Retningslinje for klassifisering av informasjon

Type dokument	Retningslinje
Forvaltes av	Leder av IT-avdelingen
Godkjent av	Direktør for Organisasjon og infrastruktur
Gjelder fra	12.06.2023
Neste revisjon	12.06.2025
Unntatt offentlighet	Nei
Referanse ISO	ISO27002:2022 5.9,5.10,5.12,5.13,8.12
Referanse NSMs grunnprinsipper for IKT-sikkerhet	2.7.5
Referanse LOV/Regel	Sikkerhetsloven, Personvernloven, Sikkerhetsinstruksen
Referanse interne dokumenter	Politikk for informasjonssikkerhet

1. Formål

Formålet med klassifisering av informasjon er å ha oversikt over hvilke informasjonsverdier NTNU forvalter.

2. Gjelder for

Retningslinjen for klassifisering av informasjon gjelder for alle som har tilgang til, og/eller bearbeider og forvalter informasjon ved NTNU, for eksempel gjennom NTNUs informasjonssystemer, tjenester og utstyr (NTNUs IKT-infrastruktur).

3. Overordnede prinsipper

a. For å kunne møte krav til forsvarlig behandling av informasjonsverdier, skal informasjonsobjekter som produseres og forvaltes ved NTNU klassifiseres.
b. Klassifisering av informasjonen som produseres, eller tilføres, i et IKT-system eller prosess, angir krav til sikring av IKT-systemet og arbeidsprosessen som benytter, transporterer eller lagrer informasjonen.
c. Informasjon/informasjonsobjekter skal klassifiseres og merkes som nivå 1, 2, 3 eller 4 innenfor Konfidensialitet, Integritet og Tilgjengelighet for å avdekke korrekt beskyttelse og behandling av informasjonsobjektet.

4. Verdivurdering og klassifisering

En informasjonsverdi er informasjon som er definert som noe vi som enkeltpersoner, NTNU, eller samfunnet ønsker å beskytte. Informasjonsverdier kan deles inn primære informasjonsverdier, selve informasjonen, og sekundære informasjonsverdier, det vil si lokaler, systemer og mennesker som behandler og oppbevarer informasjon.

a. Informasjon som oppbevares og produseres ved NTNU skal igjennom en verdivurdering[1]. Dette gjøres ved å avgjøre hva slags verdi objektet har for NTNU, og hva slags verdi objektet har for andre aktører. Eksempel på informasjonsverdier ved NTNU er:
   i. Forskning – Har verdi for NTNU som universitet, for forskerne og potensielt en verdi for samfunnet.
   ii. Dokumentasjon – Systemdokumentasjon, planverk osv.
   iii. Systemer – Noen systemer har verdi ved at vi er avhengig av dem for å få gjort jobben vår, andre ved at de brukes for å lagre data som har verdi.
   iv. Personopplysninger – Dette er ikke en verdi for NTNU, men en verdi for hver enkelt person det gjelder. På bakgrunn i dette stilles det krav til NTNU for hvordan personopplysninger skal oppbevares.
   v. Fysiske områder – laber, arkivrom, serverrom osv. der informasjon og forskning opprettes, bearbeides og lagres.
b. Basert på verdivurderingen klassifiseres informasjonsobjektet i samsvar med interne og eksterne krav til konfidensialitet, integritet og tilgjengelighet.
   i. At noe er *konfidensielt* betyr at det er krav til tilgangsstyring; dette betyr i praksis å sikre at informasjon og informasjonssystemer bare er tilgjengelig for de som har et tjenstlig behov.
   ii. *Integritet* betyr å sikre at informasjon er korrekt, gyldig og fullstendig og ikke kan endres utilsiktet eller av uvedkommende.
   iii. Å sikre *tilgjengelighet* vil si at informasjon og informasjonssystemer er tilgjengelig innenfor de tilgjengelighetskrav som er satt.
c. Krav til riktig klassifisering av informasjonsverdier kommer fra mange parter og har forskjellige mål:
   i. Ha oversikt over hvilke verdier NTNU besitter.
   ii. Fastslå hvilke informasjon/system/objekt som er viktigst for å nå NTNUs mål, samt holde seg innenfor gjeldende regelverk og imøtekomme inngåtte avtaler.
   iii. Sortere hvilken informasjon og IKT-systemer som skal prioriteres ved en hendelse som medfører begrenset kapasitet.
   iv. Forenkle arbeidet med å bygge en effektiv og driftsøkonomisk informasjonsarkitektur

4.1. Vurdering av *Tilgjengelighet*

Klassifisering	Nivå	Beskrivelse
Svært høy	4	Informasjonsverdien påvirker kjernevirksomheten og er kritisk for drift av universitetet
Høy	3	Informasjonsverdien påvirker avdelinger, seksjoner eller fellesfunksjoner, men ikke drift av universitetet.
Moderat	2	Informasjonsverdien påvirker kun enkelte isolerte systemer, tjenester eller funksjoner.
Lav	1	Informasjonsverdien er isolert og påvirker kun et system, tjeneste eller et mindre antall brukere og har ingen betydning for drift av universitetet eller viktige funksjoner.

[1] NSMs «Veiledning i verdivurdering av informasjon»

4.2. Vurdering av *Integritet*

Klassifisering	Nivå	Beskrivelse
Svært høy	4	Det er av kritisk betydning at det avleveres autentisk og gyldig informasjon. Utilsiktet eller tilsiktet feilinformasjon vil kunne føre til feilvurderinger eller beslutninger med fatale konsekvenser. Feil i informasjonen kan medføre tap av liv, for eksempel ved feilbehandling av pasienter, eller feilkonstruksjoner i bygg. Brudd kan medføre korrupte data i sentrale systemer som fører til omfattende følgefeil og påfølgende stort tap av produsert materiale ved NTNU.
Høy	3	Den som benytter informasjonen, er avhengig av at den er autentisk og gyldig. Utilsiktet eller tilsiktet feilinformasjon vil kunne føre til feilvurderinger eller beslutninger slik at det kan medføre betydelig økonomisk tap, omdømmetap eller annen skade for NTNU, enkeltindivider eller samarbeidspartnere. Dette kan være, men ikke begrenset til; Grunndata, forskningsdata og publikasjoner hvor autentisitet er svært viktig.
Moderat	2	Den som benytter informasjonen, forventer at den er autentisk og gyldig. Feil i informasjonen kan gi moderate økonomiske skader og/eller svekket omdømme for NTNU, enkeltindivider eller samarbeidspartnere.
Lav	1	Feil påvirker ikke beslutningsprosesser Arbeidsdokumenter, hvor feil i informasjonen ikke får negativ konsekvens i beslutningsprosesser hos den/de som benytter informasjonen.

4.3. Vurdering av *Konfidensialitet*

Klassifisering	Nivå	Beskrivelse
Strengt Fortrolig	4	Strengt fortrolig benyttes dersom det vil kunne forårsake betydelig skade for offentlige interesser, NTNU, enkeltindivider eller samarbeidspartnere at informasjonen blir kjent for uvedkommende. Informasjon skal kun være tilgjengelig for medarbeidere med strengt kontrollerte rettigheter og som har behov for denne informasjonen for å utføre en pålagt oppgave. Eksempler på informasjon i denne kategorien: Store mengder særlige kategorier («sensitive») personopplysninger, store mengder helseopplysninger kunnskap/forskning som inngår i eksportkontroll.
Fortrolig	3	Fortrolig benyttes dersom det vil kunne skade offentlige interesser, NTNU, enkeltindivider eller samarbeidspartnere at informasjonen blir kjent for uvedkommende. Informasjon skal kun være tilgjengelig for medarbeidere med kontrollerte rettigheter og som har behov for denne informasjonen for å utføre en pålagt oppgave. Eksempler på informasjon: Særlige kategorier av personopplysninger (tidligere kalt «sensitive personopplysninger»), herunder helseopplysninger, taushetsbelagte opplysninger.
Intern	2	Intern benyttes om informasjon som er begrenset til å være tilgjengelig for medarbeidere for å gjennomføre pålagte oppgaver. Informasjonen kan være tilgjengelig for eksterne med kontrollerte tilgangsrettigheter. Eksempler på informasjon: Arbeidsdokumenter, informasjon som er unntatt offentlighet, mange typer av personopplysninger.
Åpen	1	Åpen informasjon som er tilgjengelig for alle uten særskilte tilgangsrettigheter. Informasjon som ikke kan skade noe eller noen, og alle kan få se. Eksempler på informasjon: Åpen kilde informasjon, offentlige websider, kursoversikter og innhold.

4.4. Krav til merking

a. Ved merking av informasjonsverdier skal merkingen være godt synlig.
b. Ved høyt krav til konfidensialitet (Fortrolig/Strengt Fortrolig) skal informasjonsverdien merkes med klassifisering, følgende merker skal brukes:

NTNU

STRENGT FORTROLIG
Iht. Beskyttelsesinstruksen

FORTROLIG
Iht. Beskyttelsesinstruksen

c. Informasjonsverdier klassifisert som Intern kan vurderes merket med følgende merking:

INTERN

5. Roller og ansvar

5.1. Leder av HR- og HMS-avdelingen

a. er ansvarlig for at ledere og ansatte er kjent med, og har tilstrekkelig kompetanse, til å ivareta sitt ansvar i henhold til denne retningslinjen

5.2. Leder av IT-avdelingen

a. skal konsulteres ved endringer i retningslinjen

5.3. Leder av Seksjon for digital sikkerhet

a. skal konsulteres ved endringer i retningslinjen

5.4. Linjeleder

a. er ansvarlig for at medarbeidere har tilstrekkelig kompetanse til å klassifisere informasjon som produseres i avdelingen og at klassifisering av informasjon er en del av arbeidsrutinene
b. skal påse at avdelingen har rutiner som sikrer at informasjon som behandles, bearbeides og lagres i IKT-systemer som er godkjent for å benytte, transportere eller lagre informasjonen iht. informasjonsklassifiseringen
c. skal påse at avdelingen har rutiner for sikker oppbevaring av informasjon som gjøres tilgjengelig på papir i henhold til klassifisering av informasjonen

5.5. Systemeier

a. skal angi hvilke klassifiseringer av informasjon IKT-systemet er godkjent for å benytte, transportere og/eller lagre