UiT
NORGES
ARKTISKE
UNIVERSITET

RETNINGSLINJE
for klassifisering av informasjon

Fastsatt av: Universitetsstyret		Dato: 5.4.19	
Ansvarlig enhet:	Avdeling for IT	Id:	UiT.ITA.infosec.ret01
Sist endret av:	--	Dato: 5.4.19	
Erstatter:	Kap. 3 i ledelsessystemet for informasjonssikkerhet	Arkivref.:	2017/5560-8

Formål

En forutsetning for å kunne si noe om akseptabel bruk samt behovet for sikkerhetstiltak er at det er foretatt en klassifisering av informasjonen som behandles. Klassifiseringen ligger til grunn for vurderingen av hvilken grad av sikring (IT-teknisk, organisatorisk og fysisk) informasjonen skal underlegges. Videre vil klassifisering bidra til å oppnå en oversikt over hvilke informasjonsverdier UiT forvalter.

Klassifiseringen vil videre gi personer som skal behandle informasjonen en konkret indikasjon og veiledning på hvordan denne skal håndtere og beskyttes.

Virkeområde

Retningslinjen gjelder for alle som behandler informasjon på vegne av UiT Norges arktiske universitet («UiT»), uavhengig av tilknytning (ansatt, student, eksterne mv).

All informasjon UiT forvalter skal klassifiseres i henhold til denne retningslinjen, med mindre annet fremkommer her.

Informasjon som er underlagt sikkerhetsloven[1] skal ikke klassifiseres etter nivåene i denne retningslinjen, men etter de klassifiseringsnivå som følger av sikkerhetsloven selv. For øvrig gjelder retningslinjen så langt den passer.

Retningslinjen regulerer ikke håndtering av innsynskrav etter offentlighetsloven, forvaltningsloven m.m.

[1] Lov av 1.6.2018 nr 24 om nasjonal sikkerhet (sikkerhetsloven).

Ansvar, myndighet og oppgavefordeling

Informasjonseier
All informasjon skal ha en entydig og identifiserbar eier. Det skal være mulig å finne ut hvem som er ansvarlig for at informasjonen er vedlikehold, oppdatert og riktig merket med tilhørende klassifiseringsklasse.

Informasjonseier skal være en organisatorisk enhet, rolle eller arbeidsprosess.

Eier av informasjonen er ansvarlig for vurderingen som ligger til grunn for plasseringen i den aktuelle klassifiseringsklassen. Dette skal gjøres i henhold til denne retningslinje samt øvrig regelverk og rutiner som omhandler klassifisering.

Systemeier
Systemeier plikter å vurdere hvilke konfidensialitets-, integritets- og tilgjengelighetsklasser systemet eller tjenesten skal godkjennes for. Dette gjøres gjennom risiko- og sårbarhetsvurderinger. Som hovedregel skal denne konklusjonen, samt eventuelle forutsetninger informasjonseier og bruker må kjenne til, bekjentgjøres via informasjonssikkerhetssidene til UiT, relevante brukerveiledninger og opplæring.

Brukere
Alle personer som håndterer informasjon for UiT har plikt til å foreta klassifisering i tråd med relevante retningslinjer og de vurderinger som informasjonseier har foretatt.

IT-direktøren
IT-direktøren kan foreta endringer i denne retningslinjen samt fastsette tilhørende rutiner og prosedyrer.

Definisjoner og forkortelser
Konfidensialitet: Informasjon skal beskyttes mot uautorisert innsyn, tilgang eller misbruk.

Integritet: Informasjon skal beskyttes mot uautorisert endring eller sletting.

Tilgjengelighet: Informasjonen skal være tilgjengelig for alle som skal ha tilgang til den, når de behøver det.

Beskrivelse
Informasjon skal klassifiseres innenfor følgende kategorier:
- Konfidensialitet,
- Integritet og
- Tilgjengelighet.

Informasjonseier må ta hensyn til systemeiers klassifisering av systemet eller tjenesten når det besluttes hvilke(t) av UiTs system eller tjeneste som skal benyttes for den aktuelle informasjonen. Dersom det er forskjeller mellom systemets eller tjenestens klassifisering og det behovet informasjonseier har, må dialog opprettes mellom system- og informasjonseier. Dette for å avklare om tiltak kan iverksettes for å imøtekomme det behovet informasjonseier har, om ny løsning må vurderes mv.

Konfidensialitet

Ved UiT skal all informasjon klassifiseres i henhold til fire konfidensialitetsklasser:

Grønn	Gul	Rød	Svart
Åpen	*Intern*	*Fortrolig*	*Strengt fortrolig*

Ved klassifisering av konfidensialitetsnivå skal enten
- kun fargekodene benyttes, *eller*
- fargekodene i kombinasjon med benevnelsene («Grønn/åpen», «Gul/intern» etc).

Benevnelsene («åpen», «intern» etc) skal ikke brukes alene med mindre annet er bestemt i disse retningslinjene.

Det aller meste av UiTs informasjon vil klassifiseres som enten Grønn, Gul eller Rød.

UiT kan ha fastsatt klare bestemmelser for plassering av enkelte typer informasjon, som overstyrer den enkelte informasjonseiers egne vurderinger. Eksempelvis skal taushetsbelagt informasjon ikke klassifiseres lavere enn Rød.

Informasjonen skal alltid plasseres i tilstrekkelig sikker klasse; ved tvil rundt rett klassifisering velges det høyeste, aktuelle nivået (dersom man f.eks er i tvil om informasjonen skal klassifiseres som Gul eller Rød, velges Rød). Tilsvarende gjelder hvis et dokument inneholder informasjon med ulik klassifisering, da skal dokumentet i seg selv klassifiseres i den høyeste, aktuelle klassen.

Det kan også være slik at informasjon skal være klassifisert i en bestemt klasse i en gitt periode, for deretter å nedgraderes. Eksempelvis vil eksamensoppgaver være klassifisert som Rød før de er gitt, mens etter eksamenen er avholdt vil de normalt sett klassifiseres som Grønn.

Videre skal man være oppmerksom på sammenstilling av informasjon. Resultatet av sammenstillingen kan få en høyere klassifisering enn de enkelte informasjonselementene som ligger til grunn (eksempelvis sammenstilling av informasjon som hver for seg er klassifisert som Gul, men hvor resultatet får et innhold som medfører klassifiseringsnivå Rød).

Særlig om Beskyttelsesinstruksen

Beskrivelsene av kategoriene Rød (fortrolig) og Svart (strengt fortrolig) er harmonisert med Beskyttelsesinstruksen[2], som regulerer behandling av dokumenter som trenger beskyttelse av andre grunner enn de som er nevnt i Sikkerhetsloven, jf Beskyttelsesinstruksen § 1.

Dette medfører *ikke* at all informasjon som klassifiseres («graderes») som hhv Rød og Svart ved UiT faller innenfor Beskyttelsesinstruksen. Nærmere vilkår for gradering følger av Beskyttelsesinstruksen § 3 jf § 4. Ved motstrid mellom disse retningslinjene og Beskyttelsesinstruksen vil instruksen ha forrang.

[2] For-1972-03-17-3352 Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrift (beskyttelsesinstruksen)

I vurderingen av om Beskyttelsesinstruksen skal anvendes må man være oppmerksom på anvendelsesområdet til instruksen, og hvilke hensyn den skal ivareta. Det kan her nevnes at instruksen har nær tilknytning til Sikkerhetsloven, tilsvarende hensyn ligger bak og det er viktig at informasjon ikke klassifiseres etter Beskyttelsesinstruksen hvis vilkårene ikke er oppfylt.

Før informasjon klassifiseres etter Beskyttelsesinstruksen bør informasjonssikkerhetsrådgiver kontaktes.

Når informasjon er klassifisering etter Beskyttelsesinstruksen skal melding sendes til informasjonssikkerhetsrådgiver, slik at det kan holdes en oversikt over omfanget av denne typen informasjon ved UiT.

Dersom et dokument skal graderes etter Beskyttelsesinstruksen skal ikke fargekodene benyttes, kun betegnelsene «Fortrolig» og «Strengt fortrolig».

Beskyttelsesinstruksen har bestemmelser om behandling av dokumenter som er gradert som hhv. Fortrolig og Strengt fortrolig. Blant annet er det konkrete krav til merking etter instruksens § 6.

Nærmere beskrivelse av de ulike konfidensialitetsklassene:

	Åpen

Informasjon *kan* eller *skal* være tilgjengelig for alle uten særskilte tilgangsrettigheter.

Det aller meste av informasjonen UiT forvalter er i klassen Grønn, enten som konsekvens av mål og hensikt med universitets virksomhet eller gjennom pålegg om åpenhet i lov, forskrift og annet regelverk som regulerer offentlig forvaltning og virksomhet. Informasjon kan være i klassen Grønn selv om den ikke er lagt åpent tilgjengelig for alle.

Eksempler på slik informasjon kan være

- en nettside som presenterer en avdeling eller enhet som legges åpent ut på internett
- studiemateriell for et emne eller kurs som ligger åpent, men som er merket med en gitt lisens eller opphavsrett.
- masteroppgaver som ikke trenger noen beskyttelse
  - Fakultetet står ansvarlig for vurderingen om masteroppgaver kan/skal unntas offentlighet[3], og dermed skal plasseres i en høyere klasse.
- forskningsdata som ikke trenger noen beskyttelse
  - Forskeren står ansvarlig for denne vurderingen. Ved prosjekt som involverer flere forskere, står prosjektleder ansvarlig.
- undervisningsmateriell som ikke trenger noen beskyttelse
  - Underviseren står ansvarlig for denne vurderingen.

Merk at selv om informasjon i denne klassen kan være tilgjengelig for alle, er det ikke nødvendigvis slik at alle skal kunne *endre* den. Integriteten må derfor ivaretas ved at kun autoriserte brukere skal kunne endre informasjonen, se beskrivelse av de ulike integritetsklassene. Det er heller ikke gitt at informasjon som klassifiseres som åpen kan brukes til hva som helst, av hvem som helst.

	Intern

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 UiT eller samarbeidspartner hvis informasjonen blir kjent for uvedkommende. Det foreligger ingen lovpålagte eller interne krav om at informasjonen skal være offentlig tilgjengelig.

Eksempler på slik informasjon kan være

- enkelte arbeidsdokumenter,
- informasjon som er unntatt offentlighet,
- karakterer,
- eksamensbesvarelser,
- upubliserte forskningsdata og -arbeider.
- upubliserte forslag til forskningsprosjekter

[3] Jf. forskrift for eksamener ved UiT § 15

	Fortrolig

Rød («fortrolig») benyttes hvis det vil forårsake skade for offentlige interesser, UiT, bedrifter, enkeltpersoner eller samarbeidspartner hvis informasjonen blir kjent for uvedkommende. Informasjonen skal ha strenge tilgangsrettigheter.

Eksempler på slik informasjon kan være

- enkelte strategidokumenter,
- taushetsbelagt informasjon,
- enkelte særlige kategorier personopplysninger (tidligere «sensitive personopplysninger»), slik som helseopplysninger
- enkelte opplysninger med betydning for bygningssikkerhet og/eller informasjonssikkerhet
- eksamensoppgaver før de er gitt,
- enkelte typer forskningsdata og -arbeider.
- enkelte søknader om forskningsmidler

	Strengt fortrolig

Svart («strengt fortrolig») benyttes dersom det vil kunne forårsake *betydelig* skade for offentlige interesser, UiT, bedrifter, enkeltpersoner eller samarbeidspartner at informasjonen blir kjent for uvedkommende. Informasjonen skal ha de strengeste tilgangsrettigheter.

Plassering i denne kategorien skal kun gjøres når det er strengt nødvendig, og skal alltid gjøres i samråd med informasjonssikkerhetsrådgiver på UiT.

Eksempler på slik informasjon er

- store mengder av særlige kategorier personopplysninger (tidligere «sensitive personopplysninger»)
- helseregistre av et visst omfang
- forskningsdata og -arbeider av stor økonomisk verdi
- informasjon om personer med særlig beskyttelsesbehov, f.eks «hemmelig adresse».

Integritet

Selv om det aldri er ønskelig at informasjon skal endres utilsiktet eller av uvedkommende, vil det være store forskjeller på hvor skadelig slike endringer kan være. Det er derfor viktig å ta stilling til skadepotensialet, hvilke risikoer UiT løper hvis slike endringer skjer, og dermed også sette rammene for hvordan informasjonen skal beskyttes.

Systemeier må ta stilling til hvilke av disse integritetsklassene som systemet eller tjenesten kan klareres for, og klart gjøre kjent eventuelle forutsetninger som gjelder.

Lave krav til integritet:

Informasjonen ligger ikke til grunn for beslutninger. Handlinger basert på eventuelle feil i informasjonen kan enkelt rettes opp og vil normalt sett ikke medføre konsekvenser av økonomisk, omdømmemessig eller personlig art.

Eksempel på slik informasjon kan være:

- Generell informasjon på nettsidene,

Eksempel på tiltak:

- Tilgangsstyring med brukernavn og passord,

Middels krav til integritet

Feil i informasjonen kan medføre en viss skade. Informasjonen kan ligge til grunn for avgjørelser fattet av UiT og/eller enkeltpersoner. Handlinger basert på feil i informasjonen kan medføre konsekvenser av økonomisk art, for UiTs omdømme og/eller for enkeltpersoner.

Eksempel på slik informasjon kan være:

- studiekatalogen,
- emnebeskrivelser,
- sensorveiledninger,
- offentlig tilgjengelig versjon av UiTs interne regelverk,
- lønnsopplysninger for enkeltpersoner,
- formidling av forskningsresultater mv.

Eksempel på tiltak:

- tilgangsstyring med brukernavn og passord,
- logging,
- versjonskontroll

Høyt krav til integritet:

Feil i informasjonen kan få store konsekvenser for UiT, enkeltpersoner eller samarbeidspartnere. Disse kan være av økonomisk, omdømmemessig eller personlig art. Det kan være vanskelig å oppdage endringer i informasjonen.

Eksempel på slik informasjon kan være:

- karakterprotokoll,
- utstedte grader,
- forskningsdata (rådata),
- forskingsresultater som berører liv og helse,
- visse krypteringsnøkler,
- utbetaling av større lønnsbeløp

Eksempler på tiltak:

- sterk tilgangsstyring med multifaktorautentisering,
- endringer skal godkjennes av minst en annen,
- rutiner for å kontrollere at uautoriserte endringer ikke har funnet sted,
- logging,
- versjonskontroll

Tilgjengelighet

Brudd på tilgjengelighet kan enten innebære at
- informasjonen er utilgjengelig i en periode *eller*
- informasjonen går tapt *eller*
- informasjonen kan ikke registreres inn
    - F.eks at digital eksamen-systemet er nede under eksamensavviklingen og studenten ikke får arbeidet med besvarelsen sin, tjenester som skal ta imot forskningsdata går ned under innsamlingsperioden etc.

Informasjonen kan ha ulike krav til tilgjengelighet avhengig av kontekst og tidsperiode (f.eks vil det være høye krav til tilgjengelighet til digital eksamen-plattformen under selve eksamensavviklingen, men utenom vil kravene til tilgjengelighet være lavere).

Lave krav til tilgjengelighet

Informasjonen kan være utilgjengelig i lengre perioden uten at dette medfører konsekvenser av betydning for UiT eller enkeltpersoner. Informasjon som går tapt kan relativt enkelt gjenskapes via andre kilder, internt eller eksternt.

Eksempler på slik informasjon kan være:
- informasjon fra andre statlige organer,

Middels krav til tilgjengelighet

Dersom informasjonen er utilgjengelig kan dette redusere produksjonen ved enten hele eller deler av UiT, og/eller ha visse konsekvenser av økonomisk art, for UiTs omdømme, enkeltpersoner og/eller samarbeidspartnere.

Informasjon som går tapt kan gjenskapes, men det krever betydelig ressursbruk og/eller skaper store forsinkelser.

Eksempel på tiltak
- Backup

Høye krav til tilgjengelighet

Selv korte avbrudd kan få store konsekvenser for enkeltpersoner, samarbeidspartnere, UiTs omdømme eller økonomi.

Informasjon som går tapt kan ikke gjenskapes og dette kan få stor betydning for forsknings- og utdanningsaktiviteter, enkeltpersoner og/eller UiTs omdømme eller økonomi.

Eksempel på slik informasjon kan være:
- digital eksamen på eksamenstidspunktet,
- forskningsdata som ikke kan gjenskapes,
- forskningsdata på innsamlingstidspunktet,
- visse krypteringsnøkler,

Eksempel på tiltak:

- vaktordning for feilretting,
- beredskapsplaner
- redundans,
- backup

Referanser

- Personopplysningsloven med forskrift
- Personvernforordningen (GDPR)
- Sikkerhetsloven
- Beskyttelsesinstruksen
- Forvaltningsloven
- Offentlighetsloven
- ISO 27001 / 27002
- Klassifikasjonsnivåene samsvarer med de som er anbefalt i UNINETTs fagspesifikasjon – UFS136 Veiledning i klassifisering av informasjon.