Orientering om status for arbeidet med informasjonssikkerheit

Gjennomgang for leiinga

Styremøte 3-2026
Bergen - torsdag 23. april 2026

- Trusselbiletet
- Status 2025
  - avvik og hendingar
  - utførte tiltak
- Planar for 2026
  - organisering
  - ledelsessystemet (som profesjonalisering for å bli universitet)

Kvifor vi er her:
HVL - Ledelsessystem for informasjonssikkerhet og personvern

Ledelsessystem for informasjonssikkerhet og personvern er vedteke av styret og basert på standarden ISO/IEC 21001:2013

Fastsatt av KD i Rundskriv F-04-20 *Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning* :

1. Virksomheten har et ledelsessystem for informasjonssikkerhet
Det er virksomhetens øverste ledelse som har ansvaret for at informasjonssikkerheten er tilfredsstillende. Virksomhetens øverste ledelse må derfor se til at arbeidet med informasjonssikkerhet skjer på en systematisk og planmessig måte.

Dette gjøres ved at:

(i) det innføres et ledelsessystem for informasjonssikkerhet

(ii) informasjonssikkerhet inngår i den generelle virksomhetsstyringen

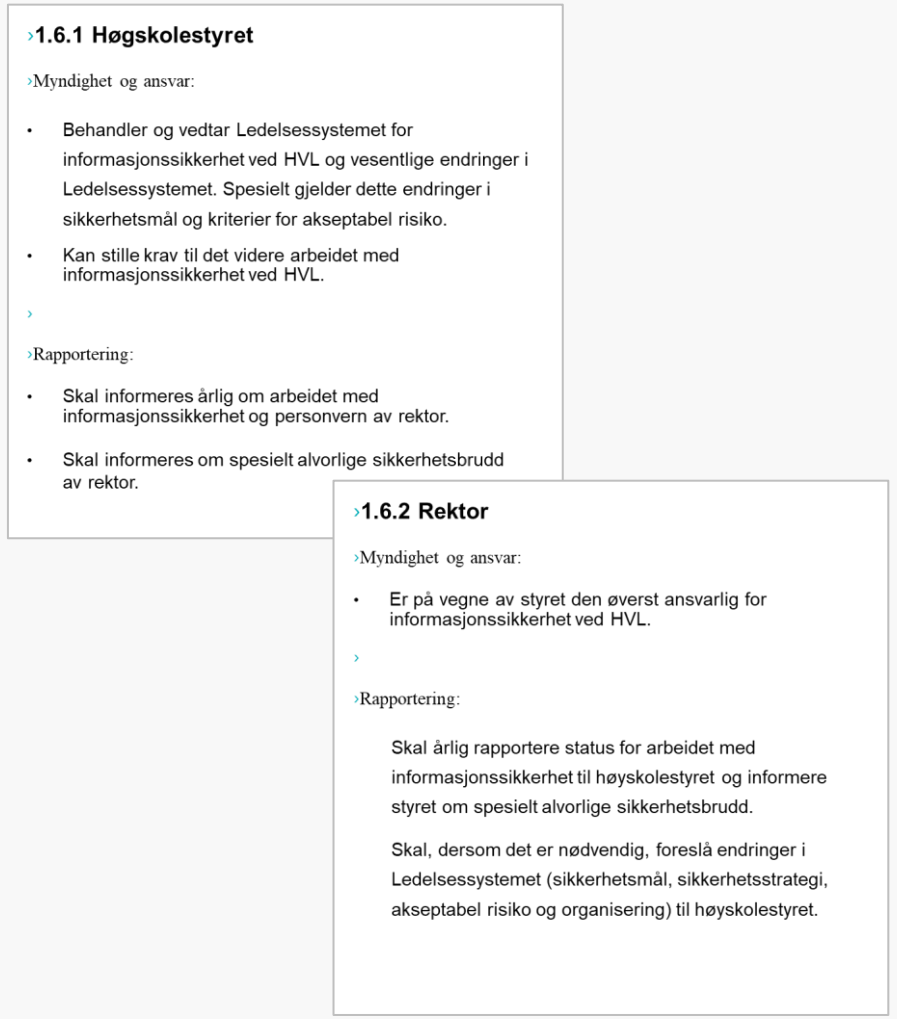
a) Virksomheten innfører, vedlikeholder og forbedrer et ledelsessystem for informasjonssikkerhet tilpasset virksomhetens størrelse og behov. Ledelsessystemet bør basere seg på anerkjente internasjonale standarder, for eksempel ISO/IEC 27001.

…

f) Virksomhetens øverste ledelse sørger for periodisk revisjon av arbeidet med informasjonssikkerhet og oppdatering av ledelsessystemet (ved behov).

g) Virksomhetens øverste styrende organ fører kontroll med arbeidet med informasjonssikkerhet.

Dette kjem vi tilbake til mot slutten når vi ser på planar for 2026



1.6.1 Høgskolestyret

Myndighet og ansvar:

- Behandler og vedtar Ledelsessystemet for informasjonssikkerhet ved HVL og vesentlige endringer i Ledelsessystemet. Spesielt gjelder dette endringer i sikkerhetsmål og kriterier for akseptabel risiko.
- Kan stille krav til det videre arbeidet med informasjonssikkerhet ved HVL.

Rapportering:

- Skal informeres årlig om arbeidet med informasjonssikkerhet og personvern av rektor.
- Skal informeres om spesielt alvorlige sikkerhetsbrudd av rektor.

1.6.2 Rektor

Myndighet og ansvar:

- Er på vegne av styret den øverst ansvarlig for informasjonssikkerhet ved HVL.

Rapportering:

Skal årlig rapportere status for arbeidet med informasjonssikkerhet til høyskolestyret og informere styret om spesielt alvorlige sikkerhetsbrudd.

Skal, dersom det er nødvendig, foreslå endringer i Ledelsessystemet (sikkerhetsmål, sikkerhetsstrategi, akseptabel risiko og organisering) til høyskolestyret.

Trusselbiletet: Vanlegvis gjerne tre viktigaste punkt. I år berre eit…

- **KI / AI:**
  Kva er KI?
  Spørsmålet i dag er snart: kva er ikkje KI?

- «deep fake» og svindel er sjølsagt farlig, men uvettig intern bruk av kraftig KI har eit større skadepotensial (jfr. rapport frå Personvernombodet).

  HVL gjer grundig og rett arbeid med å innføra KI i form av chat-løysing til bruk både i undervising, forsking og administrasjon.

  Samstundes kjem IT verktøy vi kjenner og nyttar av gammal vane – med ulike former KI-støtte.
  KI får då same tilgangar som du har til data.

- For at ikkje noko skal gå under radaren er det viktig at vi har eit fungerande og godt implementert *ledelsessystem for informasjonssikkerheit* å falla tilbake på…

Bilde: Copilot chat

Avvik og hendingar

Fire saker melde til Datatilsynet (DT) i 2025

- To saker menneskelig svikt / rutinebrudd ifm hhv praksis og masteroppgåve
- To saker av IT-teknisk karakter:
  - Studentar og tilsette kan knyta tredjeparts applikasjonar / tenester til sin Microsoft 365-brukerkonti. Applikasjonene kan få tilgang til brukarane sine data.
    HVL har – som UiO og flere andre – ikkje hatt gode nok rutiner for godkjenning av slike tredjepartstenester
  - Problem med tilgang i *Studentweb* og *Søknadsweb*. Brukarar kunne sjå andre sine brukarsider

Begge saker er avslutta av DT utan særskilde pålegg

IT-hjelp har og i år handtert fleire mindre alvorlege saker

- Færre svindelforsøk vert melde frå brukarane.
  Dei er meir merksame og fleire vert stoppa automatisk

Område som derimot vekkjer stor bekymring er

- Tilsette, stipendiatar og studentar sin IT bruk frå land der vi veit at digital infrastruktur kan bli misbrukt av myndigheier eller kriminelle
- Det går for sint med **verdivurdering** og **klassifisering** som grunnlag for høveleg sikring eller publisering av data.
  Kontroll med HVL sine data er føresetnad for trygg IT-bruk

Apper kan ha hatt uautorisert tilgang til personopplysninger i ti år

Uautorisert tilgang til e-post og filer har pågått i over ti år ved Universitetet i Oslo. Rundt 17.000 brukere kan være berørt.

Studenter og ansatte har kunnet bruke eksterne applikasjoner

avviksmelding i Datatilsynet. Foto: Eva Tønnessen

PST: «Sannsynlig» at Sandbergs sikkerhetsbrudd er blitt misbrukt av Kina og Iran

Her er statsminister Erna Solbergs svar på ti spørsmål fra kontroll- og konstitusjonskomiteen om Per Sandbergs mobilbruk i Iran og Kina.

PST sier at en norsk statsråd er «høyverdig etterretningsmål», og at Per Sandbergs sikkerhetsbrudd sannsynligvis har gitt fremmede makter informasjon de ikke skulle hatt. *Foto: Stein Bjørge*

Bilder: Khrono og Aftenposten

Utførte tiltak

- To samøvingar i regi av Sikt eduCSC (Cybersikkerhetssenter for forskning og utdanning)
  - april «øvelse mayday»
  - oktober «øvelse nullpunkt»
- Oppgradert bruk av virtuelt private nett (vpn)
- SILAF – Sikker lagring av forskingsdata
  - sikkerheitstesta i 2024 - sårbar i 2026
  - stengde tenesta i tre arbeidsdagar og ei helg for å retta alvorlege feil som gjorde at forskingsdata kunne kome på avveg (avvik meldt DT).

Planar for 2026

- Ny organisering av IT-eininga 01.01.26
  - to einingsleiarar rekruttert eksternt, to internt.
  - godt og modernisert utgangspunkt for ei utfordrande framtid

- Omforma ledelsessystemet frå
  - eit dokument basert på ISO/IEC27001:2013

    til

  - «system» basert på ISO/IEC27001:2022 for for heile HVL