

Internkontroll av behandlinger av personopplysninger ved UiO 2026

Hva heter du (fornavn og etternavn)?

Hva er din e-postadresse?

Hvilken enhet er du leder for?

Angi hvilken organisatorisk enhet enheten du er leder for har nærmest tilknytning til

Det humanistiske fakultet

Det juridiske fakultet

Det matematisk-naturvitenskapelige fakultet

Det medisinske fakultet

Det odontologiske fakultet

Det samfunnsvitenskapelige fakultet

Det teologiske fakultet

Det utdanningsvitenskapelige fakultet

Museer og samlinger

Universitetsbiblioteket

Ledelse og fellesadministrasjonen

Andre enheter

Opplæring og ressurser

Før ansatte eller andre får tilgang til UiOs informasjon eller tjenester, bør de få hensiktsmessig opplæring. Dette omfatter krav til informasjonssikkerhet, personvern og interne sikringstiltak, så vel som opplæring i riktig bruk av tjenestene. Dette inkluderer for eksempel innloggingsprosedyrer, bruk av programvare, sikkerhetsinstruks, og rapportering av avvik. I tillegg bør de få regelmessig oppdatering i organisasjonens policy og rutiner.

Har de ansatte på din enhet fått tilstrekkelig opplæring innen personvern og informasjonssikkerhet?

Ikke i det hele tatt

I liten grad

I moderat grad

I stor grad

Ikke relevant

Vet ikke

Hvilke av de tilgjengelige ressursene for personvern som tilbys ved UiO benytter din enhet seg av?

Obligatorisk grunnkurs i personvern og IT-sikkerhet

E-læringskurs for administrativt ansatte

E-læringskurs for vitenskapelig ansatte

Personvernkontakter

Utøver av behandleransvaret

Personvernombud

Ressurser på nettsidene (informasjon, avtalemaler o.l.)

Vet ikke

Her kan du skrive inn eventuelle kommentarer til det obligatoriske grunnkurset eller gjennomføringen av det.

I 2025 ble det vedtatt at UiOs grunnkurs i personvern og IT-sikkerhet er obligatorisk for alle ansatte. Frist for gjennomføring av kurset ble satt til 31. januar 2026. Nyansatte skal også ta kurset.

Beskriv eventuelle andre måter opplæring innen personvern og informasjonssikkerhet ivaretas på din enhet.

Hvordan kan IT-avdelingen bedre støtte din enhet i arbeidet med informasjonssikkerhet og personvern?

Bruk av kunstig intelligens (KI)

I hvilken grad er ansatte ved din enhet kjent med hvilke KI-tjenester som kan benyttes i forbindelse med arbeid på UiO?

Se oversikt over KI-tjenester som inngår i UiOs tjenestekatalog her: <https://www.uio.no/tjenester/it/ki/>

Ikke i det hele tatt

I liten grad

I moderat grad

I stor grad

Ikke relevant

Vet ikke

I hvilken grad benytter ansatte ved din enhet KI-tjenester som ikke er godkjent til bruk ved UiO til arbeid som kan innebære behandling av personopplysninger?

Tjenester som ikke inngår i UiOs tjenestekatalog er for eksempel ChatGPT (ikke GPTUiO), Claude, Gemini, DeepSeek.

Ikke i det hele tatt

I liten grad

I moderat grad

I stor grad

Ikke relevant

Vet ikke

Hva opplever du at er årsaken til at ansatte tar i bruk ikke-godkjente KI-tjenester?

Dette elementet vises kun dersom alternativet «I liten grad eller I moderat grad eller I stor grad eller Ikke relevant eller Vet ikke» er valgt i spørsmålet «I hvilken grad benytter ansatte ved din enhet KI-tjenester som ikke er godkjent til bruk ved UiO til arbeid som kan innebære behandling av personopplysninger?»

Fordi de ansatte ikke kjenner til hvilke tjenester som er godkjent og ikke

Fordi tjenestene UiO tilbyr ikke oppleves tilstrekkelige eller hensiktsmessige for å løse arbeidsoppgaven

Fordi prosessen for å søke om å ta i bruk nye tjenester oppleves som for tidkrevende

Fordi ansatte vurderer at det er nødvendig for å være konkurransedyktig

Fordi de ansatte ønsker å ha administratortilgang i tjenestene

Annet

I hvilken grad har ansatte ved din enhet fått opplæring i bruk av KI-tjenester?

Opplæring med hensyn til personvern og informasjonssikkerhet i tjenestene og/eller hvordan KI brukes på en hensiktsmessig måte.

Ikke i det hele tatt

I liten grad

I moderat grad

I stor grad

Ikke relevant

Vet ikke

Dersom du ønsker å utdype svarene over, kan du gjøre det her.

Bruk av IT-tjenester

I hvilken grad er ansatte ved din enhet kjent med hvilke IT-tjenester som kan benyttes i forbindelse med arbeid på UiO?

Se UiOs tjenestekatalog: <https://www.uio.no/tjenester/it/alle/>

Ikke i det hele tatt

I liten grad

I moderat grad

I stor grad

Ikke relevant

Vet ikke

I hvilken grad benytter ansatte ved din enhet IT-tjenester som ikke er godkjent ved UiO til arbeid som kan innebære behandling av personopplysninger?

Eksempler på tjenester som ikke er godkjent ved UiO i dag er Slack, Questback og Surveymonkey, samt private brukerkontoer i Google, Dropbox, Microsoft etc.

Ikke i det hele tatt

I liten grad

I moderat grad

I stor grad

Ikke relevant

Vet ikke

Hva opplever du at er årsaken til at ansatte tar i bruk ikke-godkjente tjenester?

Dette elementet vises kun dersom alternativet «I liten grad eller I moderat grad eller I stor grad eller Vet ikke» er valgt i spørsmålet «I hvilken grad benytter ansatte ved din enhet IT-tjenester som ikke er godkjent ved UiO til arbeid som kan innebære behandling av personopplysninger?»

Fordi de ansatte ikke kjenner til hvilke tjenester som er godkjent og ikke

Fordi tjenestene UiO tilbyr ikke oppleves tilstrekkelige eller hensiktsmessige for å løse arbeidsoppgaven

Fordi prosessen for å søke om å ta i bruk nye tjenester oppleves som for tidskrevende

Fordi ansatte vurderer at det er nødvendig for å være konkurransedyktig

Fordi de ansatte ønsker å ha administratortilgang i tjenestene

Annet

Dersom du ønsker å utdype svarene over, kan du gjøre det her.

Tilgangsstyring

Tilgangsstyring handler om hvem som skal ha tilgang til data, systemer eller lokaler. Rett person skal ha riktig tilgang til rett tid.

Spørsmålene under gjelder særlig hvordan dere følger opp tilganger som ikke styres automatisk via stedkoder, SAP-DFØ, Cerebrum eller lignende systemer, men som må opprettes, endres eller fjernes manuelt.

Det kan for eksempel gjelde når brukere legges manuelt inn i brukergrupper i brukerinfo.uio.no, eller for IT-systemer eller fagsystemer som kun brukes av deres enhet hvor tilgang ofte administreres lokalt.

I hvor stor grad har din enhet kontroll på hvem som har tilgang til og rettigheter i IT-tjenestene og -systemene?

Inkludert når ansatte starter, slutter eller bytter rolle.

Ikke i det hele tatt

I liten grad

I moderat grad

I stor grad

Ikke relevant

Vet ikke

Har dere en etablert rutine eller praksis for å følge opp tilganger når ansatte starter, slutter eller bytter rolle?

Ja

Nei

Vet ikke

Har du kommentarer til spørsmålene over eller undersøkelsen?