

Gjennomgang av sentrale tilbakemeldinger fra høringsrunden

Det juridiske fakultet

Tilbakemelding	Oppfølging fra arbeidsgruppen
Det bør fremgå hvordan opplæring i informasjonssikkerhet skal gjennomføres (analogt og/eller digitalt), hvordan gjennomføringen skal registreres, når den må være gjennomført og hvilke konsekvenser unnlatelser vil ha.	Vi er enige i at det er viktig at dette fastsettes og formidles. Imidlertid har vi vurdert det slik at dette ikke tas inn i selve strategien, men må utarbeides i forbindelse med oppfølgingen og iverksettelse av strategien.
Tilbakemeldinger på strategiens angivelse av <i>akseptabel risiko</i> . Disse går på primært forholdet mellom beskrivelsene i de ulike kategoriene (utdanning, FoU, formidling og administrasjon), nivået for risikoaksept og begrepsbruk i de ulike tabellene.	Vi har omarbeidet denne delen av strategien, og har lagt til mer utdypende informasjon innledningsvis. Videre har vi tatt ut to figurer (nr. 9 og 10) som var med i hoveddokumentet i høringsrunden. Nå fremkommer disse kun av underlagsmaterialet (s. 33 og 34 i vedlegg to i denne sak). Vi ser at å presentere dem «løsrevet» fra øvrig materialet, slik dokumentet var da det ble sendt på høring, kan medføre at avveiningene blir vanskelig tilgjengelig. Videre har vi tatt inn en oppfordring om at informasjonssikkerhetsrådgiver skal involveres første gang enhetene foretar vurderinger mtp akseptabel risiko.
Underlagsmaterialet, s. 13, «administrasjon». Formidling bør med i første setning.	Dette er ordnet.
Forslag om å ta inn henvisninger i hoveddokumentet om hvor man kan finne mer informasjon i underlagsmaterialet.	Dette innspillet ble diskutert, og vi endte med å ikke ta inn konkrete henvisninger da det er viktig at hoveddokumentet kan stå selvstendig. Vi har istedenfor foretatt noen omformuleringer og omstruktureringer i den delen hvor vi oppfattet at behovet for mer informasjon var størst (delen om «akseptabel risiko»). Det var også her risikoen for misforståelser var størst.
Forslag om at begrepslisten utvides slik at «metrikker» forklares.	Vi har byttet ut «metrikker» med et annet begrep («måleparameter»).

Studentparlamentet

Tilbakemelding	Oppfølging fra arbeidsgruppen
<p>Kommentar knyttet til visjonen, og om hvorfor den er rettet mot at samfunnets tillit skal ivaretas – fremfor fokus på at ingen informasjon skal komme på avveie.</p>	<p>Ved å ivareta informasjonssikkerheten vil samfunnets tillit ivaretas, så dette er bakgrunnen for at visjonen er formulert slik. Informasjonssikkerhet er ikke et mål i seg selv, men en forutsetning for å andre mål (ivaretagelse av tillit, personvern, gjennomføre forskningsprosjekter, undervisning mv).</p>
<p>Spørsmål rundt målbildet «overvåking og hendelsesstyring», især punktet om «kontinuerlig overvåking av tjenester, systemer og IKT-infrastruktur» og hvordan dette stiller seg mtp ivaretagelse av personvern.</p>	<p>For å ivareta informasjonssikkerheten er kontroll med tjenester, systemer og infrastruktur en forutsetning. En av kjernetiltakene her er logging. Formålet er ikke å overvåke enkeltpersoner, og bruk av logger må være strengt regulert ved UiT. Det må også være åpenhet rundt hva som logges og hva disse brukes til. Logging gjøres bl.a. for å hindre misbruk, rette feil, avdekke inntrengere og hindre at f.eks personopplysninger havner hos uvedkommende og misbrukes. Logging skal aldri gjøres uten en legitim hensikt, men for lite logging er en direkte trussel mot UiTs mulighet for å ivareta informasjonssikkerheten.</p> <p>God og hensiktsmessig logging er en forutsetning for ivaretagelsen av ansatte og studenters personvern.</p>
<p>Kommentar rundt rollefordeling og ansvar, og at prosessene innenfor informasjonssikkerhet gjennomføres på en effektiv måte</p>	<p>Strategien beskriver i liten grad de rollene og den ansvarsfordeling som eksisterer innenfor informasjonssikkerhetsarbeidet ved UiT. Dette reguleres av kap. 3 i styringssystemet for informasjonssikkerhet. Men vi ser at det er en del spørsmål rundt dette, og har derfor tatt inn en oversikt i strategien (s. 12 i hoveddokumentet) som klargjør noen sentrale punkter rundt ansvarsfordelingen.</p> <p>Vi ser et klart behov for at kompetansen innenfor informasjonssikkerhet økes ute på enhetene slik at prosesser kjøres mer smidig og effektivt.</p>
<p>Informasjon til studenter om informasjonssikkerhet, og om strategien bør nevne eksplisitt hvem som har ansvaret for dette</p>	<p>Det er helt sentralt at også studentene får opplæring i informasjonssikkerhet. Vi har vurdert dette likt som for tilbakemeldingen fra Det juridiske fakultet vedrørende opplæring; at regulering av dette må fastsettes gjennom arbeidet med oppfølgingen av strategien.</p>

Avdeling for forskning, utdanning og formidling

Tilbakemelding	Oppfølging fra arbeidsgruppen
Vanskelig å vurdere om og hvordan kriteriene som fremgår under akseptabel risiko vil fungere i det praktiske informasjonssikkerhetsarbeidet. Også usikre på om noen formuleringer er for snevre.	Vi har gjort større endringer i delen om akseptabel risiko, ref. kommentar ovenfor ifbm kommentarene fra JurFak. Økt fokus på at det må gis veiledning før disse anvendes første gang av en enhet.
Figur 10, burde understrekes at det gjelder <i>utilsikt</i> et tap av data.	Vi har tatt dette inn for å unngå misforståelser. Figuren det siktes til er også tatt ut av hoveddokumentet, og fremkommer nå kun i underlagsdokumentet (ref. kommentar ovenfor om akseptabel risiko)