Dokumentstatus:

Høringsforslag av 2022-12-19 med mål om å etablere en sektorstandard

Sikt
Kunnskapssektorens tjenesteleverandør

KLASSIFISERING AV INFORMASJON

Sektorstandard

for universiteter, høgskoler og forskningsinstitutter

Sikt – Kunnskapssektorens tjenesteleverandør
Telefon: 73 98 40 40 | Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Org.nr: 919 477 822
Besøksadresser: Trondheim: Abels gate 5 – Teknobyen ● Oslo: Fridtjof Nansens vei 19 ● Bergen: Harald Hårfagres gate 29
Postadresse: Abels Gate 5A, 7030 Trondheim

Innhold

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

Klassifisering av informasjonsverdier

Med informasjonsverdi eller bare verdi menes det i dette dokumentet primært immaterielle ressurser virksomheten rår over, og som det kan medføre skade for virksomheten å miste eller miste kontroll over. 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 av informasjonsverdier gjør ressursfordeling og prioritering av sikkerhetsprosesser som hendelseshåndtering, risikostyring og kontinuitetsplanlegging enklere og mer målrettet. Dette dokumentet beskriver et rammeverk for slik klassifikasjon, basert på beste praksis på området og på behov utløst av andre prosesser i arbeidet med informasjonssikkerhet. Mens *gradering* etter sikkerhetsloven bare berører spesielt sensitive felter vil *klassifisering* 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:

- 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, 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 gjennom prosesser og systemer. Dette inkluderer også ved overføring av informasjon til eksterne aktører, hvor kravene som klassifiseringen utløser må avtalefestes. 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.

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

Akser og nivåer

Informasjon klassifiseres langs de tre aksene som til sammen utgjør informasjonssikkerhet:

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, hvorav det høyeste er definert slik at det vil brukes langt sjeldnere enn de øvrige. Nivåene identifiseres med farger, slik at grønt nivå indikerer lavest kritikalitet og utløser færrest krav, gult nivå utløser signifikante krav og rødt nivå indikerer at beskyttelse er kritisk. Det fjerde nivået, svart, benyttes kun under særskilte omstendigheter hvor skadevirkningene ved sikkerhetsbrudd er svært store eller berører rikets sikkerhet. Dette kan for eksempel utløses av sikkerhetsloven, beskyttelsesinstruksen, regelverket for eksportkontroll eller utpekelse som grunnleggende nasjonale funksjoner.

Konfidensialitet	Integritet	Tilgjengelighet
Lav **Åpen**	**Lav** Uoffisiell	**Lav** Unnværlig
Middels **Beskyttet**	**Middels** Offisiell	**Middels** Forventet
Høy **Fortrolig**	**Høy** Forvaltet	**Høy** Vesentlig
Kritisk **Strengt fortrolig**	**Kritisk** Uerstattelig	**Kritisk** Uunnværlig

Forgjengeren til denne sektorstandarden, Uninett fagspesifikasjon (UFS) 136, fokuserte primært på konfidensialitetsaksen selv om også de andre ble omtalt. Av de tre klassifiseringene er det denne som gir den mest umiddelbare nytteverdien, og det er kun denne som har fått større utbredelse i sektoren så langt. Erfaringer fra dette arbeidet har vist at betegnelsen «intern» for gul konfidensialitetsklasse medførte misforståelser, og denne er derfor endret til «beskyttet». I dette dokumentet utvides omtalen av de øvrige to aksene, og omtalen av temaer som ikke direkte berører klassifisering er utelatt.

Spørsmål til sektoren:

- Er det riktig å benytte (samme) fargeskala for alle tre aksene, slik at «røde data» kan brukes ikke bare om data med høy konfidensialitetsklasse, men også der det stilles krav til integritet og/eller tilgjengelighet?
- Er det mest hensiktsmessig å bare benytte de generelle termene lav – middels – høy – kritisk for de to «nye» aksene, eller burde også disse ha unike beskrivende termer? I siste fall, er det noen av forslagene over som bør erstattes for å bli mer forståelige?

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

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 stile for hvert nivå. Kravene som er angitt nedenfor er å regne som minstekrav 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.

Høyt konfidensialitetsnivå utløser primært krav til sikring mot uautorisert innsyn, eventuelt også logging av autorisert innsyn. Høyt tilgjengelighetsnivå utløser krav til robusthet og redundans i tekniske systemer, eventuelt med alternative mer manuelle rutiner som kan aktiveres ved tjenestebortfall. Kravene som kan utløses av høyt integritetsnivå er noe mer varierte. De 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.

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

Konfidensialitet

Kriterier	Eksempler	Krav
Informasjon som er laget for offentliggjøring eller som offentleglova krever er offentlig tilgjengelig. Annen informasjon som ikke inneholder personopplysninger eller virksomhetssensitivt innhold kan også klassifiseres som grønn.	• Åpne nettsider • Fysiske og elektroniske publikasjoner (også bak betalingsmur) • Møtereferater som det kan kreves innsyn i • Studieinformasjon	Ingen særskilte krav utøses.
Informasjon som ikke er laget for offentliggjøring og enten ikke dekkes av offentleglova eller er unntatt offentlighet på et spesifikt grunnlag.	• Lukkede nettsider for spesifikke brukergrupper • Interne arbeids-doku-menter som ikke inneholder vedtak • Ikke-sensitive person-opplysninger	Lagring, overføring og bruk av informasjonen skal risikovurderes. Tilgang skal kreve innlogging eller tilsvarende sikkerhetsbarriere. Elektronisk overføring skal skje kryptert.
Informasjon som er sensitiv for egen virksomhet, avtalepartnere eller offentligheten, eller som inneholder persondata hvor skadevirkningen for de registrerte av en lekkasje vurderes som stor.	• Taushetsbelagt informasjon • Informasjon unntatt offentlighet • Sensitive eller store mengder person-opplysninger	All tilgang skal kreve personidentifiserbar tofaktorautentisering og logges. Informasjonen bør være kryptert på lagringsmedia.
Vurderes på individuell basis.	• Informasjon som er *skjermingsverdig* men ugradert etter sikkerhetslovens bestemmelser. • Omfattende registre over sensitive personopplysninger	Vurderes på individuell basis.

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

Integritet

Kriterier	Eksempler	Krav
Hverken informasjonen selv eller konteksten den gjøres tilgjengelig i uttrykker at virksomheten står ansvarlig for korrektheten av innholdet, hverken avtalemessig, økonomisk eller moralsk.	• Upublisert informasjon under utarbeidelse • Intern sosial informasjon • Meningsytringer fra ansatte og studenter som ikke skjer på vegne av virksomheten	Ingen særskilte krav utøses.
Informasjonen er ment til å brukes til å basere aktiviteter eller avgjørelser på, eller er av historisk eller offentlig interesse, og virksomheten anser seg som ansvarlig for innholdet.	• Hovednettsidene • Fysiske og elektroniske publikasjoner i virksomhetens navn • Uttalelser på vegne av virksomheten • Studieinformasjon	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.
Informasjon av kritisk viktighet for egen virksomhet, avtalepartnere, offentligheten eller enkeltpersoner som ikke fritt kan velge å være inkludert.	• Økonomiske transaksjoner • Kontrakter og andre formelle avtaler • Informasjon om eksamensrett, karakterer og vitnemål • Vitenskapelig informasjon som leveres på offentlig oppdrag eller mandat	Innsamling, generering, import, endring og sletting skal kreve personidentifiserbar multifaktorautentisering og logges. Det skal finnes sikkerhetskopier som ikke kan endres eller slettes fra primærsystemene.
Vurderes på individuell basis.	• Ikke reproduserbar informasjon av stor sikkerhetsmessig, kulturell eller annen nasjonal viktighet	Vurderes på individuell basis.

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

Tilgjengelighet

Kriterier	Eksempler	Krav
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 • Studieinformasjon • Praktisk informasjon for ansatte, studenter og andre	Ingen særskilte krav utøses.
Manglende tilgjengelighet utløser en vesentlig forringelse av utførelsen av virksomhetens primæroppgaver, eller bryter forpliktelser i tjenestenivåavtaler med eller uten økonomisk skadevirkning.	• Eksamensinformasjon • Undervisnings-støttesystemer • 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.
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.
Vurderes på individuell basis.	– Sjelden relevant i vår sektor	Vurderes på individuell basis.

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim

Utvalgte lovkrav, standarder og forskrifter

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 (etter GDPR)

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

En mer omfattende liste over lovgivning og føringer finnes i Policy for informasjonssikkerhet for forskning og høyere utdanning. (oppdater med lenke når den er klar på sikt.no)

Spørsmål til sektoren:

- Er det fornuftig å referere til et slikt utvalg av lover og reguleringer?
- Er utvalget i så fall noenlunde riktig?
- Burde det inkluderes et avsnitt som forklarer relevansen for dette dokumentet?

Sikt ● Telefon: 73 98 40 40 ● Epost: postmottak@sikt.no ● Kundekontakt: kontakt@sikt.no ● Postadresse: Abels gate 5A, 7030 Trondheim