forutsette effektiv medvirkning og samarbeid mellom aktører i næringsliv, sentrale og lokale myndigheter og den enkelte bruker. Utviklingen innen IKT er global, og et omfattende internasjonalt samarbeid om informasjonssikkerhet er en helt nødvendig forutsetning for å lykkes med informasjonssikkerhetsarbeidet. Samtidig må man også kunne ivareta de rent nasjonale interessene på dette området.

Det enkelte fagdepartement er – i samsvar med ansvarsprinsippet – ansvarlig for at strategiens prioriteringer blir fulgt opp innenfor sin sektor. Oppfølgingen vil skje i henhold til en vedtatt handlingsplan på nasjonalt nivå. Departementene må i denne forbindelse samarbeide tett med underlagte virksomheter og berørte aktører i sektorene slik at planlagte sikkerhetstiltak i nødvendig grad blir koordinert med andre departementer. Hvert fagdepartement skal aktivt involvere berørte parter i privat sektor i utarbeidelsen av tiltak i handlingsplanen. Departementene skal sørge for å kartlegge hvorvidt de iverksatte tiltakene i egen sektor bidrar til at målformuleringene under de strategiske prioriteringene nås.

Justis- og beredskapsdepartementet vil ha et overordnet sansvar for å bidra til oppfølgingen av strategien.

Samtidig som gamle sikkerhetsproblemer løses, dukker det nye opp som følge av innføring av ny teknologi, endringer i bruksmønstre og endringer i trusselbildet. Følgelig vil sikkerhetstiltak som er aktuelle i dag kunne være utdaterte i morgen. Regjeringen har derfor valgt å holde strategien på et overordnet nivå, og fokusere på områder som skal vektlegges framfor konkrete sikkerhetstiltak. Det vil utvikles en egen handlingsplan som i mer detalj framstiller hvordan strategiens prioriteringer skal følges opp. Handlingsplanen utgis separat, og skal revideres ved behov. Fagdepartementene skal i forbindelse med utvikling og gjennomføring av tiltakene i handlingsplanen inkludere berørte aktører i sektoren.

Initiering av konkrete tiltak innenfor de ulike innsatsområdene skal skje i forbindelse med utarbeidelsen av departementenes årlige tildelingsbrev til underliggende virksomheter, hvor mål og prioriteringer for virksomhetene gis. Tiltak som berører næringslivet forutsettes gjennomført i nært samarbeid med næringslivets egne organer. Tiltak som berører forbrukerne bør gjennomføres i samarbeid med forbrukerorganisasjonene. Før innføring av nye tiltak bør det alltid foretas en vurdering av hvordan tiltaket berører personvernet, og om nødvendig må personvernmyndighetene involveres ved planlegging og gjennomføring.

For å kartlegge status i oppfølgingen av strategiens utvalgte satsingsområder, vil Regjeringen følge utviklingen på informasjonssikkerhetsområdet gjennom regelmessig å innhente status fra fagdepartementenes oppfølging av tiltakene i handlingsplanen. Ansvaret for dette er lagt til Justis- og beredskapsdepartementet. Det vil bli nedsatt en egen interdepartemental gruppe som skal jobbe langsiktig og kontinuerlig med oppfølgingen av strategien. Gruppen skal blant annet følge utviklingen når det gjelder sikkerhetsutfordringer og trender, og fortløpende vurdere om dette utløser et behov for å revidere hele eller deler av innholdet i den nasjonale strategien. Gruppen skal også være en pådriver for å oppdatere og videreutvikle handlingsplanen.

6 Økonomiske og administrative konsekvenser

Primæransvaret for sikring av informasjonssystemer og nett ligger hos eier eller operatør, og er ledelsens ansvar. Sikkerhetsarbeidet må ivaretas i daglig oppgaveløsning og finansieres innenfor rammene for finansiering av den ordinære virksomheten. Hvert fagdepartement har et sektoransvar. Tiltak i sektorene skal finansieres innenfor gjeldende budsjettrammer.

Størrelsen på kostnadene til tiltak for å fremme informasjonssikkerhet må stå i forhold til den antatte risikoen på de enkelte forvaltningsområdene. Dersom en velger å ikke iverksette risikoreduserende tiltak, må faren for uheldige konsekvenser og tap vurderes.

Vedlegg A:
Ord og uttrykk

CERT	Engelsk: Computer Emergency Response Team. Ekspert-team som håndterer sikkerhetshendelser. CERT er et registrert varemerke for Carnegie Mellon University. Mange benytter derfor forkortelsen C(S)IRT; Computer (Security) Incident Response Team.
CSIRT	Computer Security Incident Response Team (CSIRT) er en ekspertgruppe for håndtering av IKT-sikkerhetshendelser.
Cybersikkerhet	Beskyttelse av data og systemer som er koblet til internettet.
Ekomnett	Ekomnett er elektroniske kommunikasjonsnett.
IKT-infrastruktur	Elektroniske systemer som behandler data eller kommuniserer med annet utstyr, som en enhet eller organisasjon er avhengig av for å fungere på en effektiv måte
IKT-sikkerhet	Hvordan elektroniske nettverk og systemer som behandler data eller kommuniserer med hverandre, og som virksomhetene er avhengig av for å fungere effektivt, skal beskyttes.
IKT-systemer	Se informasjonssystemer.
Informasjonssikkerhet	Beskyttelse av informasjonens konfidensialitet, integritet og tilgjengelighet.
Informasjonssystemer	System for innsamling, lagring, behandling, overføring og presentasjon av data.
Infrastruktur	Grunnleggende strukturer og systemer* som er nødvendige for en organisasjon, en samling organisasjoner eller et land for å fungere på en effektiv måte. *strukturer og systemer: «tekniske anlegg og utstyr, og administrative og organisatoriske tiltak knyttet til disse».
Integritet	Sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter.
Konfidensialitet	Sikkerhet for at nærmere angitt informasjon ikke avsløres for uvedkommende, og at kun autoriserte personer får tilgang til denne.
Kritisk IKT-infrastruktur	Kritisk IKT-infrastruktur defineres som kritisk infrastruktur for elektronisk kommunikasjon. Se også IKT-infrastruktur.
Kritisk infrastruktur	Samfunnets funksjonsdyktighet er svært avhengig av en rekke fysiske og tekniske infrastrukturer. Ved alvorlig svikt i disse infrastrukturene er samfunnet ikke i stand til å opprettholde de leveranser av varer og tjenester som befolkningen er avhengig av (jf. samfunnskritiske funksjoner). Disse infrastrukturene kan omtales som kritiske for samfunnet.

Nettsky (skytjenester)	Engelsk: Cloud computing. Samlebetegnelse på datatjenester som ytes over internett og som er satt opp for å kunne samvirke med andre datatjenester. Betegnelse for alt fra dataprosessering og datalagring til programvare på servere som står i eksterne serverparker tilknyttet internett.
Samfunnskritiske funksjoner	Funksjoner som dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse f.eks. bank- og finanstjenester, helse- og omsorgstjenester mv. Se også kritisk infrastruktur.
Sensitiv informasjon	Benyttes i strategien som en samlebetegnelse for informasjon det er viktig å beskytte av ulike hensyn jf. personopplysningsloven, offentlighetsloven, forvaltningsloven, sikkerhetsloven mv.
Styringssystem for informasjonssikkerhet	Et system for å styre og rettlede organisasjonen når det gjelder informasjonssikkerhet. Kan omfatte verktøy som: • Informasjonssikkerhetshåndbok • Risiko- og sårbarhetsanalyser • Samsvarsrevisjoner • Beredskapsplaner • E-læring om informasjonssikkerhet for hele organisasjonen
Sårbarhet	Et uttrykk for de problemer et system vil få med å fungere når det utsettes for en uønsket hendelse, og de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet. Sårbarheten til et system er et uttrykk for de svakheter og mangler som finnes i systemet og spesielle omstendigheter som øker sannsynligheten for at trusler vil materialisere seg i en sikkerhetshendelse (eksempler på spesielle omstendigheter kan være størrelse, kompleksitet, at mange aktører er involvert, geografisk spredning, hyppige endringer og utsatt beliggenhet). Et systems sårbarhet reduseres ved å øke systemets robusthet.
Tilgjengelighet	Sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov.
Trusselaktør	Entitet som utgjør en reell eller potensiell trussel mot et identifiserbart mål eller i en avgrenset og identifiserbar sammenheng.

Vedlegg B:
Utvalgte nasjonale kontaktpunkter for informasjonssikkerhet

Nasjonal sikkerhetsmyndighet (NSM)
Det sentrale direktorat for beskyttelse av informasjon og infrastruktur av betydning for samfunnskritiske funksjoner. – Beskytter informasjon, informasjonssystemer og andre objekter mot spionasje, sabotasje og terrorhandlinger gjennom tilsyn iht sikkerhetsloven, utvikling av sikkerhetstiltak, råd og veiledning og varsling og håndtering av alvorlige dataangrep (se NorCERT). Pådriver for styrking av sikkerhetstilstanden.
www.nsm.stat.no

NorCERT - Nasjonalt senter for varsling og koordinering av håndteringen av alvorlige dataangrep og andre IKT-sikkerhetshendelser rettet mot IKT-infrastruktur av betydning for samfunnskritiske funksjoner
www.cert.no

Post- og teletilsynet (PT)
Driver tilsyn med aktører som tilbyr elektroniske kommunikasjonstjenester, elektroniske kommunikasjonsnett og posttjenester, samt utstedere av kvalifiserte sertifikater for esignatur. PT skal bidra til sikre og robuste nett og tjenester.
www.npt.no

Nettvett.no - Nettsted drevet av PT for informasjon, råd og veiledning om sikker bruk av internett. Informasjonen er rettet både mot forbrukere og små og mellomstore bedrifter.
www.nettvett.no

Norsk senter for informasjonssikring (NorSIS)
Et ressurssenter opprettet etter et initiativ fra Fornyings- og administrasjonsdepartementet. Senteret driver rådgiving innen informasjonssikkerhet for alle norske private og offentlige virksomheter. Alle samfunnsgrupper skal kunne dra nytte av tjenestene som tilbys. NorSIS driver også nettstedet s*lettmeg.no,* som gir rådgivning for dem som føler seg krenket på nett.
www.norsis.no
www.slettmeg.no

Direktoratet for samfunnssikkerhet og beredskap (DSB)
Pådriver, veileder og samordner i arbeidet med forebyggende samfunnssikkerhet og kriseberedskap nasjonalt, regionalt og lokalt. Kapasitets- og bistandsleverandør for å støtte overordnet myndighet og alle andre myndigheter ved større kriser og når det meldes om behov.
www.dsb.no
www.kriseinfo.no

Kripos
Den nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet. Hovedmålet for Kripos er bekjempelsen av organisert og annen alvorlig kriminalitet.
www.politiet.no/kripos

Etterretningstjenesten (E-tjenesten)
Ansvar for å kartlegge utenlandske trusselaktører, deres motiver, kapasiteter og metoder, jf. lov om Etterretningstjenesten. Formålet med etterretnings-virksomheten er å bidra til å gi norske myndigheter et solid beslutningsgrunnlag i saker som gjelder utenriks-, sikkerhets- og forsvarspolitikk.

Politiets sikkerhetstjeneste (PST)
Ansvar for nasjonens indre sikkerhet.
Forebygger og etterforsker lovbrudd som kan true nasjonens sikkerhet, gjennom blant annet innsamling av informasjon i forhold til personer og grupper som kan utgjøre en trussel, utarbeidelse av ulike analyser og trusselvurderinger, etterforskning og andre operative mottiltak og rådgivning
www.pst.politiet.no

Datatilsynet (DT)
Nasjonal myndighet innen personvern. Etaten fører tilsyn etter en rekke lover og forskrifter, hvor informasjons-sikkerhet utgjør en viktig del av reguleringen. Det samlede regelverket berører store deler av offentlige og private virksomheter. Datatilsynet har utviklet en rekke veiledere innen informasjonssikkerhetsområdet og gir veiledning om oppfyllelse av regelverkets krav.
www.datatilsynet.no

Utgitt av:
Fornyings-, administrasjons-, og kirkedepartementet

Offentlige institusjoner kan bestille flere eksemplarer fra:
Departementenes servicesenter
Internett: www.publikasjoner.dep.no
E-post: publikasjonsbestilling@dss.dep.no
Telefon: 22 24 20 00

Publikasjonskode: P-0976
Design: Melkeveien Designkontor AS
Foto: ©Fotolia.com
Trykk: Andvord Grafisk
12/2012 – opplag 5000