Veikart for informasjonssikkerhet og personvern 2023

Virketid for dette veikartet vil være februar 2023 til januar 2024. Rapportering på tiltakene vil tas gjennom årsrapport for informasjonssikkerhet og personvern, og i samme sak for Universitetsstyret vil neste års veikart behandles.

I dette veikartet vil NSMs grunnprinsipper for sikkerhetsstyring være relevant å se hen til med tanke på struktur. NSM deler prinsippene opp i fire hovedkategorier, og også NSMs øvrige grunnprinsipper (IKT-sikkerhet, personellsikkerhet og fysisk sikring) følger denne inndelingen.

Disse kategoriene er:

1. Identifisere og kartlegge
2. Beskytte og opprettholde
3. Oppdage
4. Håndtere og gjenopprette

Disse kategoriene kan brukes til å synliggjøre sammenhengen mellom de ulike tiltakene, og hvilken type tiltak det er, og kan være nyttige selv om de benyttes i en mer utvidet kontekst enn hva NSM selv gjør.

Merk at for IKT-sikkerhetstiltak vil en helhetlig oversikt bli svært detaljert og omfattende. Både av hensyn til helheten samt hva som er viktig og hensiktsmessig å forankre i styret er kun de større og mest sentrale tiltakene innenfor IKT-sikkerhet tatt med. Med utgangspunkt i dette lages det mer detaljerte handlingsplaner i Avdeling for IT.

Det er å forvente at målbilde A vil ha en overvekt av tiltakene, både grunnet det ovennevnte om hva som er hensiktsmessig å forankre i styret, men også fordi dette måbildet har tatt opp i seg ett av de øvrige målbildene i den forrige strategien og slikt sett er utvidet.

A. Helhetlig og effektiv styring innenfor sikkerhet og personvern

Delmål	Tiltak 2023	Kategori tiltak 2023	Ansvarlig tiltak 2023
Helhetlig ledelsessystem for sikkerhet, beredskap og personvern	Dagens ledelsessystem for informasjonssikkerhet og personvern bygges ut til å omfatte samfunnssikkerhet og beredskap. Det utvidede ledelsessystemet skal også oppfylle kravene til styringssystem for sikkerhet etter sikkerhetsloven.	Identifisere og kartlegge Beskytte og opprettholde	ITA i samarbeid med ORGØK
Helhetlig håndtering av adgangs- og tilgangskontroll. *Felles forståelse og sikre et overordnet regelverk for adgangskontroll (fysisk sikring) og tilgangskontroll (IT-tjenester/-systemer)*	Gjennomgang/kartlegging av adgangskontroll. Identifisere behovet for nye og/eller reviderte reglement, retningslinjer og rutiner.	Identifisere og kartlegge	BEA
Prosesser, prosjekter og beslutninger skal ha et risikobasert beslutningsgrunnlag, og UiT skal være i stand til å se risikoer i sammenheng	Anskaffe verktøy for risikovurdering innen informasjonssikkerhet	Identifisere og kartlegge	ITA
IT-tjenester og systemer skal ivareta personvernet til UiTs ansatte, studenter, forskningsdeltakere, samarbeidspartnere og gjester	Personvernkonsekvensanalyse (DPIA) av den påvirkning av UiTs IKT-sikkerhetsmekanismer har på ansatte, og om tilstrekkelig risikoreduserende tiltak er iverksatt	Identifisere og kartlegge	ITA
Porteføljestyring, forvaltning og drift av IKT-tjenester og -systemer ved UiT skal være helhetlig	Etablere helhetlig kvalitetssystem for IKT-drift ved UiT, ved å utvide og påbegynne tilpasningen av dagens kvalitetssystem for Avdeling for IT til å gjelde all IKT-drift uavhengig av hvilken enhet som eier og drifter systemet/tjenesten	Identifisere og kartlegge Beskytte og opprettholde	ITA
Fungerende og oppdatert protokoll over	Etablere kontaktpersoner pr enhet som har et	Identifisere og kartlegge	ITA

behandlingsaktiviteter	særskilt ansvar for protokollen for den enheten, og kan kvalitetssikre og holde eksisterende protokoll ajourført.		
UiT skal ivareta sine forpliktelser etter eksportkontrollregelverket	Etablere nødvendige retningslinjer og rutiner for identifisering av teknologi, varer og kunnskap ved UiT som omfattes av eksportkontroll	Identifisere og kartlegge	FUF
	Etablere fungerende kontrollfunksjon for at retningslinjer og rutiner for eksportkontroll følges og fungerer.	Oppdage	FUF
UiT skal gi god informasjon om hvordan personopplysninger behandles	Identifisere og utbedre mangelfulle eller manglende personvernerklæringer	Identifisere og kartlegge	ITA i samarbeid med ORGØK, FUF og BEA
UiT skal ha en robust og moderne sikkerhetsarkitektur, tilpasset et skiftende trussel- og risikobilde	Gjennomgå og revidere prinsipper for sikkerhetsarkitekturen	Alle fire kategorier	ITA
UiT skal ha kontroll med sikkerheten hos sine leverandører	Etablere retningslinjer og rutine for leverandøroppfølging	Beskytte og opprettholde	ITA
UiT skal følge NSMs grunnprinsipper for IKT-sikkerhet	Utarbeide manglende retningslinjer innenfor IKT-drift og -forvaltning	Alle fire kategorier	

B. Overvåkning og hendelsesstyring

Delmål	Tiltak 2023	Kategori tiltak 2023	Ansvarlig tiltak 2023
UiT skal være i stand til å oppdage og håndtere IKT-hendelser på en robust og forsvarlig måte	Styrke operativ IKT-sikkerhet, især CSIRT-teamet.	Oppdage Håndtere og gjenopprette	ITA
	Styrke monitoreringen av aktivitet i UiTs IKT-tjenester og -systemer slik at uønskede eller mistenkelige hendelser oppdages tidlig	Oppdage	ITA
UiT skal kunne gjenoppta normal drift også i tilfelle en katastrofehendelse	Identifisere og prioritere hvilke systemer og verdier som skal kunne gjenopprettes etter en katastrofal hendelse	Identifisere og kartlegge	ITA
	Etablert plan og teknisk støtte for katastrofegjenopprettelse (disaster recovery)	Håndtere og gjenopprette	ITA
UiT skal ha samarbeid både i og utenfor sektoren for håndtering av sikkerhetshendelser	Videreutvikle samarbeidet med Sikt Cybersikkerhetssenter (eduCSC), BOTT digital sikkerhet.	Oppdage Håndtere og gjenopprette	ITA
	Etablere samarbeid med kommersielt sikkerhetsselskap for rådgivning, sårbarhetsindikatorer og bistand ved større hendelser.	Oppdage. Håndtere og gjenopprette	ITA
UiT skal følge NSMs grunnprinsipper for IKT-sikkerhet	Utarbeide manglende retningslinjer innenfor IKT-drift og -forvaltning	Alle fire kategorier	ITA

C. Ansvarsbevisst kultur

Delmål	Tiltak 2023	Kategori tiltak 2023	Ansvarlig tiltak 2023
Ansatte og studenter skal være kjent med hvilke IT-tjenester som kan brukes til hvilke typer data	Styrke bevisstheten om krav til «integritet» og «tilgjengelighet» ved å lage tilsvarende godkjenningstabell for IT-tjenester som i dag finnes for «konfidensialitet».	Beskytte og opprettholde	ITA i samarbeid med FUF og ORGØK
Ansatte og studenter skal ha tilstrekkelig kompetanse innenfor informasjonssikkerhet og personvern	Gjennomføre sikkerhetskulturundersøkelse	Identifisere og kartlegge	ITA
	Følge opp enhetenes gjennomføring av styrets vedtak i 2022 om å inkludere informasjonssikkerhet og personvern i all relevant internopplæring	Beskytte og opprettholde	ITA i samarbeid med ORGØK og FUF
	Etablere målrettet opplærings- og bevisstgjøringsprogram innenfor grunnleggende informasjonssikkerhet	Beskytte og opprettholde	ITA i samarbeid med ORGØK og FUF