Klassifisering av informasjonsverdier

[Dokumentstatus: Innstilling fra sektorens arbeidsgruppe]

Innhold

Klassifisering av informasjonsverdier

Med informasjonsverdi menes det primært immaterielle ressurser som det kan medføre skade å miste eller miste kontroll over, slik som forskningsresultater, forretningshemmeligheter og personopplysninger. Sekundært omfattes også materielle ressurser 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 behandles, slik at alle behandlingsprosesser blir enklere og mer målrettet, inkludert å etterleve lovkrav. Dette dokumentet beskriver et rammeverk for slik klassifikasjon, basert på beste praksis på området.

Virkeområdet er begrenset til informasjon som ikke er gradert etter sikkerhetsloven. *Gradering* etter sikkerhetsloven berører bare spesielt sensitive felter, mens *klassifisering* vil være relevant for all informasjon og alle systemer som behandler informasjon.

Klassifikasjon foretas bevisst eller ubevisst hver gang man vurderer hvordan informasjonsbehandling skal foregå, men gir betydelig større effekt om det skjer konsekvent som en del av et *ledelsessystem for informasjonssikkerhet*. Der er det mest naturlig å dokumentere klassifiseringen i en *verdioversikt*. Felter som typisk vil kunne finnes i en slik oversikt er:

- Beskrivelse og avgrensning av den aktuelle verdien
- En informasjonseier som har myndighet til å regulere bruken av informasjonen – inkludert ansvaret for at klassifisering blir utført i henhold til virksomhetens behov
- Klassifisering av informasjonen, fortrinnsvis i henhold til denne sektorstandarden
- Eventuelle lovhjemler som tillater eller regulerer lagring og behandling av informasjonen
- Interne policyer, retningslinjer og rutiner for hvordan informasjonen skal lagres og behandles
- 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

Klassifisering bør skje på et så tidlig punkt i informasjonens livsløp som mulig, og følge informasjonen mellom prosesser og systemer. Dette inkluderer også ved overføring av informasjon til eksterne aktører, hvor kravene som klassifiseringen utløser må avtalefestes, for eksempel gjennom databehandleravtaler. Informasjon om klassifiseringen av gitte informasjonsverdier og hvilke krav de ulike klassene utløser må være lett tilgjengelig for alle som behandler informasjonen. Der det er mulig bør dette integreres i verktøyene som benyttes i behandlingen, men en søkbar samleoversikt vil også være en fordel. Som med all detaljert sikkerhetsinformasjon kan en slik oversikt i seg selv være sensitiv og må sikres deretter.

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

Sikt

Akser og nivåer

Informasjon klassifiseres langs de tre aksene som informasjonssikkerhetsområdet vanligvis deles opp i:

Konfidensialitet – Informasjonen er ikke tilgjengelig for uvedkommende

Integritet – Informasjonen er korrekt og fullstendig

Tilgjengelighet – Informasjonen kan ved behov brukes etter intensjonen

Langs hver akse klassifiseres informasjonen i fire nivåer: **Lav**, **Middels**, **Høy** og **Kritisk**. Det fjerde nivået, kritisk, benyttes kun under særskilte omstendigheter hvor skadevirkningene ved sikkerhetsbrudd er svært store eller berører rikets sikkerhet. Dette kan for eksempel utløses av beskyttelsesinstruksen, regelverket for eksportkontroll eller utpekelse som grunnleggende nasjonal funksjon, og skal kun settes i dialog med sikkerhetspersonell.

Konfidensialitet	Integritet	Tilgjengelighet
Lav 🟢 **(Åpen)**	**Lav**	**Lav**
Middels 🟡 **(Beskyttet / Intern)**	**Middels**	**Middels**
Høy 🔴 **(Fortrolig)**	**Høy**	**Høy**
Kritisk ⚫ **(Strengt fortrolig)**	**Kritisk**	**Kritisk**

Konfidensialitetsnivåene har unike navn som ble etablert i UFS 136, hvorav ett ble endret fra «intern» til «beskyttet» fordi det første viste seg å ofte bli misforstått. Det anbefales å fase ut disse til fordel for en felles terminologi på tvers av kategoriene, og å alltid være tydelig på hvilken kategori som omtales. Her benyttes også en fargekoding hvor nivåene betegnes som Grønn, Gul, Rød og Svart. Disse er i noen grad innarbeidet i sektoren og kan fortsatt benyttes i tillegg til nivåbetegnelsene så lenge dette ikke skaper tvetydighet for fargeblinde. Det anbefales derimot at bruken av fargekoder ikke generaliseres til de andre to aksene.

Sikt

Brudd på tilgjengelighet handler om at informasjonen ikke kan aksesseres av den som har behov for det i kortere eller lengre perioder, mens permanent tap er å anse som brudd på integritet.

Kriterier, eksempler og krav

Mens kriteriene i størst mulig grad bør holdes konsistente både over tid og på tvers av sektoren er det naturlig at virksomheter som tar i bruk rammeverket vurderer hvilke krav de ønsker å stille for hvert nivå. Kravene som er angitt nedenfor er å regne som referansekrav ut fra den nåværende situasjonen. De utgjør ikke et målbilde, og det må forventes at de vil kunne skjerpes etter hvert som tekniske muligheter, sektorens modenhet og trusselbildet vi utsetter oss for endres.

- Konfidensialitetsnivået utløser primært krav til sikring mot uautorisert innsyn, eventuelt også logging av autorisert innsyn.
- 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 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.

Alle krav som utløses for et gitt nivå er også gjeldende for høyere nivåer.

Konfidensialitet

	Kriterier	Eksempler på informasjonstyper	Eksempler på krav som utløses
LAV 🟢	Informasjon som skal eller kan gjøres åpent tilgjengelig for allmennheten.	• 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.
MIDDELS 🟡	Det foreligger ingen lovpålagte krav eller interne avgjørelse om at informasjonen skal være offentlig tilgjengelig.	• Lukkede nettsider for spesifikke brukergrupper • Enkelte arbeidsdokumenter • Informasjon unntatt 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 🔴	Informasjon som er sensitiv for egen virksomhet, avtalepartnere eller offentligheten. Dette omfatter også persondata hvor skadevirkningen for de registrerte av en lekkasje vurderes som stor.	• 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 • Enkelte typer forskningsdata og -arbeider, herunder forretningssensitive data som forskningsprosjekt har fått tilgang til	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 store samfunnsmessige konsekvenser.	• Informasjon fra enkelte typer samarbeid med Forsvaret • Datasett av stor økonomisk verdi • Omfattende registre over personopplysninger med betydelig skadepotensiale	Vurderes på individuell basis.

Tabellen tar ikke stilling til regler om offentlig innsynsrett slik det er formulert i kapittel 2 i offentleglova, som i prinsipp åpner opp for å søke innsyn i all informasjon som utformes i virksomheten uavhengig av klassifikasjon.

Sikt

Integritet

	Kriterier	Eksempler på informasjonstyper	Eksempler på krav som utløses
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.
MIDDELS	Informasjonen er ment som grunnlag for tiltak eller beslutninger, eller har historisk eller offentlig interesse, og virksomheten har tatt ansvar for innholdet.	• Hovednettsidene • Fysiske og elektroniske publikasjoner i virksomhetens navn • Uttalelser på vegne av virksomheten • Formidling av forskningsresultater • Sensorveiledninger • Styrende dokumenter	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	Informasjon som er av stor betydning for virksomheten, samarbeidspartnere, allmennheten eller personer.	• 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 store samfunnsmessige konsekvenser.	• Ikke reproduserbar informasjon av stor sikkerhetsmessig, kulturell eller annen nasjonal viktighet	Vurderes på individuell basis.

Tilgjengelighet

	Kriterier	Eksempler på informasjonstyper	Eksempler på krav som utløses
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.
MIDDELS	Manglende tilgjengelighet utløser en vesentlig forringelse av utførelsen av virksomhetens 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, avtalepartnere, 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 store samfunnsmessige konsekvenser.	Sjelden relevant i vår sektor	Vurderes på individuell basis.

Utvalgte lovkrav, forskrifter og veiledere

Sikkerhetsloven

> LOV-2018-06-01-24 Lov om nasjonal sikkerhet

Virksomhetsikkerhetsforskriften

> FOR-2018-12-20-2053 Forskrift om virksomheters arbeid med forebyggende sikkerhet

Beskyttelsesinstruksen

> FOR-1972-03-17-3352 Instruks for behandling av dokumenter som treger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter

Personopplysningsloven

> LOV-2018-06-15-38 Lov om behandling av personopplysninger

Eksportkontrolloven

> LOV-1987-12-18-93 Lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v.
>
> Denne suppleres av årlige stortingsmeldinger om «Eksport av forsvarsmateriell fra Norge»

Offentleglova

> LOV-2006-05-19-16 Lov om rett til innsyn i dokument i offentleg verksemd

Forvaltningsloven

> LOV-1967-02-10 Lov om behandlingsmåten i forvaltningssaker

EForvaltningsforskriften

> FOR-2004-06-25-988 Forskrift om elektronisk kommunikasjon med og i forvaltningen

Sikts veileder om verdioversikt

> Veileder: Utarbeidelse av verdioversikt

Sikts veileder om kontinuitetsplan

> Veileder: Kontinuitetsplan for informasjonssikkerhetshendelser

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