Forfatter:	ØS
Godkjent av:	Håvard Breivik
Dokumenttype:	Interne retningslinjer
Godkjent dato:	01.11.2022 **Ikke gyldig etter utskriftsdag**

Retningslinjer for klassifisering av informasjon ved Nord universitet

Formål

Nord universitet forvalter store mengder informasjon. Informasjon kan ha behov for beskyttelse av flere årsaker. Konfidensiell informasjon vil alltid ha behov for beskyttelse. Ofte vil det også være nødvendig å beskytte annen informasjon, f.eks. dersom den har stor økonomisk verdi. I en del tilfeller må informasjonens integritet beskyttes, f.eks. ved at uvedkommende hindres tilgang til å endre/slette forskningsdata, virksomhetskritisk informasjon m.m.

Formålet med retningslinjene er å beskrive hvordan informasjon skal klassifiseres ut fra beskyttelsesbehov og virksomhetskritikalitet. Klassifiseringen vil være en konkret indikasjon på hvilken grad av sikring (IT-teknisk, organisatorisk og fysisk) informasjonen skal underlegges.

Klassifisering skal bidra til bevisstgjøring på hvordan informasjon skal behandles, og gi en tryggere behandling av informasjon som har behov for beskyttelse. Videre vil klassifisering bidra til å oppnå en oversikt over hvilke informasjonsverdier Nord forvalter.

Virkeområde

Retningslinjen gjelder for alle som behandler informasjon på vegne av Nord universitet (Nord) uavhengig av tilknytning (ansatt, student, ekstern oppdragstaker mv).

All informasjon Nord forvalter skal klassifiseres i henhold til denne retningslinjen, uavhengig av hvilket medium informasjonen er tilgjengelig på.

Informasjon som er underlagt *Lov 1. juni 2018 nr. 24 om nasjonal sikkerhet* (sikkerhetsloven) skal ikke klassifiseres etter nivåene i denne retningslinjen, men etter de klassifiseringsnivå som følger av loven med forskrifter. Klassene ***Fortrolig*** og ***Strengt fortrolig*** er harmonisert med Beskyttelsesinstruksen[1]. For øvrig gjelder retningslinjen så langt den passer.

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

Forfatter:	ØS
Godkjent av:	Håvard Breivik
Dokumenttype:	Interne retningslinjer
Godkjent dato:	01.11.2022 **Ikke gyldig etter utskriftsdag**

Ansvar, myndighet og oppgavefordeling

Informasjonseier

All informasjon skal ha en entydig og identifiserbar eier. Dette vil som regel være prosesseier. Det skal være mulig å finne ut hvem som er ansvarlig for at informasjonen behandles, oppdateres og klassifiseres. Informasjonseier er ansvarlig for å:

- sikre at informasjonen er plassert i riktig klasse ut fra denne retningslinjen.
- gjøre en ny vurdering når informasjonen *bytter* klasse.
- påse at all informasjon behandles i henhold til de beskyttelseskrav som stilles til den aktuelle klasse. Dette omfatter både digital og fysisk behandling av informasjon. Herunder skal brukeren bl.a. påse at uvedkommende ikke har tilgang til informasjonen, at digital behandling foregår i systemer som er godkjent for dette (se lagringsguide), og at fysisk materiale er forsvarlig oppbevart.
- regelmessig sjekke at man oppfyller eventuelle endringer i kravene.

Systemeier

Systemeier skal sørge for at det gjennomføres en vurdering av hvilke konfidensialitetsklasser et system eller tjeneste skal godkjennes for. Dette gjøres gjennom risiko- og sårbarhetsvurderinger, der bl.a. behov for tilgjengelighet, integritet og konfidensialitet skal vurderes. IT-avdelingen kan bistå i ROS-vurderingen. Systemeier er ansvarlig for at det finnes relevante brukerveiledninger, og for at brukere gis nødvendig opplæring.

Brukere

Alle personer som håndterer informasjon for Nord skal:

- foreta klassifisering i tråd med gjeldende retningslinjer, med mindre klassifisering allerede er gjort at informasjonseier.
- påse at all informasjon behandles i henhold til de beskyttelseskrav som stilles til den aktuelle klasse. Dette omfatter både digital og fysisk behandling av informasjon. Herunder skal brukeren bl.a. påse at uvedkommende ikke har tilgang til informasjonen, at digital behandling foregår i systemer som er godkjent for dette (se lagringsguide), og at fysisk materiale er forsvarlig oppbevart.

Forfatter:	ØS
Godkjent av:	Håvard Breivik
Dokumenttype:	Interne retningslinjer
Godkjent dato:	01.11.2022 **Ikke gyldig etter utskriftsdag**

CSO (Chief Security Officer)

CSO ved Nord kan foreta endringer i denne retningslinjen samt fastsette tilhørende rutiner.

Tekniske løsninger for digital behandling av informasjon (lagringsguide)

Nord har en «**lagringsguide**» med oversikt over tekniske løsninger som er godkjent for digital behandling av informasjon. I guiden finnes oversikt over hvilke konfidensialitetsklasser som kan behandles i de ulike systemer.

Dersom informasjonseier/bruker har behov for å behandle informasjon utover det som lagringsguiden tillater, må IT-avdeling kontaktes. Dette for å avklare om tiltak kan iverksettes for å imøtekomme det behovet informasjonseier har, om innkjøp av ny løsning må vurderes mv.

Dersom det er behov for å behandle opplysninger i andre systemer enn de som Nord har godkjent, må fakultetet/avdelingen før innkjøp/bruk sørge for at det blir gjennomført ROS-analyse, og ved behov gjennomføre en DPIA (personvernkonsekvensanalyse). IT-avdelingen skal da informeres. Ved gjennomføring av DPIA skal personvernombudet kontaktes.

Informasjonseier må ta hensyn til systemeiers klassifisering av systemet eller tjenesten når det besluttes hvilke(t) av Nords tekniske løsninger (systemer eller tjenester) som skal benyttes for den aktuelle informasjonen.

Klassifisering

Ved Nord skal all informasjon klassifiseres i henhold til fire konfidensialitetsklasser. Klassene beskriver grad av beskyttelse som kreves for informasjonen. De tre laveste klassene Åpen, Beskyttet og Fortrolig er de som oftest vil bli brukt. Klassene Fortrolig og Strengt fortrolig er harmonisert med Beskyttelsesinstruksen.

Ved vurderingen må det tas hensyn til hvem som kan få tilgang til informasjonen og hvilke konsekvenser det kan få dersom denne informasjonen blir tilgjengelig for uvedkommende. På bakgrunn av dette setter du en klassifikasjon - **grønn/åpen**, **gul/beskyttet**, **rød/fortrolig** eller **sort/strengt fortrolig**.

Informasjonen skal alltid plasseres i tilstrekkelig sikker klasse. I tvilstilfeller skal høyeste aktuelle klassifisering velges. Dersom man f.eks. er i tvil om informasjonen skal klassifiseres som

Forfatter:	ØS
Godkjent av:	Håvard Breivik
Dokumenttype:	Interne retningslinjer
Godkjent dato:	01.11.2022 **Ikke gyldig etter utskriftsdag**

Gul/Beskyttet eller Rød/fortrolig velges Rød/Fortrolig. Hvis et dokument inneholder informasjon med ulik klassifisering, skal dokumentet klassifiseres i den høyeste, aktuelle klassen.

I enkelte tilfeller kan informasjonens beskyttelsesbehov endre seg, slik at klassifiseringen må endres. Eksempelvis vil eksamensoppgaver være klassifisert som Rød/Fortrolig før de er gitt, mens de normalt klassifiseres som Grønn/Åpen etter at eksamenen er avholdt.

Sammenstilling av informasjon kan få en høyere klassifisering enn de enkelte informasjonselementene. F.eks. kan man ha informasjon som hver for seg er klassifisert som Gul, men der sammenstillingen gir et innhold som skal klassifiseres som Rød. Eksempelvis vil en persons fødselsnummer og kontonummer hver for seg klassifiseres som Gul/Beskyttet men samlet skal de klassifiseres som Rød/Fortrolig.

Nord kan ha fastsatt klare bestemmelser for plassering av enkelte typer informasjon, som overstyrer den enkelte informasjonseiers egne vurderinger.

De fire konfidensialitetsklassene:

Åpen (Grønn)

Informasjonen kan være tilgjengelig for alle og kan deles både internt og eksternt.

Selv om informasjonen kan være *tilgjengelig* for alle, skal likevel informasjonens integritet sikres ved at kun personer og brukere med riktige rettigheter har tilgang til å *endre* informasjonen.

Eksempler på slik informasjon kan være:

- en web-side 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.

Beskyttet (Gul):

Benyttes dersom det vil kunne forårsake en *viss skade* for institusjonen, enkeltperson eller samarbeidspartner hvis informasjonen blir kjent for uvedkommende.

Informasjonen skal beskyttes med kontrollerte tilgangsrettigheter. Informasjonen kan deles med dem den har relevans for, både internt og eksternt.

Forfatter:	ØS
Godkjent av:	Håvard Breivik
Dokumenttype:	Interne retningslinjer
Godkjent dato:	01.11.2022 **Ikke gyldig etter utskriftsdag**

Eksempler på slik informasjon kan være:

- enkelte arbeidsdokumenter
- informasjon som er unntatt offentlighet
- mange typer av personopplysninger
- karakterer
- eksamensbesvarelser
- upubliserte forslag til forskningsprosjekter
- upubliserte forskningsdata/arbeider

Fortrolig (Rød):

Benyttes dersom det vil kunne forårsake *skade* for institusjonen, offentlige interesser, enkeltpersoner eller samarbeidspartnere hvis informasjonen blir kjent for uvedkommende.

Dette er informasjon som universitetet er pålagt å begrense tilgangen til iht. lov, forskrift, avtaler, reglementer og annet regelverk. All taushetsbelagt informasjon skal minimum klassifiseres som Rød. Informasjonen skal ha strenge og kontrollerte tilgangsrettigheter, og valg av lagringsområde må vurderes nøye ut ifra hvem som skal ha tilgang.

Eksempler på slik informasjon kan være:

- taushetsbelagte opplysninger
- særskilte kategorier av personopplysninger (tidligere kalt «sensitive personopplysninger»)
- eksamensoppgaver før de er gitt
- personalmapper
- en del informasjon om f.eks. sikring av bygninger og IT-systemer
- forskningsdata/-arbeider/-søknader som inneholder konfidensielle opplysninger eller har stor økonomisk verdi

Forfatter:	ØS
Godkjent av:	Håvard Breivik
Dokumenttype:	Interne retningslinjer
Godkjent dato:	01.11.2022 **Ikke gyldig etter utskriftsdag**

Strengt fortrolig (Sort):

Benyttes dersom det vil kunne forårsake *betydelig skade* for institusjonen, offentlige interesser, enkeltpersoner eller samarbeidspartnere hvis informasjonen blir kjent for uvedkommende. Denne kategorien omfatter samme type informasjon som Fortrolig (rød), men der spesielle hensyn gjør at man ønsker å beskytte dataene ytterligere. Informasjonen skal ha de strengeste tilgangsrettighetene. Egendefinert beskyttelse.

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

Eksempler på slik informasjon er

- svært konfidensielle forskningsdata og -arbeider. Dette kan f.eks. være datasett som inneholder store mengder sensitive personopplysninger som direkte kan knyttes til enkeltpersoner, eller som inneholder variabler som muliggjør indirekte identifisering via sammenstilling av personopplysninger («bakveisidentifisering»)
- store mengder sensitive personopplysninger
- store mengder helseopplysninger
- forskningsdata og datasett av stor økonomisk verdi
- informasjon om personer med særlig beskyttelsesbehov, f.eks. adressesperre kode 7 (hemmelig adresse)

Bruk av koder og benevnelser

Ved klassifisering skal enten kun fargekode benyttes, eller fargekode i kombinasjon med benevnelse («***Røde***» data, «***Grønn/åpen***», «***Beskyttet***» etc).

Klassifisering av dokumenter i Office 365

Office 365 gir mange muligheter for å dele dokumenter. Saksdokumenter skal alltid behandles/lagres i P360 eller et godkjent fagsystem, men i spesielle tilfeller kan det være behov for midlertidig lagring og deling av saksdokumenter på Office 365-plattformen. Det kan for eksempel være behov for å

Forfatter:	ØS
Godkjent av:	Håvard Breivik
Dokumenttype:	Interne retningslinjer
Godkjent dato:	01.11.2022 **Ikke gyldig etter utskriftsdag**

samskrive dokumenter (Sharepoint), eller dele dokumentmapper i forbindelse med prosjekter (OneDrive).

I verktøylinjen i Office 365 har man mulighet for å klassifisere dokumenter i henhold til konfidensialitetsklassene som er beskrevet i denne retningslinjen. Her er det på forhånd lagt inn beskyttelse i form av kryptering på klassene **Rød/Fortrolig** og **Sort/Strengt fortrolig**.

Tilgangsbegrensning og deling:

For klassen **Gul/beskyttet** kan brukeren sette på en tilgangsbegrensning, slik at kun Nord-ansatte har tilgang til dokumentet.

For klassen **Rød/fortrolig** er det lagt inn forhåndsdefinerte grupper som brukeren kan velge å gi tilgang. (f.eks. Økonomiavdelingen, Kommunikasjonsenheten og Skikkethetsansvarlig.)

For klassen **Sort/strengt fortrolig** må brukeren velge hvilke enkeltpersoner som skal ha tilgang til informasjonen.

For at vedkommende gruppe/person som har fått tilgang skal kunne lese/redigere det klassifiserte dokumentet, må brukeren i tillegg aktivt dele dokumentet med vedkommende. Selv om et dokument er klassifisert som **Gult/beskyttet** - beskyttet til Nord-ansatte har altså ikke alle ansatte ved Nord tilgang til å lese/redigere dokumentet. Dokumentet må i tillegg være delt med vedkommende via f.eks. epost, OneDrive eller Teams.