Klassifisering av informasjonsverdier

Sektorstandard for høyere utdanning og forskning

Versjon: 1.0

Mars 2026

Innholdsfortegnelse

Informasjonsverdier og klassifisering

Med *informasjonsverdi* menes det primært informasjon som det kan medføre skade å miste eller miste kontroll over. Dette kan for eksempel omfatte rådata til forskning, forskningsresultater, upubliserte eksamensoppgaver, forretningshemmeligheter og personopplysninger. Sekundært omfattes i tillegg infrastruktur hvor slike verdier lagres og behandles, og som dermed må beskyttes i tråd med sitt innhold og sin funksjon.

Klassifisering kategoriserer informasjonsverdier etter hvordan de skal beskyttes. Dette muliggjør enklere og mer målrettede prosesser, og bidrar til å etterleve lovkrav. Dette dokumentet beskriver kunnskapssektorens sektorstandard for slik klassifisering, basert på beste praksis på området.

Sektorstandardens virkeområde grenser opp mot mange ulike lovverk. Spesielt gjøres det oppmerksom på at informasjon som er gradert etter sikkerhetsloven må håndteres i tråd med kravene der.

Ledelsessystem for informasjonssikkerhet og verdioversikt

Verdien av klassifisering blir enda større dersom den også inngår i et *ledelsessystem for informasjonssikkerhet* og dokumenteres i en *verdioversikt*. Felter som typisk vil kunne finnes i en slik oversikt er:

- Beskrivelse og avgrensning av den aktuelle informasjonsverdien
- Eventuelle lover og regelverk som tillater eller regulerer lagring og behandling av informasjonen
- Verdieier (ansvarlig leder som har myndighet til å regulere bruken av informasjonen, samt ansvar for at vurderinger og klassifisering blir utført)
- Verdivurdering basert på skadepotensialet ved sikkerhetsbrudd
- Klassifisering av informasjonen
- Interne policyer, retningslinjer og rutiner for hvordan informasjonen skal lagres og behandles
- Risikovurdering, dersom aktuelt også personvernkonsekvensvurdering
- Dokumentasjon av hvordan informasjonen flyter mellom systemer, inkludert hvilke tilgangskontroller ulike grensesnitt skal kreve
- Oversikt over alle steder hvor informasjonen er lagret, inkludert sikkerhetskopier, logger og arkiv

Som med annen detaljert sikkerhetsinformasjon kan det ha et høyt skadepotensiale om verdioversikten kommer på avveier, og bør dermed klassifiseres og sikres deretter.

Klassifisering bør skje på et så tidlig punkt i informasjonens livsløp som mulig, og følge informasjonen mellom prosesser og systemer. For forskningsdata kan dette eksempelvis oppdateres og dokumenteres gjennom en datahåndteringsplan. Ved overføring av informasjon til eksterne aktører bør kravene som klassifiseringen utløser avtalefestes, for eksempel gjennom databehandleravtaler.

Alle som behandler klassifisert informasjon, må ha forståelse for hvilke krav dette utløser. Der det er mulig bør dette integreres i verktøyene som benyttes i behandlingen.

Det må også tas høyde for at noen typer informasjon vil endre klassifisering gjennom sitt livsløp, for eksempel eksamensoppgaver som har ulike beskyttelsesbehov før og etter eksamen er avholdt. Merking av klassifisering bør derfor alltid være datert slik at nyere klassifisering overstyrer eldre, og det bør være rom for å oppgi start- og sluttdato for gyldigheten.

Klassifiseringskriterier

Informasjonen klassifiseres separat for de tre sikkerhetsaspektene konfidensialitet, integritet og tilgjengelighet, hver av dem på skalaen lav–moderat–høy–kritisk. Ulikt nivå for aspektene vil være vanlig.

Konfidensialitet (K) Informasjonen er ikke tilgjengelig for uvedkommende	**Integritet (I)** Informasjonen er korrekt og fullstendig	**Tilgjengelighet (T)** Informasjonen kan nås og brukes etter intensjonen
Lav 🟢 Informasjon som skal eller kan gjøres offentlig tilgjengelig.	**Lav** Informasjonen og konteksten den gis i tilsier ikke at virksomheten har noe ansvar for innholdets riktighet, verken juridisk, økonomisk eller etisk.	**Lav** Virksomheten får ingen betydelige skadevirkninger av at informasjonen ikke er tilgjengelig i en periode, og har ikke gitt andre implisitte eller eksplisitte garantier for tilgjengeligheten.
Moderat 🟡 Det foreligger ingen lovpålagte krav eller interne avgjørelse om at informasjonen skal være offentlig tilgjengelig, og skadepotensialet vurderes som begrenset.	**Moderat** Informasjonen har offentlig eller historisk interesse, og virksomheten har tatt ansvar for innholdet. Feil kan medføre begrenset skade.	**Moderat** Manglende tilgjengelighet forstyrrer virksomhetens utførelse av primæroppgaver, eller bryter forpliktelser i tjenestenivåavtaler med eller uten økonomisk skadevirkning.
Høy 🔴 At informasjonen kommer på avveier kan medføre betydelig skade for enkeltpersoner, egen virksomhet, partnere eller offentligheten.	**Høy** Validiteten og troverdigheten til informasjon har stor betydning, og feil kan medføre betydelig skade for enkeltpersoner, egen virksomhet, partnere eller offentligheten.	**Høy** Manglende tilgjengelighet kan medføre at egen virksomhet, partnere, offentligheten eller enkeltpersoner ikke kan få gjennomført vesentlige oppgaver innen en tidsfrist som ikke påvirkes av utfallet.
Kritisk ⚫ Kan vurderes benyttet ved fare for svært store skadevirkninger.	**Kritisk** Kan vurderes benyttet ved fare for svært store skadevirkninger.	**Kritisk** Kan vurderes benyttet ved fare for svært store skadevirkninger.

Presiseringer

Det fjerde nivået, kritisk, benyttes kun under særskilte omstendigheter hvor skadevirkningene ved sikkerhetsbrudd er svært store for virksomheten, samarbeidspartnere, enkeltpersoner eller samfunnet, og skal kun settes i dialog med sikkerhetspersonell. For konfidensialitet kan dette for eksempel gjelde større helseregistre, for integritet compliance-logger, og for tilgjengelighet Feideinnlogging under eksamensavvikling. Siden hver situasjon vil være unik legger ikke sektorstandarden føringer for hvordan virksomhetene eventuelt utdyper dette nivået med mer spesifikke regler.

Konfidensialitetsnivået kan også indikeres med fargebetegnelsene «grønn», «gul», «rød» og «svart». Markering med farge bør ikke brukes alene, da dette kan skape tvetydighet for fargeblinde. Det benyttes ikke tilsvarende alternativer for integritet og tilgjengelighet.

Permanent tap av informasjon kan ses på som en ekstrem form for tap av enten integritet eller tilgjengelighet. Sektorstandarden tar ikke stilling til hvilken av disse som skal foretrekkes så lenge det gjøres konsistent ved den enkelte virksomheten.

Eksempler på sikkerhetstiltak

For hvert av de tre sikkerhetsaspektene gjentar tabellene nedenfor klassifiseringskriteriene over, og beriker disse med veiledende eksempler på informasjonstyper og relevante sikkerhetstiltak som kan utløses av klassifiseringen.

Selve klassifiseringskriteriene bør i størst mulig grad holdes konsistente både over tid og på tvers av sektoren. Derimot er det naturlig at virksomheter som tar i bruk rammeverket løpende vurderer hvilke krav de ønsker å stille for hvert nivå, for til enhver tid å oppnå forsvarlig sikring. Tiltakene som er angitt nedenfor er ansett som relevante basert på situasjonen i 2026. De utgjør ikke et målbilde, og det må forventes at behovet for tiltak vil øke etter hvert som tekniske muligheter, sektorens modenhet og trusselbildet vi utsettes for endres.

Alle tiltak angitt for et gitt nivå er også relevante for høyere nivåer.

De tre sikkerhetsaspektene utløser av natur noe ulike typer tiltak:

- Konfidensialitetsnivået utløser primært krav til sikring mot uautorisert tilgang, eventuelt også logging av autorisert tilgang (audit-logging).
- Tilgjengelighetsnivået utløser krav til kontinuitetsplanlegging. Dette kan inkludere både robusthet og redundans i tekniske systemer, og alternative rutiner med mer manuelle grep som kan aktiveres ved tjenestebortfall.
- Integritetsnivået utløser noe mer varierte krav. Disse inkluderer backup, sikring mot uautorisert endring eller sletting, logging av endringer attribuert til identifiserbare brukere, dokumentasjon av at innhenting og behandling av data følger vedtatte rutiner, samt eventuelt alternative mer manuelle rutiner for mottak av endringer dersom nedetid ellers ville gjøre informasjonen ufullstendig.

Konfidensialitet

	Kriterier	Eksempler på informasjonstyper	Relevante sikkerhetstiltak
LAV 🟢	Informasjon som skal eller kan gjøres offentlig tilgjengelig.	• Åpne nettsider • Informasjon om studier • Åpne forskningsdatasett • Fysiske og elektroniske publikasjoner (også bak betalingsmur) • Masteroppgaver som ikke er unntatt offentlighet	Det må verifiseres at offentliggjøring ikke bryter med personvernregler eller opphavsrettigheter.
MODERAT 🟡	Det foreligger ingen lovpålagte krav eller interne avgjørelse om at informasjonen skal være offentlig tilgjengelig, og skadepotensialet vurderes som begrenset.	• Lukkede nettsider for spesifikke brukergrupper • Enkelte arbeidsdokumenter • Informasjon med hjemmel for å unntas offentlighet • Karakterer for enkeltpersoner • Eksamensbesvarelser • Upubliserte forskningsdata og –arbeider • Upubliserte forslag til forskningsprosjekter • Personopplysninger uten betydelig skadepotensiale	Tilgang skal begrenses til interne eller eksterne autoriserte brukere gjennom innlogging eller tilsvarende sikkerhetsbarriere.
HØY 🔴	At informasjonen kommer på avveier kan medføre betydelig skade for enkeltpersoner, egen virksomhet, partnere eller offentligheten.	• Taushetsbelagt informasjon • Personopplysninger med betydelig skadepotensiale eller store mengder personopplysninger • Informasjon underlagt eksportkontroll • Informasjon om virksomhetens fysiske og elektroniske sikkerhet • Eksamensoppgaver før de er gitt • Forskningsdata og -arbeider som angår sensitive teknologier • Data fra samarbeidspartnere som kan være forretningssensitive	Lagring, overføring og bruk av informasjonen skal risikovurderes. All tilgang skal kreve personidentifiserbar tofaktorautentisering og logges. Elektronisk overføring skal skje kryptert, og informasjonen bør være kryptert på lagringsmedia.
KRITISK ⚫	Kan vurderes benyttet ved fare for svært store skadevirkninger.	• Omfattende registre over personopplysninger med betydelig skadepotensiale • Datasett av stor økonomisk verdi	Ytterligere tiltak vurderes på individuell basis.

Integritet

	Kriterier	Eksempler på informasjonstyper	Relevante sikkerhetstiltak
LAV	Informasjonen og konteksten den gis i tilsier ikke at virksomheten har noe ansvar for innholdets riktighet, verken juridisk, økonomisk eller etisk.	• Informasjon under utarbeidelse • Intern sosial informasjon • Meningsytringer fra ansatte og studenter som ikke skjer på vegne av virksomheten	Den som produserer informasjonen kan selv velge hvilket tilgangsregime informasjonen skal underlegges.
MODERAT	Informasjonen har offentlig eller historisk interesse, og virksomheten har tatt ansvar for innholdet. Feil kan medføre begrenset skade.	• Hovednettsidene • Fysiske og elektroniske publikasjoner i virksomhetens navn • Uttalelser på vegne av virksomheten • Formidling av forskning • Sensorveiledninger	Innsamling, generering, import, endring og sletting skal kreve innlogging eller tilsvarende sikkerhetsbarriere, og skje i henhold til fastsatt rutine eller instruks. Offentliggjøring skal skje signert, i offisielle kanaler eller med elektronisk sertifikat.
HØY	Validiteten og troverdigheten til informasjon har stor betydning, og feil kan medføre betydelig skade for enkeltpersoner, egen virksomhet, partnere eller offentligheten.	• Forskningsresultater • Informasjon om emner og studieprogrammer • Informasjon om eksamensrett, karakterer og vitnemål • Eksamensoppgaver • Vitenskapelig informasjon som leveres på offentlig oppdrag eller mandat • Informasjon om økonomiske transaksjoner • Kontrakter og andre formelle avtaler • Krypteringsnøkler til sentrale systemer og/eller viktige data	Innsamling, generering, import, endring og sletting skal kreve personidentifiserbar multifaktorautentisering og logges. Det skal finnes sikkerhetskopier som ikke kan endres eller slettes fra primærsystemene.
KRITISK	Kan vurderes benyttet ved fare for svært store skadevirkninger.	• Ikke reproduserbar informasjon av stor sikkerhetsmessig, kulturell eller annen nasjonal viktighet	Ytterligere tiltak vurderes på individuell basis.

Tilgjengelighet

	Kriterier	Eksempler på informasjonstyper	Relevante sikkerhetstiltak
LAV	Virksomheten får ingen betydelige skadevirkninger av at informasjonen ikke er tilgjengelig i en periode, og har ikke gitt andre implisitte eller eksplisitte garantier for tilgjengeligheten.	• Enkeltpublikasjoner, både vitenskapelige og andre • Praktisk informasjon for ansatte, studenter og andre	Ingen særskilte krav utøses.
MODERAT	Manglende tilgjengelighet forstyrrer virksomhetens utførelse av primæroppgaver, eller bryter forpliktelser i tjenestenivåavtaler med eller uten økonomisk skadevirkning.	• Informasjon om emner og studieprogrammer • Eksamensinformasjon • Støttesystemer for undervisning • Publikasjonsbaser • Sak- og arkivsystem • Lønns- og personalsystem • Økonomisystem	Systemer skal være risikovurdert, og skal ha innebygd redundans eller raskt kunne erstattes av en alternativ rutine. Det skal foreligge rutiner for backup, oppgradering og vedlikeholdsvinduer.
HØY	Manglende tilgjengelighet kan medføre at egen virksomhet, partnere, offentligheten eller enkeltpersoner ikke kan få gjennomført vesentlige oppgaver innen en tidsfrist som ikke påvirkes av utfallet.	• Systemer for avvikling av eksamen • Brukerdatabaser for tjenesteinnlogging eller adgangskontroll	Systemer skal være fritt for avhengigheter av enkeltkomponenter (*single point of failure*) eller enkeltpersoner. Avtaler med tredjepartsleverandører skal ha tilgjengelighetsgarantier med kompensasjonsrett i tråd med skadepotensialet.
KRITISK	Kan vurderes benyttet ved fare for svært store skadevirkninger.	• Systemer som stiller strenge krav til sanntidsdata • Systemer for kontinuitet i miljøkontroll	Ytterligere tiltak vurderes på individuell basis.

Bakgrunn

Denne sektorstandarden erstatter Uninett fagspesifikasjon (UFS) nummer 136. Grunnstrukturen er den samme, men både omfang og terminologi er justert. Praksisen med å navngi nivåene for konfidensialitet som «åpen», «intern/beskyttet», «fortrolig» og «strengt fortrolig» fases ut av flere grunner (betegnelsene har vist seg lette å mistolke, kan komme i konflikt med tilstøtende lovverk og reguleringer, og det er enda vanskeligere å finne tilsvarende terminologi for integritet og tilgjengelighet).

En liste over relevant lovgivning og føringer finnes i vedlegg 1 i Kunnskapsdepartementets rundskriv Policy for informasjonssikkerhet for forskning og høyere utdanning