UNINETT Fagspesifikasjon

Veiledning i klassifisering av informasjon

FAGSPESIFIKASJON FRA UNINETT

Veiledning i klassifisering av informasjon

Versjon 2 - 2017

UFS nr:	136
Status:	Utkast
Dato:	25. 10. 2017
Tittel:	Veiledning i klassifisering av informasjon
Arbeidsgruppe:	Informasjonssikkerhet
Ansvarlig:	Øivind Høiem
Kategori:	Anbefaling

UNINETT

SAMMENDRAG

Dette dokumentet spesifiserer universitets- og høgskolesektorens anbefalte krav til klassifisering av informasjon. Veiledningen beskriver hvordan man kan identifisere institusjonens informasjonsobjekter, klassifisere disse med hensyn til konfidensialitet og kritikalitet og å definere oppbevaringsperioder og disponeringsregler. Det er spesielt viktig å få gjort denne type klassifisering før man legger informasjon ut i skyen, og ved bruk av mobile enheter som lesebrett og smarttelefoner.

Videre er dette dokumentet ment som et verktøy for informasjonseiere for å sikre at virksomhetskritisk innhold blir behandlet på rett måte.

Retningslinjene har referanser til relevante standarder, lover og forskrifter.

Innholdsfortegnelse

1 INTRODUKSJON

Vår største utfordring er ikke hvordan vi skal få dokumentert alt, men hvordan vi skal få sortert ut og tatt vare på den informasjonen som er viktig for oss alle. Hvor lenge skal informasjonen oppbevares? Hva må oppbevares på grunn av lovkrav? Hva er viktig å ta vare på for ettertidens historikere? Hvilken informasjon må makuleres etter bruk på grunn av personvernet? Har vi fokus på hvordan vi forvalter den informasjonsmengden vi omgir oss med til daglig? Klassifisering og verdivurdering av informasjon har ofte blitt forsømt. I vårt samfunn av informasjonsoverflod er det viktig å ta vare på det vi må bevare, og kvitte oss med resten.

Arkivloven med forskrifter danner det rettslige grunnlaget for arbeidet med bevaring og kassasjon i offentlig forvaltning. Formålet med bevaring av offentlige arkiver er å sørge for at arkiver som har stor kulturell eller forskningsmessig verdi, eller som inneholder rettslig eller viktig forvaltningsmessig dokumentasjon, blir bevart og gjort tilgjengelig for ettertida.

I praksis kan vi ikke bevare alle papirarkiver og all informasjon i de elektroniske systemene som virksomheter etterlater seg. Det er knyttet store kostnader til oppbevaring og tilgjengeliggjøring av papirarkiv og elektroniske arkiv. Arkiver som blir avlevert arkivdepot skal ofte oppbevares for all framtid. Vurdering og klassifisering er derfor viktig.

Hensikten med retningslinjene er å være til hjelp i det daglige arbeidet ved å beskrive hvordan man kan identifisere institusjonens informasjonsobjekter, klassifisere disse med hensyn til beskyttelsesgrad og virksomhetskritikalitet og å definere oppbevaringsperioder og disponeringsregler.

Veiledningen er ment som et verktøy for informasjonseiere og andre for å sikre at virksomhetskritisk innhold vil bli tatt vare på, behandlet og avhendet i samsvar med interne og eksterne krav og beste praksis. Det er spesielt viktig å få gjort denne type klassifisering før man legger informasjon ut hos skyleverandører, og ved bruk av mobile enheter som lesebrett og smarttelefoner.

Kapittel 2 gir en oversikt over prosessen for informasjonsklassifisering og gjør rede for attributtene som bør vurderes.

En bevarings- og kassasjonsplan er viktig for god drift av et effektivt informasjons-behandlingssystem. Det gir retningslinjer for oppbevaring og disponering av informasjon som genereres i løpet av den daglige virksomhet og sikrer kontinuitet, beskytter organisasjonens juridiske rettigheter, og gjør at informasjonen lett kan hentes fram etter behov.

Veiledningen er utarbeidet av UH-sektorens sekretariat for informasjonssikkerhet i samarbeid med UH-sektoren.

INFORMASJONS-KLASSIFISERING

Det anbefales at man bruker følgende attributter når informasjon skal klassifiseres:

Eier
Hvilken organisatorisk enhet, rolle eller arbeidsprosess har eierskapet til informasjonen.

Innhold
Type informasjon, uavhengig av format og medium. Hva informasjonen handler om.

For eksempel FOU-søknader, arbeidskontrakter, fagplaner eller regnskapsrapporter.

Hjemmel
Referanse til regulatoriske dokument (lov, regel, forskrift, styrende dokument) hvor oppbevaring og/eller disponering framgår.

For eksempel **offl. § 25** (LOV 2006-05-19 nr 16: Lov om rett til innsyn i dokument i offentleg verksemd, offentleglova § 25) eller **fvl. § 13.1** (LOV 1967-02-10 nr 00: Lov om behandlingsmåten i forvaltningssaker, forvaltningsloven § 13, første ledd).

Lagringssted
Navnet på systemet og/eller fysiske arkiv der informasjonsobjektet oppbevares i lagringsperioden.

Fore eksempel NOARK-system, annen elektronisk journal, saksbehandlingssystem, økonomisystem m.fl.

Det er viktig at man foretar en vurdering av egnet lagringssted før lagring skjer. Man må vurdere behov for å foreta en risikovurdering, tegne en databehandleravtale med mere. Man må gjøre en særskilt vurdering hvis det er aktuelt å lagre informasjon i skyen.

Konfidensialitetsklasser
Konfidensialitetsklassene beskriver grad av beskyttelse som kreves for informasjon.

Eksempler på informasjon hvor konfidensialiteten er viktig er helseopplysninger, eksamensoppgaver før de er gitt og forskningsresultater som ikke er publisert. Det er definert fire klasser for konfidensialitet. De tre laveste klassene Åpen, Intern og Fortrolig er de som oftest vil bli brukt. Klassene Fortrolig og Strengt fortrolig er harmonisert med Sikkerhetsinstruksen.

- **Åpen (Grønn):** Informasjon kan være tilgjengelig for alle uten særskilte tilgangsrettigheter.

  Eksempler på slik informasjon er en web-side som presenterer en avdeling eller enhet som legges åpent ut på internett eller studiemateriell for et emne eller kurs som ligger åpent, men som er merket med en gitt lisens eller opphavsrett.

- **Intern (Gul):** Informasjonen må ha en viss beskyttelse og kan være tilgjengelig for både eksterne og interne, med kontrollerte tilgangsrettigheter. Benyttes dersom det vil kunne forårsake en viss skade for institusjonen, eller samarbeidspartner hvis informasjonen blir kjent for uvedkommende.

  Eksempler på slik informasjon er enkelte arbeidsdokumenter, informasjon som er unntatt offentlighet, personopplysninger, karakterer, store studentarbeider, eksamensbesvarelser, forskningsdata og -arbeider.

- **Fortrolig (Rød):** Benyttes hvis det vil forårsake skade for offentlige interesser, institusjonen, enkeltperson eller samarbeidspartner hvis informasjonen blir kjent for uvedkommende. Informasjonen skal ha strenge tilgangsrettigheter.

  Eksempler på slik informasjon er enkelte strategidokumenter, store mengder av sensitive personopplysninger, helseopplysninger, eksamensoppgaver før de er gitt, enkelte typer forskningsdata og -arbeider.

Hvis man har behov for et fjerde og høyere nivå for konfidensialitet kan man bruke klassen

- **Strengt fortrolig (Sort)** og gjøre en avgrensning mellom den og Fortrolig. Strengt fortrolig benyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, institusjonen, enkeltperson eller samarbeidspartner at informasjonen blir kjent for uvedkommende. Informasjonen skal ha de strengeste tilgangsrettigheter.

  Eksempler på slik informasjon er informasjon om personer som har adressesperre kode 7 eller som har behov for annen særlig beskyttelse og svært konfidensielle forskningsdata og -arbeider.

Noen institusjoner har informasjon som skal beskyttes etter beskyttelsesinstruksen eller sikkerhetsloven. Se kapittel 3 Standarder, lover og forskrifter for mer informasjon.

Integritetsklasser
Hvor viktig det er at ikke informasjonen kan endres av uvedkommende eller ved et uhell? Hvis det er krav til at informasjonen ikke skal endres av uvedkommende eller ved et uhell må den sikres spesielt. Aktuelle sikringstiltak kan være spesielle krav til pålogging for å få mulighet til å endre dokumentet, skrivebeskyttelse eller digital signering av dokument.

Eksempler på krav til beskyttelse av dokumenters integritet:

- **Lavt krav til integritet**
  En-faktor autentisering

- **Medium krav til integritet**
  To-faktor autentisering.

- **Høyt krav til integritet**
  To-faktor autentisering. Skrivebeskyttelse. Digital signering. Logging.

At integriteten overholdes er viktig for all informasjon, men noen eksempler på informasjon hvor integriteten er spesielt viktig er søknadsfrister, karakterer og forskningsdata.

Tilgjengelighetsklasser
Hvor lenge man kan akseptere at informasjonen er utilgjengelig? Noen systemer eller tjenester er kritiske for at virksomheten skal fungere. Akseptabel nedetid kan for noen systemer variere gjennom året i forhold til for eksempel eksamen, opptak, rapporteringer m.m.

Eksempler på perioder er:
- 1 time
- 1 dag
- 1 uke
- 1 måned

Man må også vurdere om informasjonen kan lagres i skyen. Da er man avhengig av at man har internett-tilgang helt frem til datasenteret som tilbyr skytjenesten.

Eksempler på informasjon hvor tilgjengeligheten er viktig er fagsystemer i kritiske faser for studentopptak og eksamensavvikling, store student- eller forskningsarbeider, eksamensbesvarelser og forskningsdata.

Bevaringsverdi
Bevaringsverdi er en vurdering som angir den relative betydningen informasjonen har for organisasjonen. Dette kan for eksempel være:

- Juridisk verdi
- Virksomhetskritisk
- Historisk verdi

Personopplysninger
Hvis informasjonsobjektet inneholder eller kan inneholde personopplysninger, skal dette avmerkes i tabellen.

- **PERSONOPPLYSNINGER** er opplysninger og vurderinger som kan knyttes til en enkeltperson. Eksempler på personopplysninger er navn, fødselsnummer, bilde, video og lydopptak, logg fra bruk av adgangskort, informasjon fra en kilde, blodprøver og google-søk på person.

- **SENSITIVE PERSONOPPLYSNINGER** er definert som opplysninger om rasemessig eller etnisk bakgrunn, politisk, filosofisk eller religiøs oppfatning, at en person har vært

mistenkt, siktet, tiltalt eller dømt for en straffbar handling, helseforhold, seksuelle forhold, medlemskap i fagforeninger samt genetiske data og biometriske data som anvendes til identifisering av personer.

Skylagring
Angi om informasjonen er egnet for skylagring. Enkelte informasjonstyper kan ikke lagres i skyen på grunn av lovkrav eller er ikke egnet for skylagring av andre grunner. Dette gjelder spesielt lagring utenfor Norge eller EU/EØS-området. Informasjon som kan falle inn under disse kategoriene må gjennomgå en særskilt risikovurdering før en eventuell lagring i skyen.

Dette gjelder for eksempel:

- Regnskapsdata
- Arkivverdig materiale
- Sensitive personopplysninger
- Fortrolig informasjon
- Virksomhetskritisk informasjon

UNINETT har utarbeidet en juridisk veileder for skytjenester.
Lenke: https://www.uninett.no/skytjenester/juridisk-veileder-skytjenester

Den norske arkivloven er under revisjon (pr. oktober 2017) så det vil muligens bli endringer i hva som kan lagres utenlands.

Arkivnøkkel
En arkivnøkkel er et system for ordning av sakarkiv basert på ett eller flere ordningsprinsipper. Arkivnøkler beskriver inndelingsprinsipper og rekkeordningssystemer og benytter vanligvis et ordningsprinsipp på inndeling etter emne. Statlige organer skal ifølge arkivforskriften bruke «Felles arkivnøkkel for statsforvaltningen».

Oppbevaringsperiode
Den tid som informasjonen skal oppbevares i arkivet. Oppbevaringsperioden starter når informasjonsobjekt blir til, og oppgis i antall år.

- **PERMANENT** – informasjonsobjektet oppbevares permanent.
- **LEVETIDSRELATERT** – informasjonsobjektet er levetidsrelatert i forhold til andre objekter (datasystemer, prosjekter, programmer, kontrakter, bygninger, ansettelsesforhold, studieforhold eller lignende). Det er vanlig at man setter en oppbevaringsperiode som kan være 5 eller 10 år etter at objektet er avhendet, kontrakten er utløpt osv.
- – institusjonen har definert oppbevaringsperioden, for eksempel hvis oppbevaringsperiode er koblet til en hendelse, aktivitet eller er lovpålagt.

Avhendingsregler
Regler for avhending av informasjonen etter endt oppbevaringsperiode. Merk at det kan være spesielle regler for bevaring av informasjon som gjelder egen virksomhet eller som har prinsipiell karakter. Rutinemessige enkeltsaker som har mistet sin administrative betydning kan ofte kasseres.

- **GJENNOMGANG** – send informasjonsobjektet til informasjonseieren for gjennomgang etter utløpt oppbevaringsperiode.

- **KASSER** – kasser informasjonsobjektet umiddelbart etter utløpt oppbevaringsperiode. Vær oppmerksom på at informasjonsobjekter som inneholder personopplysninger krever sikker destruering.
- **DEPONER** – deponer informasjonsobjekt i arkivdepot, for eksempel hos Statsarkivet, etter utløpt oppbevaringsperiode.
- **BEVARES** – skal ikke avhendes på grunn av krav om permanent oppbevaring.

IV STANDARDER, LOVER OG FORSKRIFTER

Forvaltningsloven
LOV 1967-02-10 nr 00: Lov om behandlingsmåten i forvaltningssaker
http://www.lovdata.no/all/hl-19670210-000.html

Loven regulerer visse typer arkivmateriale gjennom bestemmelser om hvilke regler som gjelder for saksbehandling, og om hvilke rettigheter forvaltningsloven gir den enkelte. Formålet med loven er å regulere de rettigheter borgerne har når de er i kontakt med offentlige instanser. Forvaltningsloven skal ivareta rettssikkerheten til borgerne og sikre en betryggende saksbehandling. Loven er en overordnet lov som tas i bruk i all saksbehandling, så lenge ikke annen lov gjelder etter særlovgivning.

Offentleglova
LOV 2006-05-19 nr 16: Lov om rett til innsyn i dokument i offentleg verksemd
http://www.lovdata.no/all/hl-20060519-016.html

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.

Pliktavleveringslova
LOV-1989-06-09-32: Lov om avleveringsplikt for allment tilgjengelege dokument
http://www.lovdata.no/all/hl-19890609-032.html

Føremålet med denne lova er å tryggja avleveringa av dokument med allment tilgjengeleg informasjon til nasjonale samlingar, slik at desse vitnemåla om norsk kultur og samfunnsliv kan verta bevarte og gjorde tilgjengelege som kjeldemateriale for forsking og dokumentasjon.

Personopplysningsloven
LOV 2000-04-14 nr 31: Lov om behandling av personopplysninger
http://www.lovdata.no/all/hl-20000414-031.html

Loven omfatter behandling av personopplysninger med elektroniske hjelpemidler, og manuell behandling av personopplysninger som innebærer opprettelse av et personregister.

Formålet med loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. 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.

Forskrift om behandling av personopplysninger (personopplysningsforskriften)
https://lovdata.no/dokument/SF/forskrift/2000-12-15-1265?q=personopplysningsforskriften

UNINETTs veileder om den nye Personvernforordningen
https://www.uninett.no/personvernforordningen-gdpr

eForvaltningsforskriften
FOR-2004-06-25-988 Forskrift om elektronisk kommunikasjon med og i forvaltningen
http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20040625-0988.html

Formålet med forskriften har vært å utarbeide et felles regelverk som legger rammene for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Forskriften skal fremme forutsigbarhet og fleksibilitet, samt legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger, herunder e-signatur.

eForvaltningsforskriften inneholder bestemmelser som gir føringer for rutiner og prosedyrer knyttet til arkivdanningen.

Sikkerhetsloven
LOV-1998-03-20-10 Lov om forebyggende sikkerhetstjeneste
http://www.lovdata.no/all/hl-19980320-010.html

Lov om forebyggende sikkerhetstjeneste har et eget kapittel om informasjonssikkerhet.

Formålet med loven er ved forebyggende tiltak å trygge rikets sikkerhet og vitale nasjonale sikkerhetsinteresser mot spionasje, sabotasje og terrorhandlinger, og gjelder for hele forvaltningen. Loven skal dessuten ivareta den enkeltes rettssikkerhet og trygge tilliten til og forenkle kontrollen med tjenesten. Tiltakene skal implementeres i stat, kommune og private institusjoner som loven gjelder for.

Det er utarbeidet forskrifter innen informasjonssikkerhet, personellsikkerhet, industrisikkerhet og sikkerhetsadministrasjon. For arkivmessig behandling av dokumenter gradert etter sikkerhetsloven, er det særlig forskrift om informasjonssikkerhet som er aktuell.

Informasjon som skal beskyttes etter **Sikkerhetsloven** har følgende sikkerhetsgrader:

- **BEGRENSET** nyttes dersom det i noen grad kan medføre skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
- **KONFIDENSIELT** nyttes dersom det kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
- **HEMMELIG** nyttes dersom det alvorlig kan skade Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.
- **STRENGT HEMMELIG** nyttes dersom det kan få helt avgjørende skadefølger for Norges eller dets alliertes sikkerhet, forholdet til fremmede makter eller andre vitale nasjonale sikkerhetsinteresser om informasjonen blir kjent for uvedkommende.

Forskrift om informasjonssikkerhet
FOR-2001-07-01-744: Forskrift om informasjonssikkerhet
http://www.lovdata.no/for/sf/fo/xo-20010701-0744.html

Forskriften har samme formål og virkeområde som sikkerhetsloven.
Beskyttelsesinstruksen
FOR 1972-03-17 nr 3352: Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter
http://www.lovdata.no/for/sf/in/xm-19720317-3352.html

Instruks av for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (beskyttelsesinstruksen), omfatter dokumenter uavhengig av mediet de er tilgjengelig på.

Beskyttelse av et dokument etter beskyttelsesinstruksen skal bare foretas når dokumentet kan unntas fra offentlighet i medhold av offentleglova og skadevirkninger kan inntreffe.

Informasjons som skal beskyttes etter **Beskyttelsesinstruksen** har følgende beskyttelsesgrader:

- **FORTROLIG** benyttes dersom det vil kunne skade offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende.
- **STRENGT FORTROLIG** benyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, en bedrift, en institusjon eller en enkeltperson at dokumentets innhold blir kjent for uvedkommende.

Noark 5 - Norsk arkivstandard
https://www.arkivverket.no/forvaltning-og-utvikling/regelverk-og-standarder/noark-standarden/noark-5/noark5-standarden

Arkivloven
LOV 1992-12-04 nr 126: Lov om arkiv
http://www.lovdata.no/all/nl-19921204-126.html

Arkivforskriften
FOR 1999-12-01 nr 1566: Forskrift om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver
http://www.lovdata.no/for/sf/ku/xu-19991201-1566.html.

Forvaltningens arkivfunksjon har i lang tid vært regulert gjennom et eget regelverk. Forskriften kom som et resultat av behovet for ytterligere regulering blant annet for å regulere elektronisk arkivering av arkivmateriale. Sammen utgjør arkivloven og arkivforskriften kjernen i det regelverket som regulerer håndtering av offentlige arkiver.

Arkivloven gir en del overordnede og grunnleggende bestemmelser om arkiv og spesielt om arkiv i offentlig forvaltning. Bestemmelsene gjelder, med få unntak jf. arkivloven § 5, for all virksomhet som utøves av den offentlige forvaltning.

Formålet med arkivloven er å sikre arkiv som har betydelig kulturell eller forskningsmessig verdi, eller som inneholder rettslige eller viktig forvaltningsmessig informasjon, slik at disse kan bli tatt vare på og gjort tilgjengelige for ettertiden, jf. arkivloven § 1. Videre fastsetter arkivloven i § 6 at offentlige organ plikter å ha arkiv, og at disse skal ordnes og innrettes slik at dokumentene er sikret som informasjonskilder for samtid og ettertid.

Sammen med de utfyllende forskriftene representerer loven et helhetlig juridisk rammeverk rundt alle arkivrelaterte spørsmål i offentlig forvaltning, helt fra dokumentet oppstår som ledd i den daglige institusjonen, via arkivbegrensning og avlevering av bevaringsverdig arkiv-materiale til arkivdepot, og under oppbevaring og tilgjengeliggjøring for ettertiden.

Stortingsmelding nr. 8 (2012 – 2013) Eksport av forsvarsmateriell fra Norge i 2011, eksportkontroll og internasjonalt ikke-spredningssamarbeid

http://www.regjeringen.no/nb/dep/ud/dok/regpubl/stmeld/2012-2013/meld-st-8-2012--2013.html?id=707794

Regjeringens melding til Stortinget om omfanget av eksporten av forsvarsmateriell. I tillegg redegjøres det for norsk eksportkontrollpolitikk, regelverket og det internasjonale arbeidet når det gjelder eksportkontroll og ikke-spredning. Kapittel 3.3 tar for seg kontroll med kunnskapsoverføring til utenlandske studenter ved norske læresteder.

UNINETT

- Adresse: 7465 Trondheim
- Sentralbord: +47 73 55 79 00
- E-post: kontakt@uninett.no
- Web: www.uninett.no