Politikk for informasjonssikkerhet og personvern ved UiS

Formål

Formålet med Politikk for informasjonssikkerhet og personvern er å ivareta de informasjonsverdier som utvikles, behandles og forvaltes gjennom UiS' forskning, utdanning, herunder kunstnerisk utviklingsarbeid, formidling, nyskaping og administrasjon, og overholdelse av gjeldende lover og regler. Politikk for informasjonssikkerhet og personvern stadfester mål og strategi for informasjonssikkerhet og personvern i virksomheten, og setter rammer for arbeidet med ivaretakelse av UiS' informasjonsverdier og for den digitale sikkerheten i UiS' IKT-infrastruktur.

Denne Politikken gjelder for

- Alle ansatte og studenter ved UiS
- Alle som har tilgang til, bearbeider og/eller forvalter informasjonsverdier på vegne av UiS, uavhengig av lagrings- og prosesseringsform.
- Informasjonsverdier lagret på UiS' utstyr, på utstyr tilkoblet UiS' IKT-infrastruktur, på privat utstyr tilkoblet UiS-infrastruktur, eller på eksterne tjenester forvaltet av UiS.

Målsettinger og strategi

Det overordnede målet er at UiS skal etterleve virksomhetens føringer for informasjonssikkerhet og personvern, inkludert følgende målsettinger:

- UiS skal etterleve lover og regler for innsamling, oppbevaring og sikring av data og personvern.
- UiS skal ivareta personvernet ved å ha fokus på den registrertes rettigheter og friheter, samt informasjonssikkerheten.
- Beskytte UiS sin informasjon og informasjonssystemer mot tyveri, misbruk, forringet kvalitet og andre former for skade og tap.
- Sørge for at alle som er omfattet av denne Politikken følger etablerte rutiner for ivaretagelse av sikkerhet og personvern, slik at frekvens og skadenivå av hendelser minimeres.
- Hendelser, avvik eller brudd på informasjonssikkerheten og personvernet, skal være kartlagt, dokumentert og varslet.
- Det skal utarbeides og gjennomføres rollebasert opplæring i henhold til roller i UiS reglement for informasjonssikkerhet og personvern.
- Krav til informasjonssikkerhet og personvern skal ivaretas i design, anskaffelse, utvikling, forvaltning og avhending av IKT-systemer og infrastruktur.

For å nå målsetningene, skal det være etablert et ledelsessystem for informasjonssikkerhet og personvern. Ledelsessystemet skal gi rammene for en systematisk og helhetlig praksis mellom styrende, gjennomførende og kontrollerende del av arbeidet med informasjonssikkerhet. Ledelsessystemet skal følge metoder fra ISO 9001 (kvalitet) og ISO 27001 / ISO 27014. Det skal inneholde rutiner for internkontroll, personvern, risikostyring, IT-sikkerhet, avvikshåndtering, varsling og vedlikehold av informasjonsverdier. Dette vedlikeholdes og følges opp som angitt i årshjulet.

Konsekvenser / sanksjoner

Overtredelse av denne Politikk for informasjonssikkerhet og personvern, og vedtatte sikkerhetskrav vil håndteres på ordinær måte i ledelseslinjen.

Appendix A: Oppgaver

Styret

- Har det øverste ansvaret for risikoen som knytter seg til virksomhetens informasjonsverdier, og er ansvarlig for at sikkerheten er tilpasset denne risikoen.
- Har det overordnede ansvaret for personvernet ved all behandling av personopplysninger ved UiS.
- Skal fastsett sikkerhetsmål og kriterier for akseptabel risiko for UiS' informasjonsverdier
- Skal fastsette krav til arbeid med informasjonssikkerhet og personvern ved UiS
- Skal sette virksomheten i stand til å håndtere risikoen slik at denne er på et nivå som styret aksepterer.

Rektor

- Skal årlig rapportere status for arbeidet med informasjonssikkerhet og personvern til universitetsstyret
- Skal løpende informere styret om spesielt alvorlige sikkerhetsbrudd.

Appendix B: Definisjoner

IKT-infrastruktur: Med UiS IKT-infrastruktur menes alt utstyr, digital informasjon, informasjonssystemer og tjenester som benyttes til informasjonsbehandling og kommunikasjon.

Informasjonssikkerhet: Informasjonssikkerhet handler om å sikre informasjon, ut ifra krav om konfidensialitet, integritet, tilgjengelighet og robusthet.

Informasjonsverdier: Deles inn i to kategorier:
Primærverdier handler om hva vi gjør og hvordan, og informasjonen vi benytter:

- forretningsprosesser og aktiviteter
- informasjon

Sekundærverdier handler om de verktøyene vi bruker og kompetansen hos de som bruker verktøyene:

- hardware
- software
- nettverk
- ansatte
- lokasjoner
- organisasjonsstrukturer

Integritet: Integritet betyr å sikre at informasjon er korrekt, gyldig og fullstendig og ikke kan endres utilsiktet eller av uvedkommende.

Internkontroll: Systematiske styrings- og kontrolltiltak som skal sikre at institusjonens aktiviteter planlegges, organiseres, utføres, sikres og vedlikeholdes i samsvar med krav fastsatt i eller i medhold av lov, og styrende dokumenter.

Konfidensialitet: Konfidensialitet betyr å sikre at informasjonen ikke blir kjent for uvedkommende, men at informasjon og informasjonssystemer bare er tilgjengelig for de som har et tjenstlig behov.

Ledelsessystem: Ledelsessystemet for informasjonssikkerhet og personvern ved UiS følger ISO 27001-standarden og deler fra ISO 9001-standarden, og angir et systematisk arbeid ut fra et sett med styrende dokumenter og prosessbeskrivelser med angitte roller og ansvarsforhold, en aktiv internkontroll og forbedringssløyfer. I praksis fungerer ledelsessystemet i en tredeling mellom styrende del (ledelseselementet), gjennomførende del (linjen, herunder brukere og prosesseiere) og av kontrollerende del (løpende internkontroll, intern- og ekstern revisjon).

Robusthet: Robusthet betyr organisasjonen og systemers evne til å gjenopprette normaltilstand

Vedtatt av universitetsstyret 24.09.2019