UiT
NORGES
ARKTISKE
UNIVERSITET

RETNINGSLINJE for UiTs kontrollaktiviteter innenfor informasjonssikkerhet og personvern

Fastsatt av:	IT-direktør	Dato:	30.6.2022
Ansvarlig enhet:	Avdeling for IT	Id:	
Sist endret av:		Dato:	
Erstatter:		Arkivref.:	2017/5560-23

1.Formål
Formålet med kontrollaktiviteter er å kunne vurdere i hvilken grad de etablerte tiltakene er tilstrekkelige og effektive for å sikre etterlevelse av relevant regelverk, overordnede føringer og interne retningslinjer. Gjennom kontrollerende aktiviteter vil det kunne avdekkes forbedringsområder knyttet til eksisterende tiltak og identifiseres eventuelle ytterligere tiltak som bør iverksettes.

2. Virkeområde
Retningslinjen er gitt med hjemmel i Ledelsessystem for informasjonssikkerhet og personvern («ISMS») kapittel 7: «*Internkontroll og -revisjon*». Retningslinjen vil gjelde for alle enheter ved UiT.

3. Ansvar, myndighet og oppgavefordeling
IT-direktør fastsetter denne retningslinjen, samt tilhørende rutiner som omfatter hele UiT.

Enhetsleder (avdelingsdirektør, dekan, direktør for UB, UMAK) fastsetter eventuelle rutiner for gjennomføring av kontrollaktiviteter på egen enhet. Dette kan delegeres til f.eks fakultetsdirektør eller instituttleder. Enhetsleder eller den som dette delegeres til kan beslutte gjennomføring av kontrollaktiviteter på egen enhet.

Faggruppe for informasjonssikkerhet og personvern (FPI) kan beslutte at kontrollaktiviteter skal gjennomføres på enhetene og/eller på tvers av enhetene.

4. Definisjoner og forkortelser

ISMS - Ledelsessystem for informasjonssikkerhet og personvern (uit.no/sikkerhet).
GDPR – Personvernforordningen (EU 2016/679)
FPI – Faggruppe for informasjonssikkerhet og personvern

5. Beskrivelse

Personvern og informasjonssikkerhet blir ofte omtalt som om det er det samme, uten at det alltid er tilfelle.

Informasjonssikkerhet er å sikre at informasjonen i alle former

- Ikke blir kjent for uvedkommende (**konfidensialitet**)
- Ikke blir endret utilsiktet eller av uvedkommende (**integritet**)
- Er tilgjengelig ved legitimt behov (**tilgjengelighet**)

Konfidensialitet, integritet og tilgjengelighet er like viktige og det er ingen rangering mellom dem. Informasjonssikkerhet er også sentralt for å ivareta forpliktelsene etter personvernforordningen (GDPR). Informasjonssikkerhet er imidlertid ikke begrenset til personopplysninger, men skal ivaretas for alle UiTs informasjonsverdier.

Tilsvarende gjelder også motsatt. Det er langt mer til ivaretagelsen av personvernet enn informasjonssikkerhet. Eksempelvis må en etter GDPR ha et lovlig grunnlag for å behandle opplysningene og det er særskilte vurderinger knyttet til gjenbruk av opplysninger. Dette er ikke en direkte del av informasjonssikkerheten, men er forpliktelser UiT er underlagt etter lovverket for ivaretagelse av personvernet.

Kontrollaktivitet vil kunne omfatte bare informasjonssikkerhet, bare personvern eller begge områdene.

Det fremgår av ledelsessystemet at UiTs kontrollaktiviteter innenfor informasjonssikkerhet og personvern skal bestå av både faste aktiviteter som gjennomføres jevnlig, samt aktiviteter som gjennomføres ved behov.

Faste kontrollaktiviteter

- *Statusrapporten:* UiT har etablert en fast årlig rapportering der enhetene rapporterer status på informasjonssikkerhets- og personvernområdet som sendes til faggruppen for informasjonssikkerhet og personvern.

  Rapporteringen bidrar til at fakultetene får bedre oversikt og kontroll over sine informasjonsverdier, verdiens sikkerhetsbehov og tilhørende risiko. For at enhetene skal kunne rapportere krever det gjennomføring av egenkontroller, eksempelvis gjelder dette gjennomførte risikovurderinger.

  Rapporteringen inngår i grunnlaget for årsrapporten for informasjonssikkerhet og personvern, som behandles av Universitetsstyret første kvartal.

- *Ledelsens gjennomgang:* Gjennom årsrapporten til Universitetsstyret gjennomføres også ledelsens gjennomgang, jf. ledelsessystemet kap. 9.

Kontrollaktiviteter som gjennomføres ved behov
I tillegg til de faste kontrollaktivitetene som nevnt over skal det gjennomføres aktiviteter ved behov. Denne typen egenkontroll kan gjennomføres enten som stedlig kontroll og/eller som en skriftlig kontroll.

Stedlige kontroller kan være eksempelvis være gjennomgang av IT-systemer, arbeidsmåter og tiltak fra tidligere ROS-analyser, samt oppfølging av eventuelle utfordringer avdekket i den årlige statusrapporten.

Skriftlig kontroll gjennomføres gjerne for å kontrollere et spesifikt område ved behov. Det er obligatorisk å svare på spørsmålene i en brevlig kontroll innen fristen gitt. Eksempel på skriftlig kontroll:

- kontroll av at tildelte aktive tilganger til systemer er korrekt på de enkelte enheter og hvilke rutiner enheter har for å følge opp dette.
- kontroll med hvor mange forskningsprosjekter enheten har og hvor mange av de som er risikovurdert.
- Innhold i protokoll over behandlingsaktiviteter er dekkende og oppdatert samt gjennomførte kontroller av leverandører/databehandlere.
- At forskningsprosjekt er gjennomført i tråd med informasjon innsendt til Sikt

Listen er ikke uttømmende, og tema for kontrollaktiviteter vil endre seg etter hvilke behov som er gjeldende.

Denne type egenkontroll bør gjennomføres av enhetene minst en gang hvert år. Enhetene bør utforme en årlig plan for gjennomføring av nødvendige kontrolltiltak. I utgangspunktet beslutter enheten selv hvilken type kontroll som skal gjennomføres, men i tillegg kan FPI beslutte at en særskilt type kontroll skal gjennomføres av en eller flere enheter ett gitt år.

Funn fra egenkontroll skal sammenfattes i en rapport. Rapporten bør være kortfattet, og punktbasert. Det skal skilles mellom konstaterte avvik og anbefalinger. Avvik og anbefalinger skal nummereres i rapporten for å lette oppfølgingen etter kontrollen. Kopi av rapporten skal sendes til FPI fortløpende.

6. Referanser

GDPR – Personvernforordningen

Ledelsessystem for informasjonssikkerhet og personvern, kap. 7