Informasjonssikkerhet i Norge digitalt

Tittel:	Informasjonssikkerhet i Norge digitalt
Utarbeidet av:	Arbeidsgruppe for informasjonssikkerhet i Norge digitalt
Opplagstall:	1 elektronisk
Versjon:	1.0
Dato:	01.06.2016

Innhold

1. Innledning

Formålet med dette dokumentet er å øke bevisstheten og gi råd til medlemmene av Norge digitalt i spørsmål som gjelder informasjonssikkerhet, og å hjelpe dem å oppfylle kravene som stilles.

Dette er ikke en teknisk veileder for drift av sikre nettverk og geodataservere. Slike tiltak forutsettes ivaretatt generelt for IKT-funksjoner i virksomhetene.

I Generelle vilkår for Norge digitalt-samarbeidet heter det i kapittel 7 Informasjonssikkerhet:

> Partene skal oppfylle alle aktuelle krav til informasjonssikkerhet i gjeldende lover og forskrifter, og skal sikre at data og tjenester som skal unntas offentligheten ikke kommer ut til uvedkommende.
>
> Hver part skal sørge for sikkerhetsmål og et tilstrekkelig sikkerhetsnivå basert på en dokumentert risikovurdering i forhold til konfidensialitet, integritet og tilgjengelighet.
>
> Risikovurderingen består i å identifisere, analysere og evaluere en eller flere risikoer. For å få en samlet oversikt over alle kritiske avhengigheter i en risikovurdering, er det er viktig å kartlegge samvirke, avhengigheter, sårbarheter og trusler i forhold til egne data og tjenester i verdikjeden/nettverket. På bakgrunn av risikovurderingen skal forebyggende tiltak iverksettes.
>
> Partene skal gjennomføre opplæringstiltak for å øke kunnskapen og heve bevissthetsnivået om informasjonssikkerheten.
>
> Geodatakoordinator har overordnet ansvar for veiledning om informasjonssikkerhet, og for at krav til informasjonssikkerhet blir ivaretatt i fellesløsninger.

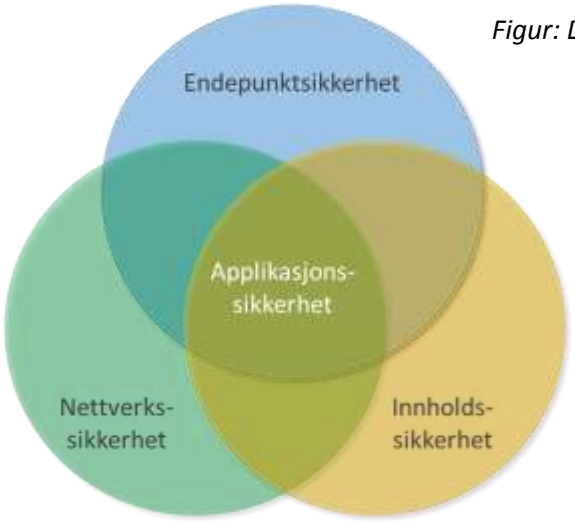
Veiledningen til Generelle vilkår anbefaler Difis veileder innen informasjonssikkerhet, se http://internkontroll.infosikkerhet.difi.no/. Her finnes anbefalinger til hovedaktiviteter innen internkontroll på informasjonssikkerhetsområdet. Dette omfatter ledelsens styring, risikovurderinger, risikohåndtering, kompetanseutvikling, overvåkning og hendelseshåndtering.

"informasjonssikkerhet i Norge digitalt" vil ikke referere innholdet i Difis veileder, men fokusere på forhold som er spesielle for Norge digitalt-samarbeidet.

2. Generelt om informasjonssikkerhet

Informasjonssikkerhet handler om:

- **Konfidensialitet**
  Å sikre konfidensialitet innebærer å hindre uautorisert tilgang til informasjon som ikke kan være åpent tilgjengelig for alle.
- **Integritet**
  Sikkerhet for at informasjonen er fullstendig, nøyaktig og gyldig og et resultat av autoriserte og kontrollerte aktiviteter.
- **Tilgjengelighet**
  Sikkerhet for at informasjonen er tilgjengelig når brukerne trenger den



Figur: De overordnede systemtekniske sikkerhetsområdene

Informasjonssikkerhet kan fra et systemteknisk perspektiv deles i:

- **Endepunktsikkerhet**: Sikkerhet for at maskiner kan behandle informasjon på en tilsiktet måte. Eksempler: fysisk sikring av hardware, systemer for autorisasjon.
- **Nettverkssikkerhet**: Sikkerhet for at informasjonen kommer fram fra avsender til mottaker. Eksempler: hindre tjenestenektangrep, virussikring.
- **Innholdssikkerhet**: Sikkerhet for at informasjonen ikke endres eller kommer på avveie underveis. Eksempler: digitale signaturer, kryptering.
- **Applikasjonssikkerhet**: Sikkerhet for at all programvare som er involvert i å produsere, sende og motta informasjon fungerer som tilsiktet gjennom hele programvarens levetid.

Disse fire sikkerhetsområdene er sterkt overlappende.

Lovverk:
Det overordnete prinsippet i Norge er at informasjon fra offentlige virksomheter skal være åpen for innsyn. En rekke lover og forskrifter gir hjemmel for unntak fra prinsippet om offentlighet. Vedlegg 2 gir oversikt over rettslige føringer som er relevante for informasjonssikkerhet i Norge digitalt-samarbeidet.

Generelle sikkerhetsutfordringer

Nasjonal strategi for informasjonssikkerhet (2012) peker på følgende sikkerhetsutfordringer og trender (forkortet) - mange av disse er svært relevante for dagens GIS-verden:

- Vi er blitt mer sårbare, men også mer effektive gjennom økt utbredelse av internett og bruken av nye datasystemer, styringssystemer for industri, mobiltelefoner, minnepinner, sosiale medier og lesebrett.

- Samfunnet er blitt mer sårbart for selv kortere driftsavbrudd i IKT-systemer og nett.

- Økt brukt av nye tjenesteplattformer, som nettbaserte tjenester og bruk av nettskyen, skaper en uoversiktlighet som kan gjøre det mer krevende for brukerne å vurdere risiko og sårbarhet.

- Drifts- og systemutviklingsoppgaver settes i økende grad ut til leverandører i andre land. Nasjonalt tilsyn og kontroll med hvordan disse håndterer data kan bli svekket.

- Internett og mobile enheter har ført til større risiko for å bli utsatt for datakriminalitet.

- Tendensen til målrettede og profesjonelle datainnbrudd mot kritiske IKT-systemer er økende. Vi må regne med at sofistikerte sabotasje- og påvirkningsangrep vil bli rettet mot samfunnskritiske informasjonsressurser, herunder datasystemer som styrer industriprosesser og kritisk infrastruktur.

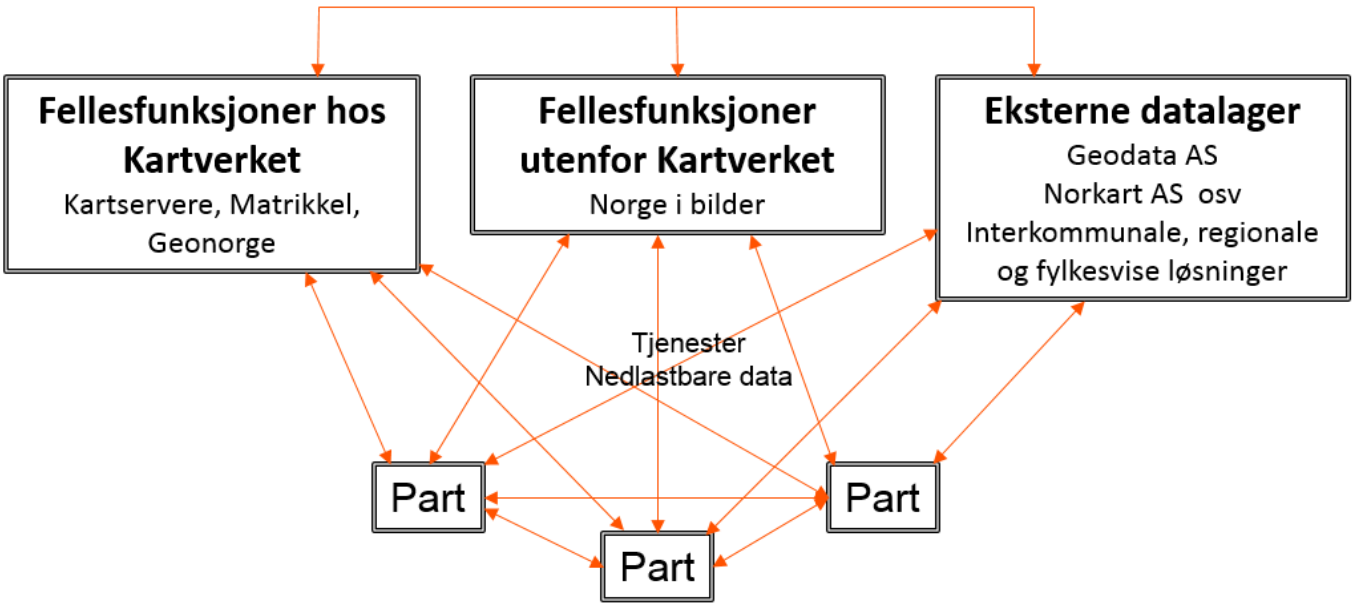
- De fleste virksomheter har en systemportefølje som er langt mer kompleks enn for bare få år siden. Nye produkter og systemer forutsettes å samspille sømløst med andre systemer og på tvers av virksomheter og sektorer. Det er en utfordring å holde oversikt over alle gjensidige avhengigheter og potensielle sårbarheter og å stille klare og presise krav til sikkerhet.

- Internt skadeverk, tyveri eller misbruk av virksomhetens IKT-ressurser fra egne ansatte kan være vanskelig å avdekke.

3. Informasjonssikkerhet i Norge digitalt

Norge digitalt er en utfordrende arena for informasjonssikkerhet.

- Vi er mer enn 600 virksomheter som deler data, og en stor andel av disse er dataleverandører.
- Hver virksomhet har sitt eget sikkerhetsregime, som hos de fleste ikke er spesielt fokusert på håndtering av geodata og derfor vanskelig kan standardiseres ut fra Norge digitalts ønsker.
- Vi har en omfattende og økende bruk av nettjenester fra mange leverandører. De utgjør utvilsomt en usikkerhet når det gjelder oppetid og tilgjengelighet for brukerne.



Figur: Data lagres, vedlikeholdes og videreformidles fra flere hundre virksomheter. Hver av disse må sørge for informasjonssikkerhet i egne systemer og leveranser. Mellom alle partene er det utstrakt bruk av nettjenester.

Hver og en av virksomhetene som lagrer, vedlikeholder og formidler kartdata har ansvar for å sikre

- Konfidensialitet, blant annet gjennom at data ikke tilbys brukere som ikke har rettigheter til dem, og at data med restriksjoner[1] bare er tilgjengelig for brukere som er autorisert for bruk (for eksempel eieropplysninger i matrikkeldata).

[1] Med "data med restriksjoner" menes i denne rapporten data med bruksbegrensninger eller krav til autorisering eller lisens generelt, uten referanse til spesielle datatyper eller spesielt lovverk.

- Integritet, blant annet gjennom at data er beskyttet mot angrep som kan manipulere datainnhold, både fra eksterne og interne (utro tjenere), og at det er gode rutiner for kvalitetssikring og for backup av originaldata.
- Tilgjengelighet, blant annet gjennom gode rutiner er iverksatt mot uønskede hendelser som gjør at data går tapt eller ikke er tilgjengelige for brukerne - alt fra hackerangrep til feilfunksjoner i datasystemer til strømbrudd til fysisk ødeleggelse av infrastruktur, for eksempel ved oversvømmelse.

Ved kjøp av tjenester for dataforvaltning må krav til informasjonssikkerhet være en viktig del av avtalegrunnlaget.

Det er et krav i Generelle vilkår for Norge digitalt-samarbeidet å gjennomføre en risikovurdering i forhold til informasjonssikkerhet i virksomhetens håndtering av geografisk informasjon. Metoden er beskrevet i Difis veiledningsmateriell. Dette er en systematisk måte å vurdere behovet for sikring av egne data ved å identifisere mulige trusler og sårbarheter i systemene og komme fram til nødvendige tiltak. Det kan være mye å lære ved å få bistand av en profesjonell konsulent første gang en slik analyse skal gjennomføres.

Informasjonssikkerhet hos Kartverket

Kartverket har ansvar for sentrale deler av den felles infrastrukturen. Matrikkelen er den aller største og viktigste, andre er Geonorge og felles nedlastningsløsning, og det er tanker om felles dataforvaltningsløsninger. I tillegg er Kartverket den absolutt største dataleverandøren av både tjenester og nedlastbare data. Kartverket har derfor et stort ansvar for å ha fokus på sikkerhet i sin it-arkitektur, sine rutiner og den fysiske sikkerheten ved kritiske elementer i nettverket. Noen sikkerhetselementer hos Kartverket er:

- I Kartverkets systemer er det alltid flerlagsarkitektur, der det aldri eksisterer noen direkte forbindelse mellom klientprogramvare på internett og interne systemer – alle databaser ligger beskyttet innenfor brannmurer.
- For å sikre tilgjengelighet er det etablert to likeverdige datasentre som er speilet, og der hvert senter har nok kapasitet til å håndtere all trafikk alene. Det er også under oppbygging en "katastrofesite", som kan overta for de andre hvis begge skulle falle ut.
- Andre viktige rutiner hos Kartverket for å sikre informasjonssikkerhet er
    - Overvåkning av applikasjoner
    - Logging av feil
    - Gode backuprutiner
    - Gode antivirussystemer
    - Gode rutiner for å ha reserver for applikasjonsansvarlige personer
    - Streng fysisk adgangskontroll ved datasentralene
    - Streng tilgangskontroll til datasystemene.

Hvilke erfaringer har vi med informasjonssikkerhet i Norge digitalt til nå?

Konfidensialitet

En stor del av dataene innenfor Norge digitalt er åpne for alle, også for allmennheten. En del av dataene er forbeholdt de som betaler for dem, som FKB-data til nedlasting. Norge digitalts nedlastingsløsning har hittil i betydelig grad vært tillitsbasert, ved at alle partene har hatt tilgang til å laste ned alle data, og man har stolt på at de bare har lastet ned data som man har rettigheter til. I hvilken grad dette systemet er blitt misbrukt, vet man lite om, men det har ikke framstått som et problem.

På grunn av denne åpenhetspolitikken har data med krav til konfidensialitet i liten grad vært gjort tilgjengelig gjennom den felles infrastrukturen. Den framtidige løsningen for Geonorge planlegges å gi differensiert tilgang til data, basert på bruker/rolle, se kapittel 8.

Integritet

Norge digitalt har hittil vært forskånet for (eller vært dyktige til å sikre mot) sabotasje som har lykkes med å ødelegge datainnhold i større omfang. Det er et betydelig fokus på rutiner for å sikre og dokumentere kvalitet i dataene. Se for øvrig kapittel 5.

Tilgjengelighet

For nettjenester har det i kortere perioder vært utfordringer med tilgjengelighet av data for brukerne i den felles infrastrukturen. Se kapittel 6.

4. Mer om konfidensialitet

Mekanismer som skal sikre at data ikke tilbys brukere som ikke har rettigheter til dem, og at data med restriksjoner bare er tilgjengelig for brukere som er autorisert for bruk, må finnes på flere nivåer i Norge digitalt-samarbeidet:

- **I den felles infrastrukturen / felleskomponentene**
- **Hos den enkelte dataleverandør**
- **Hos den enkelte brukeretat**

Gjennom Geonorge-prosjektet utvikles nå fellesløsninger som i større grad legger til rette for at hvert enkelt datasett bare er tilgjengelig for brukere autorisert for denne datatypen, se kapittel 8. For nedlastbare data har imidlertid fellesløsningene ingen kontroll med hva som skjer med dataene videre – hvem som får tilgang til dem og om det gjøres endringer i innholdet. Dataformidlingen gjennom Norge digitalt vil derfor alltid til en viss grad være tillitsbasert. Vi har tillit til at partene sørger for at data bare formidles til brukere som har rettigheter til dem. Vi har også tillit til at partene sikrer at innholdet ikke blir manipulert av egne ansatte, bevisst eller ubevisst, eller ved eksterne angrep. Men med dagens tekniske løsninger kan vi ikke kontrollere at dette skjer.

Nettjenester kan være passordbelagt. For wms- og wfs-tjenester er brukernavn og passord ikke en del av standarden. Slike tjenester er i utgangspunktet laget for åpne data. Det kan lages autoriseringsrutiner, men da er tjenestene ikke etter OGC-standarden.

Sikkerhetsloven gir hjemmel for beskyttelse av informasjon som ikke må gjøres kjent fordi dette kan true rikets sikkerhet og andre vitale nasjonale interesser. Det er ikke mulig å formidle data som er gradert etter sikkerhetsloven gjennom Norge digitalts infrastruktur. De tekniske kravene som stilles til beskyttelse av dataene, er uforenlige med en nettbasert formidling av informasjon.

Informasjon om lokalisering av skjermingsverdige objekter omfattes av sikkerhetsloven og kan ikke publiseres gjennom Norge digitalt. Det bør også være en bevissthet blant partene om å ikke publisere informasjon som *indirekte* viser hvor slike objekter finnes.

Tekniske anlegg under bakkenivå er ikke synlige, verken i virkeligheten eller i grunnkart og flybilder. Det er tilgangsrestriksjoner på data om mange av disse anleggene, men mange aktører har behov for informasjonen, til planlegging av tiltak i området og i beredskapssituasjoner. Informasjonssikkerhetsspørsmålene er diskutert i Miljøverndepartementets høringsnotat Forslag om innføring av krav etter plan- og bygningsloven om dokumentasjon, forvaltning og utveksling av geodata for ledninger og andre anlegg i grunnen.

Et enormt tilfang av ulike data fra ulike kilder kan kombineres gjennom GIS-systemer. I noen tilfeller kan sammenstillinger av data gi større konsekvenser sikkerhetsmessig enn enkeltdatasettene som blir kombinert. For eksempel kan enkelte sammenstillinger av ledningsdata vise spesielt kritiske punkt i infrastrukturen. Eller ulike datakilder kan til sammen avsløre så mye om et teknisk anlegg at det kan brukes til å skade anlegget. Norge digitalt har ikke et "publiseringspoliti". **Eiere av slike objekter må selv gjøre en vurdering av om det publiseres data i Norge digitalt som kan kompromittere objektene, og i så fall ta dette opp med dataeier.**

I forbindelse med prosjekter stilles iblant data til rådighet for deltakere som normalt ikke vil ha tilgang til denne datatypen. Disse må behandles ryddig og aldri brukes i andre sammenhenger uten tillatelse.

Hver dataleverandør må gjøre en vurdering av hvilke data som skal leveres gjennom Norge digitalts infrastruktur, ut fra de tekniske løsningene i infrastrukturen, behovet for skjerming, og hvor viktig det er at dataene blir brukt i samfunnet. Et forslag til analyse er gitt i vedlegg 1. Husk at behovet for konfidensialitet kan endre seg over tid.

Enkelte Norge digitalt-parter leverer nedlastbare datasett bare til utvalgte brukere og med særlige krav til lagring og formidling. Det vil være opp til dataleverandøren å sette slike krav. De må være godt dokumentert i metadataene, for eksempel:

- Dataene lagres på en slik måte at bare autoriserte brukere har tilgang.
- Leverandørens regler for distribusjon og innsyn (som beskrevet i metadataene) må være kjent for alle som har tilgang.
- Videreformidling av data, for eksempel fra fylkesmenn til kommuner, skal skje via passordbeskyttet og kryptert server.

5. Mer om dataintegritet

Alle dataeiere og –forvaltere har ansvar for å sikre dataene mot uautorisert endring, fra utro tjenere internt og fra eksterne angrep, eller ved feil som oppstår ved et uhell.

Muligheter til å oppdage integritetsbrudd kan være ulike kvalitetskontroller, logging av hvilke brukere som har vært inne på systemene og når, sammenligning av dataversjoner osv.

Både wms- og wfs-tjenester kan sendes kryptert, slik at innholdet ikke kan vises eller endres underveis mellom avsender og mottaker. Dette kan gjøres ved bruk av https, eventuelt i kombinasjon med sjekksum-algoritmer (for eksempel md5 checksum) som sjekker om innholdet er endret. Mange kartservere kan kryptere tjenestene, men på klientsiden er det mange som ikke kan støtte krypterte tjenester. Dette blir derfor lite brukt foreløpig.

Feil kan oppstå i data på mange måter som ikke har noe med tilsiktede angrep å gjøre. Norge digitalt legger stor vekt på kvalitetssikring av data. Det legges også vekt på gode metadata. Datakvaliteten må beskrives godt i metadataene, både fordi ikke alle brukere forstår kvalitetskoding og fordi ikke alle kvalitetsaspekter kan uttrykkes med koding. Blant annet er det viktig at brukeren kjenner til datasettets *fullstendighet*, for eksempel beskrevet som kartlagt areal eller som kartlagte objekter som andel av alle objekter.

Nedlastbare data er viktige for mange brukere, men krever at brukeren vet hva han eller hun gjør, spesielt der dataene spres til mange gjennom innsynsløsninger:

- Nedlastede kopier blir ikke oppdatert i takt med originalen.
- Lokal bearbeiding av nedlastede data kan introdusere feil. Feil i utvalg for symbolisering kan føre til at dataene framstår feil.
- I noen tilfeller kombineres egne og andres data i nye datasett. Tenk over om det er fornuftig å publisere dataene slik.

6. Mer om tilgjengelighet

Dataformidlingen i Norge digitalt er i stor grad er basert på nettjenester, og oppetid på disse tjenestene er kanskje den største informasjonssikkerhetsutfordringen i samarbeidet. Kartverket har gjort store forbedringer i sine systemer de siste årene, og brukerne opplever mye større stabilitet i Kartverkets tjenesteleveranser.

Det er mange andre parter som leverer nettjenester, med varierende stabilitet. Generelle vilkår i Norge digitalt ber partene angi tjenestenes tilgjengelighet, der for eksempel nivå B angir at tjenestene har en garantert oppetid

bare innenfor vanlig arbeidstid på virkedager og med betydelige unntak. En bruker kan altså ikke være sikker på at tjenester er tilgjengelige til enhver tid.

En spørreundersøkelse utført av Arbeidsgruppe Informasjonssikkerhet viser at mange parter bruker tjenester som er viktige i saksbehandling, beredskap og ulike utredninger. Når tjenestene er nede, vil saksbehandlingen bli forsinket, eller resultatet blir dårligere. Hvis beredskapen er avhengig av tjenester, kan konsekvensene bli store. Se også kapittel 7 om sårbarhet i egen organisasjon.

Tiltak hos tjenesteleverandørene:

- **Analysere: Hvem er brukerne? Hvor viktige er tjenestene for dem?**
- **Arbeide for høyest mulig oppetid, spesielt for viktige tjenester**
- **Varsle planlagt nedetid og endringer i tjenestene gjennom Norge digitalts kanaler**

Overvåking og varsling

Bedre overvåking av tjenester og varsling av nedetid og endringer i tjenester vil gi brukerorganisasjonene bedre mulighet for tilpasning, slik at brukerne får økt sikkerhet for at data er tilgjengelige.

Overvåking

Geonorges tjenestestatusregister gir blant annet informasjon om gjennomsnittlig responstid og oppetid for alle tjenester som er registrert i Geonorge: http://159.162.102.155/p/wms/results?order=cors.

Varsling og alarmering

Det er behov for varsling av planlagte hendelser, som at lenke til tjenester endres eller planlagt nedetid, og alarmering ved uforutsette hendelser, som plutselig feil på server.

Geonorge har et register for henholdsvis tjenestevarsler og driftsmeldinger:
https://www.geonorge.no/informasjon/aktuelt/Tjenestevarsler/ og
https://www.geonorge.no/informasjon/aktuelt/Driftsmeldinger-og-teknisk-support/

Tjenesteeiere kan selv publisere sine varsler gjennom et webgrensesnitt. Det er mulig å abonnere på endringsvarslene som RSS Feed. Man kan abonnere på varsler fra alle eller bare fra utvalgte parter. Outlook kan settes opp slik at varslene kommer inn som mail.

Det planlegges et system med alarmer for uforutsette driftsavbrudd.

7. Sårbarhet i egen organisasjon

Alle organisasjoner ønsker å arbeide mest mulig kontinuerlig, uten uønskede avbrudd. Bruk av GIS-systemer er viktig i mange organisasjoner. I noen funksjoner er GIS kritisk – man får ikke gjort jobben sin uten.

Alle organisasjoner bør gjøre en analyse av sin egen sårbarhet:

- **Hvilke GIS-data er viktigst for brukerne?**
- **Hvilke konsekvenser får det hvis GIS-systemer og -data ikke er tilgjengelig for brukerne?**
- **Hvilke tiltak kan iverksettes for å redusere sannsynligheten for at disse blir utilgjengelige?**

Noen funksjoner regnes som kritiske for samfunnet (Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner, DSB 2012). De kritiske samfunnsfunksjonene er de som sørger for befolkningens grunnleggende behov: mat, vann, varme, trygghet og lignende, se tekstboks. Legg merke til at Matrikkelen regnes som en kritisk samfunnsfunksjon, punkt 9.

KRITISKE SAMFUNNSFUNKSJONER

1. Ivareta nødvendig matforsyning
2. Ivareta nødvendig drikkevannsforsyning
3. Ivareta nasjonal sikkerhet
4. Ivareta styring og kriseledelse
5. Opprettholde demokratisk rettsstat
6. Opprettholde trygghet for liv og helse
7. Opprettholde lov og orden
8. Opprettholde finansiell stabilitet
9. Opprettholde grunnleggende sikkerhet for lagret informasjon
10. Sikre kulturelle verdier av nasjonal betydning
11. Beskytte natur og miljø

Hvis de kritiske samfunnsfunksjonene er avhengige av kartsystemer, må disse være svære svært robuste. I Forsvaret og på alarmsentralene til nødetatene benyttes ikke nettjenester for de viktigste dataene, som grunnkart og matrikkeldata. Alle har strømaggregat. Organisasjoner innenfor energiforsyningen har krav om sikkerhetskopier av informasjon som er av betydning for drift, sikkerhet og gjenoppretting. Den nødvendige informasjonen skal også foreligge som papirutskrifter.

Alle IKT-tjenester er avhengig av strømforsyning og mange er avhengig av internett. Forsyningssikkerheten for strøm er 99,99% og har blitt stadig bedre, men det er ikke mulig å garantere mot langvarige strømbrudd.

Faktorer som øker en organisasjons sårbarhet på geodataområdet:
- Utilstrekkelige tekniske løsninger
- Utstrakt bruk av nettjenester
- Utstrakt bruk av mobile plattformer som er avhengig av nettilkobling

Bruken av nettjenester øker stadig. Brukeretatene kan ikke påvirke oppetiden for disse tjenestene – det er leverandørens ansvar. I tillegg er tilgjengeligheten avhengig av at internett fungerer. Ved ulike former for kriser vet vi at det er fare for å miste nettilkoblingen.

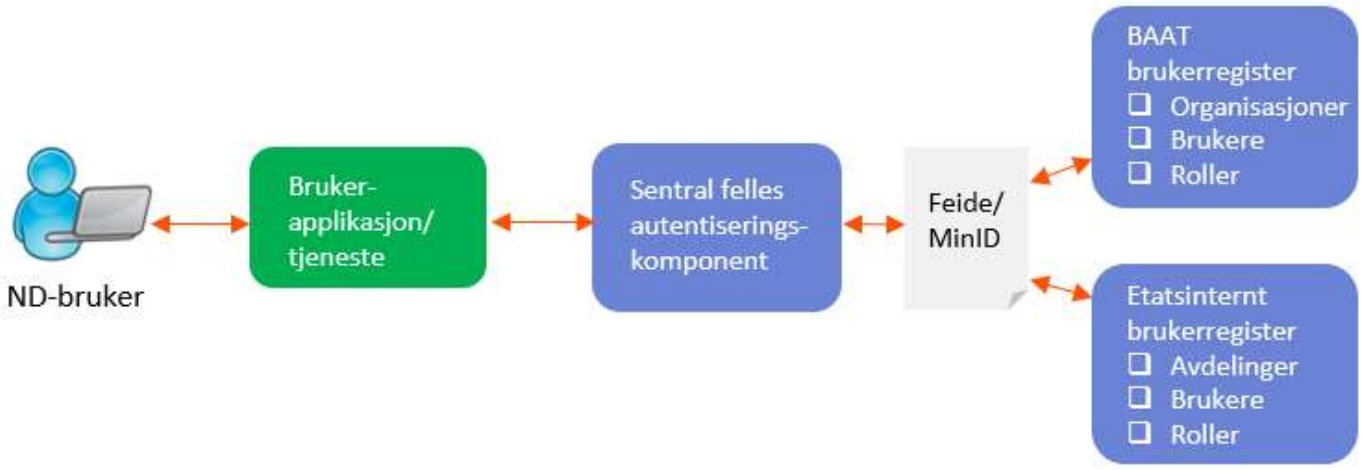
Tiltak hos brukerne som reduserer sårbarheten:

- **Lagring av lokale kopier av viktige data som normalt benyttes som nettjenester. Nødvendige forberedelser må være gjort for å kunne ta disse dataene i bruk raskt.**
- **Tilgang til lokalt lagret programvare for viktige funksjoner, hvis organisasjonen ellers bruker nettbasert programvare.**
- **For svært viktige funksjoner:**
    - **Strømaggregat**
    - **Lagring av papirkart**

8. Tilgangskontroll og autentisering i morgendagens infrastruktur

For å sikre konfidensialitet i Norge digitalts løsninger, altså å hindre uautorisert tilgang til informasjon som ikke kan være åpent tilgjengelig for alle, arbeides det nå med utvikling av en ny løsning for tilgangskontroll og autentisering i Norge digitalt. Testing av løsningen vil starte i 2016.

En sentral autentiseringsløsning vil kunne hente informasjon om brukerne både fra det sentrale BAAT brukerregisteret, som Kartverket vedlikeholder, og fra lokale brukerregistre hos den enkelte organisasjon. Autentisering vil kunne gjøres både på virksomhets- eller avdelingsnivå (alle i virksomheten/avdelingen har samme tilgang) og på brukernivå.



I brukerregistrene vil det bli definert roller og beskrevet hvilke data virksomhet/bruker med denne rollen får tilgang til. Dette vil være basert på at datasettene får angitt beskyttelsesnivå. Det blir et begrenset antall beskyttelsesnivåer, kanskje bare:

- Vanlig BAAT-beskyttelse
- Økonomisk beskyttelse (eks FKB-data)
- Streng beskyttelse. Dataene leveres ikke gjennom Norge digitalts kanaler

Det er ikke bestemt hvordan brukerne skal identifisere seg mot den sentrale autentiseringsløsningen. Det kan være aktuelt å bruke MinID og Feide (Kunnskapsdepartementets løsning for sikker identifisering i utdanningssektoren). Men det må ikke bli så rigid at man må ha bankkodebrikke for å laste ned et åpent datasett.

Det vil bli utviklet og beskrevet et standard grensesnitt mot den sentrale autentiseringsløsningen som brukerapplikasjonene må benytte, hvis det skal være tilgangsbegrensninger i applikasjonen.

Det vil ta tid før den gamle BAAT-løsningen avvikles. Antagelig vil nye applikasjoner bruke det nye autentiserings-systemet når dette er ferdig, mens gamle applikasjoner vil kunne bruke det gamle i lang tid framover.

Vedlegg 1: Analyse: Bør data publiseres gjennom Norge digitalt

Dette kapitlet gir forslag til en analyse som en dataeier kan foreta for å vurdere om et datasett bør publiseres gjennom Norge digitalt, gitt det nivået av informasjonssikkerhet som vi har i Norge digitalt.

0. Forutsetninger

a) Analysen gjelder geografiske data som formidles gjennom Norge digitalt
b) Analysen foretas av **dataleverandøren.** Det forutsettes at leverandøren eier dataene eller har rettigheter til å videreformidle dem.
c) Analysen gjelder bruk av dataene hos andre virksomheter innenfor Norge digitalt, her kalt **brukerne.**
d) I noen sammenhenger er det naturlig å skille på **nedlastbare data** og **tjenester**
e) Norge digitalts nedlastingsløsning vil i framtida gi mulighet for å definere hvilke brukere som skal ha tilgang til et datasett.

1. Tilgjengelighet

a) Gjelder **tjenester:**
   i. Hvor viktig er tilgjengelighet/oppetid for datasettets brukere i Norge digitalt?
   ii. Bør det / kan det settes inn tiltak for å øke oppetiden?
b) For **nedlastbare data** kan brukeren selv gjøre tiltak for å sikre tilgjengelighet, ved å sørge for å alltid å ha en lokal nedlastet kopi. For data som er viktige for brukeren, må dette kunne forutsettes. Høy oppetid på nedlastingsløsningen er likevel alltid ønskelig.

2. Integritet

a) Gjelder **nedlastbare data:**
   i. Dataleverandør har ingen kontroll på data som er lastet ned i forhold til uautorisert endring av innholdet. Dataene kan bli endret, og de kan bli symbolisert feil, slik at det gis feil inntrykk av innholdet. Er dataleverandør villig til å ta denne sjansen og stole på brukerne? Alternativet er at dataene bare leveres som tjenester.
b) Gjelder **alle data:**
   i. Er datakvaliteten godt dokumentert i metadataene i Geonorge, slik at brukerne kan ha realistiske forventninger til hvordan dataene kan brukes?
   ii. Kan det være feil i dataene som kan føre til så alvorlige konsekvenser hos brukerne at dataene ikke bør publiseres?
   iii. Er datakvaliteten god nok, og inneholder nedlastningsløsningen ferske nok data, så dataene ikke reflekterer negativt på dataleverandøren som virksomhet?

3. Konfidensialitet

a) Faller informasjonen inn under lovverk, forskrifter eller avtaler som definerer dem som helt eller delvis unntatt offentlighet? Se vedlegg 2 Sentrale lover og forskrifter og spesielt sikkerhetsloven og beskyttelsesinstruksen.
b) Faller datasettet inn under personopplysningsloven?
   Jfr. Veiledningsdokument for håndtering av personopplysninger i Norge digitalt
c) Er det andre grunner til at datasettet må vurderes unntatt offentlighet helt eller delvis? For eksempel
   i. Nærings-/konkurransehensyn
   ii. Opplysningene kan lette gjennomføring av straffbare handlinger (jfr. offentleglova §24)
   iii. Opplysningene kan utsette enkeltpersoner for fare (jfr. offentleglova §24)
   iv. Opplysningene kan lette handlinger som kan skade utsatte deler av miljøet (jfr. offentleglova §24)

v. Opplysningene kan skade Norges forsvarsinteresser eller utenrikspolitiske interesser (jfr. offentleglova §20 og 21)
vi. Skjerming av kritisk infrastruktur (jfr. blant annet beredskapsforskriften til energiloven kapittel 6)
vii. Opplysningene er innsamlet under løfte om konfidensialitet.
viii. Publisering kan ødelegge for videreføring av dataserien (eks analyseflater for miljøovervåking)
ix. Statistikklovens begrensninger på publisering
x. Kan sammenstilling av dette datasettet med andre datasett tilgjengeliggjort gjennom Norge digitalt gjøre dataene mer på i forhold til punktene over?

4. Analyse

Hvis gjennomgang av spørsmålene om konfidensialitet gir som resultat at datasettet må vurderes unntatt offentlighet helt eller delvis, vurderes følgende:

1. Er dataene tilgjengelige fra andre kilder som er allment tilgjengelige?

2. Er det aktuelt å fjerne noen objekter eller noen egenskaper før publisering for å gjøre dataene mindre sensitive? Eller generalisere dataene?

3. Vil informasjonssikkerheten kunne bli tilfredsstillende hvis datasettet publiseres bare som tjenester? Eller bare som nedlastbare data?

4. Er det aktuelt å gjøre nedlastbare data tilgjengelig gjennom Norge digitalt bare til en begrenset brukergruppe? Vil dette løse problemene i forhold til konfidensialitet?

5. Negative konsekvenser av å publisere datasettet veies mot negative konsekvenser ved å ikke publisere. Det kan være store positive gevinster ved at informasjonen i dataene blir kjent. Dette vurderes også for et forenklet datasett, jfr. punkt 1. Sannsynligheten for negative konsekvenser må også vurderes i begge tilfeller.

Konklusjonen kan da bli:

- Datasettet publiseres åpent
- Datasettet publiseres bare som tjenester eller bare som nedlastbare data
- Datasettet publiseres etter fjerning av noen objekter eller egenskaper eller etter generalisering
- Datasettet gjøres tilgjengelig for en begrenset brukergruppe (hvem skal ha tilgang?)
- Datasettet publiseres ikke gjennom Norge digitalt

Vedlegg 2: Sentrale lover og forskrifter

Regelverk som omhandler krav om offentlighet og unntak fra dette kravet.

Oversikten er ikke uttømmende

- **Grunnloven § 100 (lov av 17. mai 1814)**
  https://lovdata.no/dokument/NL/lov/1814-05-17/KAPITTEL_5#§100
  - Ytringsfriheten omfatter også informasjonsfriheten, friheten til å gjøre seg kjent med opplysninger, ideer og budskap som andre frivillig gir fra seg.
  - Rekkevidden av grunnlovsvernet må avveies mot andre interesser, for eksempel personvernet og privatlivets fred.
  - I forbindelse med lovendringen i Grunnloven § 100 i 2004, ble offentlighetsprinsippet grunnlovsfestet i femte ledd når det gjelder borgernes informasjonskrav overfor forvaltning og domstoler.
  - Sjette ledd inneholder infrastrukturkravet, som betyr at staten har plikt til å legge til rette for kanaler og institusjoner og for en åpen og opplyst samtale. Myndighetene vil være forpliktet til å ta dette kravet i betraktning når lovgivning og andre tiltak av betydning for ytringsfriheten vurderes.

- **Offentlighetsloven (lov om rett til innsyn i dokument i offentleg verksemd av 19. mai 2006 nr. 16)**
  https://lovdata.no/dokument/NL/lov/2006-05-19-16
  - Formålet med loven fremkommer i § 1: «Formålet med lova er å leggje til rette for at offentleg verksemd er open og gjennomsiktig, for slik å styrkje informasjons- og ytringsfridommen, den demokratiske deltakinga, rettstryggleiken for den enkelte, tilliten til det offentlege og kontrollen frå ålmenta. Lova skal òg leggje til rette for vidarebruk av offentleg informasjon.
  - Offentlighetsloven fastslår offentlighetsprinsippet i forvaltningen som en rett for allmennheten til å få gjøre seg kjent med innholdet av formelle saksdokumenter som foreligger. Utgangspunktet er at alle har adgang til å gjøre seg kjent med og publisere opplysninger som kommer frem ved statlige og kommunale myndigheters saksbehandling. Det er ikke noe vilkår for bruk av innsynsrett etter offentlighetsloven at den som ber om innsyn har noen spesiell tilknytning til eller interesse i saken.
  - Offl. § 3 angir at retten til å kreve innsyn «hos vedkomande organ» omfatter «saksdokument, journaler og liknande register til organet».
  - Unntak fra innsyn kan fremkomme av loven selv, §§ 14 – 26, eller at opplysningene er underlagt taushetsplikt etter annen lovgivning, jf. § 13.
  - Når det gis tilgang til dokumenter etter offentlighetsloven, vil den som har fått slik tilgang som alminnelig utgangspunkt kunne bruke de opplysningene som fremkommer her «til eitkvart formål» så langt ikke annen lovgivning eller tredjepersoners rettigheter er til hinder for det (offl. § 7 første ledd).

- **Offentlighetsforskriften (forskrift til offentleglova av 17. oktober 2008 nr. 1119)**
  https://lovdata.no/dokument/SF/forskrift/2008-10-17-1119
  - Forskriften har blant annet i § 7 bestemmelser om tilgjengeliggjøring av dokument på Internett. Det er listet opp hvilke opplysninger som ikke kan gjøres tilgjengelig på Internett, blant annet fødselsnummer, personnummer og nummer med tilsvarende funksjon.

- **Forvaltningsloven (lov om behandlingsmåten i forvaltningssaker av 10. februar 1967)**
  https://lovdata.no/dokument/NL/lov/1967-02-10
  - Forvaltningsloven gir regler blant annet om inhabilitet i forvaltningen, om varsel og om innsynsrett samt om rett for partene til å uttale seg ved behandlingen av forvaltningssaker.

- Forvaltningsloven har blant annet regler om partsinnsyn. Etter fvl. § 18 har den som er part i en sak om et enkeltvedtak, rett til å gjøre seg kjent med sakens dokumenter. I fvl. § 2 første ledd bokstav e er part definert som en person som en avgjørelse rettet seg mot eller som saken ellers direkte gjelder.
- Loven har i §§ 13 – 13f bestemmelser om taushetsplikt.

❖ **Forvaltningslovforskriften (forskrift til forvaltningsloven av 15. desember 2006 nr. 1456)**
https://lovdata.no/dokument/SF/forskrift/2006-12-15-1456
- Forskriften utfyller, presiserer og gjør unntak fra forvaltningsloven, når ikke annet følger av ellers gjeldende bestemmelser.

❖ **Personopplysningsloven (lov om behandling av personopplysninger av 14. april 2000 nr. 31)**
https://lovdata.no/dokument/NL/lov/2000-04-14-31
- Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger, jf. § 1 første ledd.
- Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger, jf. § 1 annet ledd.
- Loven har meget vid anvendelse, se definisjoner i § 2 og saklig virkeområde i § 3.

❖ **Personopplysningsforskriften (Forskrift om behandling av personopplysninger av 15. desember 2000 nr. 1265)**
https://lovdata.no/dokument/SF/forskrift/2000-12-15-1265
- Forskriften inneholder en rekke bestemmelser som på viktige punkter supplerer eller modifiserer personopplysninglovens bestemmelser.

❖ **Matrikkelloven kapittel 6 og Forskrift om opplysninger fra grunnbok og matrikkel (Forskrift om utlevering, viderebruk og annen behandling av opplysninger fra grunnboken og matrikkelen forskrift om opplysninger fra grunnbok og matrikkel av 18. desember 2013 nr. 1599)**
https://lovdata.no/forskrift/2013-12-18-1599
- Denne forskriften gjelder tinglysings- og matrikkelmyndighetenes utlevering av opplysninger fra grunnboken og matrikkelen. Forskriften gjelder også virksomheters utlevering, viderebruk og annen behandling av opplysninger fra grunnboken og matrikkelen.

- **Beredskapsforskriften (Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen av 7. desember 2012 nr. 1157)**
https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157
Veileder til forskriften: http://publikasjoner.nve.no/veileder/2013/veileder2013_01.pdf
  - Kapittel 6 i forskriften omhandler informasjonssikkerhet.
  - Forskriften beskriver hva som er kraftsensitiv informasjon og derfor underlagt taushetsplikt etter §9-3 i energiloven. Enhver plikter å hindre at andre enn rettmessige brukere får adgang eller kjennskap til sensitiv informasjon om kraftforsyningen. Det betyr at alle som kommer i kontakt med taushetsbelagt informasjon må følge denne taushetsplikten.

❖ **Miljøinformasjonsloven (Lov om rett til miljøinformasjon og deltakelse i offentlige beslutningsprosesser av betydning for miljøet av 9. mai 2003 nr. 31)**
https://lovdata.no/dokument/NL/lov/2003-05-09-31
- Loven pålegger offentlige organer og offentlige og private virksomheter kunnskaps- og informasjonsplikt, og gir enhver rett til å få miljøinformasjon hos disse organer og virksomheter på forespørsel, og til å delta i beslutningsprosesser av betydning for miljøet.

- Unntak i § 11 for informasjon fra offentlig organ: Grunnlaget for unntak fra rett til miljøinformasjon fra offentlig organ er de samme som i offentleglova, jf. offentleglova kap. 3.
- Unntak i § 17 for miljøinformasjon fra virksomhet. Unntakene er delvis de samme som unntakene i § 11 første ledd for offentlig organ.

❖ **Sikkerhetsloven (lov om forebyggende sikkerhetstjeneste av 20. mars 1998 nr. 10)**
https://lovdata.no/dokument/NL/lov/1998-03-20-10

- Loven har blant annet i § 13 bestemmelse som legger til Nasjonal sikkerhetsmyndighet både å typegodkjenne utstyr og programvare som skal nyttes i informasjonssystemer, og å godkjenne den enkelte installasjon for håndtering av gradert informasjon.
- Når informasjon må beskyttes av sikkerhetsmessige grunner, skal en av følgende sikkerhetsgrader brukes: Strengt hemmelig, hemmelig, konfidensielt eller begrenset. Dette følger av sikkerhetsloven § 11. Informasjonen skal merkes med aktuell sikkerhetsgrad.
  Sikkerhetsgradert informasjon er undergitt lovbestemt taushetsplikt, jf. § 12 første ledd. Slik informasjon er dermed unntatt fra offentlighet.
- Før skjermingsverdig informasjon behandles, lagres eller transporteres i et informasjonssystem, skal Nasjonal sikkerhetsmyndighet, eller den Nasjonal sikkerhetsmyndighet bemyndiger, godkjenne systemet for angjeldende sikkerhetsgrad. Dette følger av § 13 første ledd.

❖ **Forskrift om informasjonssikkerhet (av 1. juli 2001 nr. 744)**
https://lovdata.no/forskrift/2001-07-01-744

- Forskriften har samme formål og virkeområde som sikkerhetsloven. Den inneholder en del utfyllende bestemmelser om sikkerhetsgradert informasjon.

❖ **Beskyttelsesinstruksen (instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter av 17. mars 1972 nr. 3352)**
https://lovdata.no/dokument/INS/forskrift/1972-03-17-3352

- Betingelser for gradering av et dokument er at dokumentet kan unntas fra offentlighet i medhold av offentlighetsloven (jf. § 3), og at det vil kunne skade offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende (jf. § 4).
- Beskyttelsesinstruksen gjelder kun for statlige forvaltningsorganer.

❖ **Arkivloven (lov om arkiv av 4. desember 1992 nr. 126)**
https://lovdata.no/dokument/NL/lov/1992-12-04-126

- Formålet med arkivloven er å verne arkiv som har stor kulturell eller forskningsmessig verdi eller som inneholder rettslig eller viktig forvaltningsmessig dokumentasjon, slik at disse kan bli tatt vare på og gjort tilgjengelige for ettertida.

Vedlegg 3: Andre dokumenter

- **Regjeringen: Nasjonal strategi for informasjonssikkerhet**
  https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-informasjonssikker/id710469/
  - Strategien angir retning og prioriteringer for myndighetenes informasjonssikkerhetsarbeid.
- **Regjeringen: Handlingsplan for informasjonssikkerhet**
  https://www.regjeringen.no/no/dokumenter/handlingsplan-for-informasjonssikkerhet-i-statsforvaltningen/id2440093/
  - Handlingsplanen er en del av Nasjonal strategi for informasjonssikkerhet. Den er avgrenset til arbeidet med informasjonssikkerhet i statsforvaltningen. Tiltaksområdene som skal iverksettes skal primært bidra til en helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen.
- **Digitaliseringsrundskrivet**
  https://www.regjeringen.no/no/dokumenter/digitaliseringsrundskrivet/id2462793/
  - Digitaliseringsrundskrivet er en sammenstilling av pålegg og anbefalinger vedrørende digitalisering i offentlig sektor, og gir et helhetlig bilde av hvilke føringer som gjelder.
- **Regjeringen: Retningslinjer ved tilgjengeliggjøring av offentlige data av 30. november 2012**
  https://www.regjeringen.no/no/dokumenter/retningslinjer-ved-tilgjengeliggjoring-a/id708912/
  - For å sikre at data blir tilgjengeliggjort på en hensiktsmessig måte bør offentlige virksomheter tilgjengeliggjøre data i tråd med disse retningslinjene.
- **Difi: Overordnede IT-arkitekturprinsipper for offentlig sektor av 17. september 2012**
  https://www.difi.no/sites/difino/files/arkitekturprinsipper-2.1.pdf
  - Krav til informasjonssikkerhet
- **DIFI: Åpne data - Del og skap verdier – Veileder i tilgjengeliggjøring av offentlige data**
  http://data.norge.no/sites/data/files/Veileder-i-tilgjengeliggjoring-av-offentlige-data-V2.pdf
  - Krav til tilgjengelighet og unntak for taushetsbelagte opplysninger
- **DIFI: Veileder – Internkontroll i praksis – Informasjonssikkerhet**
  http://internkontroll.infosikkerhet.difi.no/
- **DFØ: Reglement og bestemmelser for økonomistyring i staten**
  https://www.regjeringen.no/globalassets/upload/fin/vedlegg/okstyring/reglement_for_okonomistyring_i_staten.pdf
  - Dekker flere sider ved sikkerhet; bl.a. krav til datasikkerhet og krav til internkontroll som skal forhindre og avdekke misligheter og kriminalitet samt sikre konfidensialitet, integritet og tilgjengelighet for vesentlig informasjon. Viktig kapittel: 4.3.6 Sikkerhet i økonomisystemet
- **Stortingsmelding 29 (2012): Samfunnssikkerhet**
  https://www.regjeringen.no/no/dokumenter/meld-st-29-20112012/id685578/
  - I denne meldingen til Stortinget redegjør regjeringen for ulike tiltak som bidrar til å styrke arbeidet med samfunnssikkerhet og beredskap. Angrepene den 22. juli 2011 satte samfunnets beredskap på prøve og er gjenstand for en bred gjennomgang i meldingen.
- **NOU 2015:13: Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden**
  https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou20152015 0013000dddpdfs.pdf
  - Utredning fra Lysneutvalget, satt ned av Regjeringen for å kartlegge samfunnets digitale sårbarhet. Utvalget foreslår konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet.

Standarder

- ISO 27000-serien av standarder om informasjonssikkerhet
- ISO 31000 Risikostyring
- ISO/NS Samfunnssikkerhet
- ADQ: Kommisjonsforordning (EU) nr. 73/2010 av 26. januar om krav til kvalitet for luftfartsdata og luftfartsinformasjon i det felles europeiske luftrom
- Forskrift om IT-standarder i offentlig forvaltning
- Liste over anbefalte og obligatoriske IT-standarder i offentlig sektor (Referansekatalogen) https://www.difi.no/veiledning/ikt-og-digitalisering/standarder/bruksomrader