

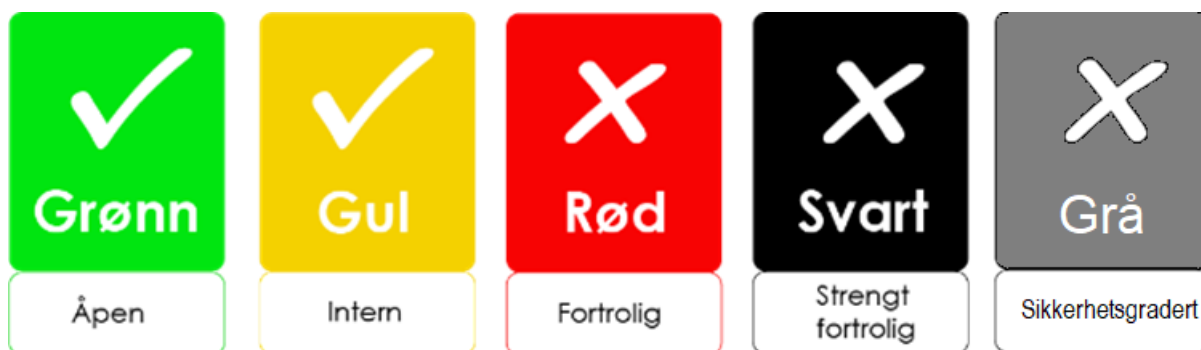
Retningslinjer for klassifisering og lagring av data og informasjon - Offentlig

September/2022/Irene L. Husa

Formål og omfang

Klassifisering av data og informasjon er nødvendig for å sikre konfidensialitet, integritet og tilgjengelighet til informasjonen. Retningslinjene gjelder alle data og informasjon som NORCE behandler og lagrer.

Våre informasjonsklasser:



IT-tjenester og applikasjoner

Klassifiseringen har betydning for hvor og hvordan informasjon skal behandles og lagres. IT-tjenestekatalog har oversikt over hvilke informasjonsklasser som er godkjent for de spesifikke IT-tjenestene og applikasjonene.

Lenke til IT-tjenestekatalog: <https://norce.sharepoint.com/sites/intranett/IT/Lists/ITTjenestekatalog>

Bestemme informasjonsklasse

Informasjon skal alltid plasseres i en tilstrekkelig sikker informasjonsklasse. Dersom du er i tvil om du skal velge f.eks. rød eller gul, skal du velge rød. Klassene er beskrevet i informasjonsklassetabellen under.

O365 er ikke godkjent for røde data, men i noen tilfeller kan prosjektleder godkjenne bruk av O365 som midlertidig arbeidsområde for røde data. Dette skal klareres med kunde eller oppdragsgiver. Alle prosjektdeltagerne forplikter seg til å kun bruke PC/Mac med NORCE oppsett og at en ikke synkroniserer informasjon ut på privat utstyr. Prosjektleder har ansvar for tilgangskontroll i O365.



Ansvar og ansvarshavende




All informasjon skal ha en entydig og identifiserbar ansvarshavende. Det skal være mulig å finne ut hvem som er ansvarlig for at informasjonen er vedlikeholdt, oppdatert og klassifisert med riktig informasjonsklasse.

Ansvarshavende av informasjonen er ansvarlig for å:

- sikre at informasjonen er plassert i riktig informasjonsklasse ut ifra disse reglene.
- gjøre en vurdering når informasjonen bytter informasjonsklasse.
- påse at all lagring, behandling og bearbeiding av informasjon foregår på tekniske løsninger som er godkjent for dette – se IT-tjenestekatalog.
- regelmessig sjekke at man oppfyller eventuelle endringer i kravene.

Informasjonsklasser

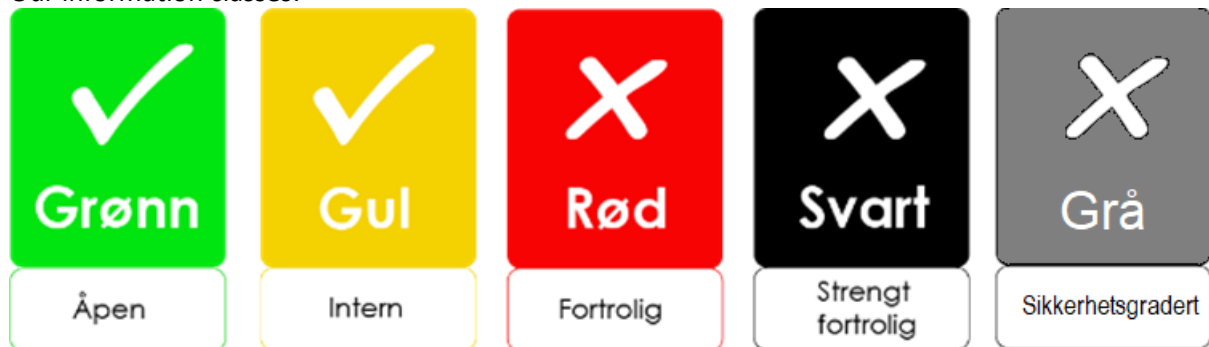
Informasjonsklasser	Beskrivelse	Eksempler	Tilgjengelighet	Beskyttelsesinstruks (Lovdata.no, 1972)	Potensiell skade (MAPS, 2022)	Lov, regelverk og begrensninger
 Grønn 	Grønn - Åpen Skal eller kan være tilgjengelig for alle	<ul style="list-style-type: none"> • en web-side åpen mot internett • publikasjoner som ligger åpent, og som er merket med en gitt lisens og/eller opphavsrett • forskningsdata som ikke trenger noen beskyttelse • undervisningsmaterieell som ikke trenger noen beskyttelse 	Kan eller skal være tilgjengelig for alle. Integritet skal sikres.		Lav	Informasjonen kan være lisensiert med begrensninger for bruk.
 Gul 	Gul - Intern Ikke klassifisert som åpen, fortrolig, eller strengt fortrolig.	<ul style="list-style-type: none"> • enkelte arbeidsdokumenter • informasjon om interne forhold • informasjon som vi ikke vil offentliggjøre • mange typer av personopplysninger • upubliserte forskningsdata og –arbeider 	Begrenset. Kan være tilgjengelig for både eksterne og interne, med kontrollerte tilgangsrettigheter.		Mindre alvorlig	
 Rød 	Rød - Fortrolig Informasjon vi er pålagt å begrense tilgang til gjennom lover, regler, avtaler og beskyttelse av kommersielle interesser.	<ul style="list-style-type: none"> • kundeforhold og kontrakter som oppdragsgiver krever holdes fortrolig • særskilte kategorier av personopplysninger, herunder helseopplysninger • informasjon underlagt eksportkontroll • personalmapper • sikring av bygninger • dokumentasjon av IT-systemer 	Begrenset	Fortrolig	Alvorlig til kritisk	NORCE er pålagt å begrense tilgangen til data i lov, forskrift, avtaler, reglementer og annet regelverk.

Informasjonsklasser	Beskrivelse	Eksempler	Tilgjengelighet	Beskyttelsesinstruks <small>(Lovdata.no, 1972)</small>	Potensiell skade <small>(MAPS, 2022)</small>	Lov, regelverk og begrensninger
	Svart - Strengt fortrolig P-data Omfatter samme type informasjon som rød, men der spesielle hensyn gjør at man ønsker å beskytte dataene ytterligere.	<ul style="list-style-type: none"> store mengder særskilte kategorier personopplysninger, herunder helseopplysninger. 	Strengt begrenset	Strengt fortrolig	Kritisk til meget kritisk	Pålegg om beskyttelse og sikring utover de lovbestemte skal være nedfelt i avtaler eller skriftlig dokumentert på annen måte. Personvernforordning (GDPR) Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.
	Svart - Strengt fortrolig S-data Omfatter samme type informasjon som rød, men der spesielle hensyn gjør at man ønsker å beskytte dataene ytterligere.	<ul style="list-style-type: none"> forskningsdata og datasett av stor økonomisk verdi. forskningsdata og datasett av særlig art. kundeforhold og kontrakter som oppdragsgiver krever behandles strengt fortrolig. 	Strengt begrenset	Strengt fortrolig	Kritisk til meget kritisk	Pålegg om beskyttelse og sikring utover de lovbestemte skal være nedfelt i avtaler eller skriftlig dokumentert på annen måte.
	Grå - Sikkerhetsgradert Data i denne kategorien kan ikke lagres i NORCE sine interne systemer.		Data må oppbevares og behandles i kunde eller oppdragsgiver sine systemer.			Informasjon som er omfattet av Sikkerhetsloven (Lovdata.no, 2018).

Purpose and scope

Classification of data and information is necessary to ensure the confidentiality, integrity, and availability of the information. The guidelines apply to all data and information that NORCE processes and stores.

Our information classes:



IT services and applications

The classification is important for where and how the information are to be processed and stored. The IT service directory has an overview of which information classes are approved for the specific IT services and applications.

Link to IT service catalog: <https://norce.sharepoint.com/sites/intranett/IT/Lists/ITTjenestekatalog>

Decide information class

Information must always be placed in a sufficiently secure information class. If you are in doubt about whether to choose e.g., red, or yellow, select red. The classes are described in the information class table below.

O365 is not approved for red data, but in some cases the project manager may approve the use of O365 as a temporary work area for red data. This must be clarified with the customer or client. All project participants are obliged to use only PC / Mac with NORCE setup and do not to synchronize information to private equipment. The project manager is responsible for access control in O365.




Responsibility and responsible




All information must have a clear and identifiable person responsible. It must be possible to find out who is responsible for the information being maintained, updated, and classified with the correct information class.

The responsible person for the information is responsible for:

- ensure that the information is placed in the correct information class based on these rules.
- make an assessment when the information changes information class.
- ensure that all storage, processing, and processing of information takes place on technical solutions that have been approved for this - see IT service catalog.
- regularly check that any changes in the requirements are met.

Information classes

Information classes	Description	Examples	Availability	Protection instructions (Lovdata.no, 1972)	Potential damage (MAPS, 2022)	Law, regulations and restrictions
	Green - Open Must or can be available to everyone	<ul style="list-style-type: none"> • a web page open to the internet • publications that are open and marked with a given license and / or copyright • research data that does not need any protection • teaching materials that do not need any protection 	Can or should be available to everyone. Integrity must be ensured.		Low	The information may be licensed with restrictions on use.
	Yellow - Internal Not classified as open, confidential, or strictly confidential.	<ul style="list-style-type: none"> • some working documents • information on internal matters • Information that we do not want to publish • many types of personal information • unpublished research data and works 	Limited. May be available to both external and internal, with controlled access rights.		Less severe	
	Red - Confidential Information we are required to restrict access to through laws, regulations, agreements and protection of commercial interests.	<ul style="list-style-type: none"> • customer relationships and contracts required by the client are kept confidential • special categories of personal information, including health information • information subject to export control • personnel folders • securing buildings • documentation of IT systems 	Limited.	Confidential	Severe to critical	NORCE is required to restrict access to laws, regulations, agreements, regulations, and other regulations.

Information classes	Description	Examples	Availability	Protection instructions <small>(Lovdata.no, 1972)</small>	Potential damage <small>(MAPS, 2022)</small>	Law, regulations and restrictions
	Black - Strictly confidential P-data Includes the same type of information as red, but where special considerations make you want to further protect the data.	<ul style="list-style-type: none"> • large amounts of special categories of personal information, including health information. 	Strictly limited.	Strictly confidential	Critical to very critical	Orders for protection and security in addition to the statutory ones shall be laid down in agreements or documented in writing in another way. Privacy Regulation (GDPR) Norm for information security and privacy in the health and care sector.
	Black - Strictly confidential S-data Includes the same type of information as red, but where special considerations make you want to further protect the data.	<ul style="list-style-type: none"> • research data and data sets of great economic value. • research data and data sets of special nature. • customer relationships and contracts required by the client are treated in strict confidence. 	Strictly limited.	Strictly confidential	Critical to very critical	Orders for protection and security in addition to the statutory ones shall be laid down in agreements or documented in writing in another way.
	Gray - Security graded Data in this category cannot be stored in NORCE's internal systems.		Data must be stored and processed in the customer's or client's systems.			Information covered by the Security Act (Lovdata.no, 2018)

Referanser og kilder / References and sources

Instruks for behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven med forskrifter (Beskyttelsesinstruksen), (1972). <https://lovdata.no/dokument/INS/forskrift/1972-03-17-3352>

Lov om nasjonal sikkerhet (Sikkerhetsloven), (2018). <https://lovdata.no/dokument/NL/lov/2018-06-01-24>

MAPS, N. (2022). *NORCE Norwegian Research Centre AS - risikomatrise og -toleransekriterier*.

<https://norcestyring.ad.norceresearch.no/norce/?oid=3ce533c4-0c6f-42e5-995b-fcbfedc3fca3>