

**Sak 67/24 Ledelsessystem for internkontroll av informasjonssikkerhet
og personvern ved NIH**

NIHs system for internkontroll av informasjonssikkerhet og personvern ble godkjent av styret i sak 111/19 Revidering av system for informasjonssikkerhet og personvern.

Riksrevisjonen påpekte etter sin gjennomgang av arbeidet med informasjonssikkerhet og personvern i forskning ved NIH i 2023, at institusjonens ledelsessystem for informasjonssikkerhet og personvern ikke var oppdatert med hensyn på organisasjonsstruktur. Kravene i ledelsessystemet var heller ikke tilstrekkelig operasjonalisert, ref. sak 42/24 Rapport om personvern og informasjonssikkerhet ved NIH for 2023.

Tilsvarende anbefalinger om oppdatering av ledelsessystemet har kommet fra HK-dir og fra Personvernombudet.

Vedlagt følger oppdatert ledelsessystem med presisering av ansvar og oppgaver hos de ulike aktørene.

Ledelsessystem for informasjonssikkerhet og personvern inngår i institusjonens overordnede Sikkerhetssystem, som er under utarbeidelse.

Forslag til vedtak:

Styret vedtar ledelsessystem for informasjonssikkerhet og personvern ved NIH.

Vedlegg:

1. Ledelsessystem

Ledelsessystem for informasjonssikkerhet og personvern ved NIH

Innholdsfortegnelse:

Ledelsessystem for informasjonssikkerhet og personvern ved NIH.....	1
1. Innledning.....	1
2. Regelverk.....	4
3. Sikkerhetsmål og sikkerhetsstrategi	6
4. Roller, ansvar og oppgaver	9
5. Klassifisering av informasjon	16
6. Risiko- og sårbarhetsanalyser	17
7. Opplæring	17
8. Håndtering av hendelser og avvik	18
9. Internkontroll og sikkerhetsrevisjon	20
10. Ledelsens gjennomgang	21

1. Innledning

Bakgrunn, formål og hensikt

Norges idrettshøgskole (NIH) er en vitenskapelig høgskole. Vårt samfunnsoppdrag er å drive høyere utdanning, forskning og formidling innen et bredt teoretisk og aktivitetsrettet idrettsvitenskapelig område.

NIH forvalter store mengder personopplysninger og annen type informasjon, inkludert sensitiv informasjon, i administrasjon, forskning, undervisning og formidling.

Forvaltningen av denne informasjonen skal bidra til at virksomhetens arbeid utføres effektivt og med høy kvalitet innenfor sikre omgivelser og i tråd med lov og regelverk.

NIH har valgt rektor og ansatt administrere direktør («delt ledelse»). Forsknings- og undervisningsvirksomheten ved NIH er organisert i fire institutt, ledet av hver sin instituttleder. I tillegg kommer to eksternt finansierte forskningssentre, organisatorisk tilknyttet hvert sitt institutt.

Den teknisk-administrative virksomheten er organisert i seks avdelinger, med hver sin avdelingsleder.

Informasjonssikkerhet

Informasjonssikkerhet innebærer *sikring av informasjon og informasjonsverdier*, uavhengig av om den er lagret digitalt eller ikke. Med informasjonsverdier menes alle typer data, opplysninger og dataressurser (IT-utstyr, applikasjoner, systemer, datanettverk, osv.) som har betydning for høgskolens virksomhet, for samarbeidspartneres virksomhet eller for samfunnets sikkerhet. IT-sikkerhet har med sikring av Informasjons- og kommunikasjonsteknologi å gjøre – altså maskinvare og programvare. Grunnen til at IT-sikkerhet og informasjonssikkerhet ofte blir brukt om hverandre, er at mye informasjon er lagret og formidlet ved hjelp av IT. For å beskytte slik informasjon, må man beskytte teknologien den er lagret og formidlet på.

Et systematisk og planmessig arbeid for å sikre våre informasjonsverdier er en sentral del av vår kunnskapsforvaltning. Både interne og eksterne aktører – ledere, ansatte, studenter, samarbeidspartnere og offentligheten – skal kunne stole på at NIH sikrer informasjon i alle former:

- Blir ikke kjent for uvedkommende (konfidensialitet)
- Blir ikke endret utilsiktet eller av uvedkommende (integritet)
- Er tilgjengelig ved legitimt behov (tilgjengelighet)

NIH er underlagt lover og forskrifter (se kapittel 2) som pålegger oss å ha en tilfredsstillende informasjonssikkerhet. Ledelsessystemet for informasjonssikkerhet og personvern ved NIH skal ivareta de kravene som lovverket og Kunnskapsdepartementet (KD) stiller til arbeidet med informasjonssikkerhet i universitets- og høgskolesektoren gjennom "[Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning.](#)"

Personvern

Det å sørge for at behandling av personopplysninger er i henhold til personopplysningsloven, GDPR samt annet relevant lovverk, er en sentral del av forpliktelsene til Norges idrettshøgskole. Dette innebærer mer enn å sikre at informasjonssikkerheten ivaretas. NIH må til enhver tid sørge for overholdelsen av regelverket ved behandling av personopplysninger, slik som lovlig grunnlag for behandling av personopplysninger, god og korrekt informasjon om behandlingene, ivaretagelsen av de registrertes rettigheter mv.

Et systematisk og planmessig arbeid for å sikre at disse forpliktelsene overholdes i alle ledd av organisasjonen er derfor sentralt for å ivareta rettighetene og personvernet til personer vi behandler opplysninger om.

Ledelsessystemet for informasjonssikkerhet og personvern ved Norges idrettshøgskole

Ledelsessystem for informasjonssikkerhet og personvern (“Ledelsessystemet”) skal sørge for at NIH sine informasjonsverdier håndteres på en systematisk, planmessig og tilfredsstillende måte. Ledelsessystemet inneholder blant annet mål, strategi og organisering av arbeidet med informasjonssikkerhet og personvern, samt beskrivelse av roller og ansvar, oversikt over informasjonsverdier, retningslinjer og relevante maler.

Ledelsessystemet består av følgende hovedelementer:

1. Styrende del – overordnede lover, forskrifter og retningslinjer for arbeidet med informasjonssikkerhet ved NIH, herunder virkeområde, sikkerhetsmål - og strategi, kriterier for akseptabel risiko og sikkerhetsorganiseringen (kapittel 2-4)
2. Gjennomførende del– konkrete retningslinjer og rutiner, herunder risikovurderinger, klassifisering av informasjon, opplæring mv. (kapittel 5-8)
3. Kontrollerende del – internrevisjon, rapportering av avvik, rapportering til ledelse, herunder ledelsens gjennomgang/ årsrapport. (kapittel 9-10)

Informasjonssikkerhet og personvern er et lederansvar. Det operative ansvaret og det praktiske arbeidet med å ivareta informasjonssikkerheten og personvernet til de enkelte enhetene ved NIH, jf. Kap. 4 om roller og ansvar.

Ledelsessystemet for informasjonssikkerhet og personvern ved NIH omfatter

- alle som får tilgang til NIH sine informasjonsverdier (studenter, ansatte, gjester, samarbeidspartnere etc.)
- Aktiviteter ved NIH/Sognsvann og ved eksterne studier
- all teknologi (IT-systemer, datanettverk, databaser/-registre etc.)
- alle informasjonsverdier

2. Regelverk

Norges idrettshøgskole er et forvaltningsorgan underlagt Kunnskapsdepartementet. Virksomheten har hovedmålsetninger som angitt i §§1-3 og 1-4 i Lov om universiteter og høgschooler. Innenfor disse hovedmålsettingene er høgskolens mål for sin virksomhet nedfelt i Strategisk plan.

Identifikasjon av relevant lov- og regelverk

Foruten universitets- og høyskoleloven har følgende lover med tilhørende forskrifter særlig betydning for høgskolens arbeid med informasjonssikkerhet og personvern i sin virksomhet. Oversikten er ikke uttømmende:

- **[Forvaltningsloven](#)** inneholder blant annet saksbehandlingsregler for forvaltningen, herunder regler om habilitet for saksbehandler og andre som har med saken eller saksbehandleren å gjøre. Denne loven inneholder også regler om taushetsplikt (§§13-13e), informasjons- og veiledningsplikt, varsling og innsyn og klager og omgjøring av enkeltvedtak
- **[Offentleglova](#)** inneholder bestemmelser om i hvilken grad forvaltningens saksdokumenter skal være tilgjengelige for offentligheten. Hovedregelen er at dokumentene er tilgjengelige hvis ikke denne loven eller andre lover bestemmer noe annet. Offentleglova har også bestemmelser om meroffentlighet
- **[Åndsverkloven](#)** inneholder regler om rettigheter til åndsverk og andre relaterte rettigheter. Loven er viktig fordi den forteller hvilke rettigheter som eksisterer og hvilken utstrekning de har, som høgskolen igjen må respektere og skal overholdes innenfor høgskolens kontrollsfære, for eksempel via IT-tjenestene
- **[Personopplysningsloven](#)** inneholder hovedreglene for behandling av personopplysninger, informasjonssikkerhet og melde- og konsesjonsplikt, hvilke plikter høgskolen som behandlingsansvarlig har og hvilke rettigheter de registrerte har i forhold til Norges idrettshøgskole som behandlingsansvarlig
- **[Helseregisterloven](#), [helsepersonelloven](#) og [lov om pasientrettigheter](#)** om blant annet behandling av klient-/pasientdata og taushetsplikt for helsepersonell
- **[Biobankloven](#)** inneholder særregler om biobanker.
- **[Arkivloven](#)** inneholder regler om hvordan høgskolens arkiver skal operere og hvilke dokumenter som skal arkiveres
- **[Lov om medisinsk og helsefaglig forskning](#)** gjelder for medisinsk og helsefaglig forskning på mennesker, humant biologisk materiale eller helseopplysninger.

Følgende lover og forskrifter har også betydning:

- **Sikkerhetsloven** gjelder for forvaltningsorgan og har som formål å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser, ivareta den enkeltes rettssikkerhet og trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste
- **Loven om eksportkontroll** gjelder kontroll med eksport av strategiske varer, tjenester og teknologi som kan være av betydning for andre lands utvikling, produksjon eller anvendelse av produkter til militært bruk eller som direkte kan tjene til å utvikle et lands militære evne samt varer og teknologi som kan benyttes til å utøve terrorhandlinger jfr straffeloven §147.
- **Reglement for økonomistyring i staten** inneholder både reglement og bestemmelser. Dette er kjent som RØS/BØS, og er et felles administrativt regelverk for økonomistyring i staten. En del av bestemmelsene er relevante for administrativ IT.

3. Sikkerhetsmål og sikkerhetsstrategi

God informasjonssikkerhet skal bidra til at NIH oppnår sine strategiske målsettinger og ivaretar sitt samfunnsoppdrag. Konfidensialitet, integritet og tilgjengelighet for høgskolens informasjonsverdier skal ivaretas på en enhetlig og systematisk måte i hele organisasjonen. Informasjonsverdier skal være tilgjengelig for de som skal ha tilgang (tilgjengelighet), de skal sikres mot utilsiktet og urettmessig endring (integritet), og de skal ikke være tilgjengelig for uvedkommende (konfidensialitet).

Sikkerhetsmål

Ved Norges idrettshøgskole gjelder følgende mål for sikkerhetsarbeidet:

1. Det skal være høy kvalitet på forvaltningen av all informasjon som benyttes i høgskolens kjerneaktiviteter
2. Arbeidet med informasjonssikkerhet og personvern skal bidra til at NIH ivaretar sine plikter som offentlig forvaltningsorgan og respekterer rettighetene til de registrerte, herunder ansatte, studenter og deltagere i forsknings- og studentprosjekter
3. Arbeidet med informasjonssikkerhet og personvern skal oppfylle de enhver tid gjeldende krav som følger av lov og forskrift, samt krav fra Kunnskapsdepartementet
4. Arbeidet med informasjonssikkerhet og personvern skal til enhver tid ivareta grunnleggende personvern hensyn
5. Arbeidet med informasjonssikkerhet og personvern skal bidra til at alle skal kunne ha tillit til kvaliteten på all informasjon som kommuniseres og formidles av NIH
6. Arbeidet med informasjonssikkerhet og personvern skal bidra til at NIH ivaretar sitt omdømme som profesjonelt og kompetent forvaltningsorgan

Akseptkriterier - Mål for akseptabel risiko.

Arbeidet med informasjonssikkerhet skal sørge for at informasjonsverdiene ved Norges idrettshøgskole til enhver tid er tilfredsstillende sikret mot brudd på konfidensialitet, integritet og tilgjengelighet. For å oppnå tilfredsstillende informasjonssikkerhet skal arbeidet basere seg på følgende kriterier for akseptabel risiko:

Åpen informasjon:

Integriteten og tilgjengeligheten til informasjon som skal være offentlig tilgjengelig, uavhengig av om dette dreier seg om forsknings-, undervisnings- eller administrativ informasjon, skal prioriteres. Integriteten til informasjonen skal vektlegges foran hensynet til tilgjengeligheten.

Intern informasjon:

Konfidensialiteten og integriteten til informasjon som benyttes i intern administrasjon og saksbehandling eller i pågående eller planlagt forskning/studentforskning skal prioriteres høyt. Dette omfatter blant annet informasjon som er unntatt offentlighet, upubliserte artikkel- eller bokmanus, ikke-konfidensielle forskningsdata som ikke er godkjent for publisering/offentliggjøring av prosjektleder, utkast til strategier/planer eller ikke-publiserte forslag til forskningsprosjekter. Det aksepteres kun mindre brudd på denne informasjonens konfidensialitet og integritet. Kortere avbrudd i informasjonens tilgjengelighet aksepteres.

Sensitiv informasjon:

Konfidensialiteten og integriteten til informasjon som er spesielt beskyttelsesverdig eller som er underlagt særskilt rettslig regulering skal prioriteres særlig høyt.

- Det aksepteres ikke brudd på konfidensialiteten eller integriteten til sensitive personopplysninger. Kortere avbrudd i personopplysningers tilgjengelighet aksepteres.
- Det aksepteres ikke brudd på konfidensialiteten og integriteten til konfidensielle forskningsdata som ikke er godkjent for publisering/offentliggjøring av prosjektleder. Kortere avbrudd i forskningsdataenes tilgjengelighet aksepteres.
- Det aksepteres ikke brudd på konfidensialiteten og integriteten til eksamensoppgaver (tekster/forslag) og eksamensbesvarelser. Det samme gjelder uferdige eller innleverte studentoppgaver (bachelor/master) og avhandlinger (p.hd.) som ikke skal eller ikke er godkjent for publisering/offentliggjøring. Korte avbrudd i tilgjengeligheten aksepteres dersom dette ikke vanskeliggjør eksamensgjennomføring eller innlevering og sensurering av eksamensbesvarelser, studentoppgaver eller p.hd.-avhandlinger.

Sikkerhetsstrategi

For å realisere sikkerhetsmålene og for å sørge for tilfredsstillende informasjonssikkerhet og personvern, skal arbeidet med informasjonssikkerhet og personvern basere seg på følgende hovedprioriteringer:

- Alt arbeid med informasjonssikkerhet og personvern skal basere seg på risikovurderinger.
- Ledelsen ved NIH skal bevilge nødvendige ressurser til opplæring og kompetanseheving for ledere og ansatte som er delegert ansvar for informasjonssikkerhet og personvern eller som er pålagt å utføre konkrete arbeidsoppgaver.

- Ledere ved NIH som er delegert ansvar for informasjonssikkerhet og personvern skal sørge for at ressurser bevilges til planlegging, gjennomføring og oppfølging av pålagte arbeidsoppgaver innenfor deres ansvarsområder.
- Alle brukere av informasjonsverdier ved NIH skal informeres om rutiner for sikker håndtering av disse.
- Alle brukere av informasjonsverdier ved NIH skal informeres om NIH sitt avvikssystem og ha en forståelse av når avvik skal meldes.
- Bruk av eksterne databehandlere for drift og forvaltning av NIH sine informasjonsverdier, eksempelvis bruk av skytjenester, kan skje dersom dokumentert risikonivå vurderes å være akseptabelt og nødvendige avtaler er inngått og blir fulgt opp.

4. Roller, ansvar og oppgaver

I det følgende gis en nærmere beskrivelse sikkerhetsorganiseringen innenfor informasjonssikkerhet og personvern (ISP) ved NIH, og hvilket ansvar og hvilke oppgaver som er lagt til de ulike rollene.

Styret ved NIH

- Styret har det overordnede ansvaret for at NIHs verdier forvaltes på en effektiv og betryggende måte og i tråd med gjeldende lover, forskrifter og avtaler for informasjonssikkerhet og personvern.
- Styret behandler og vedtar Ledelsessystemet og vesentlige endringer i dette.
- Styret kan stille krav til det videre arbeidet med ISP ved NIH.

Administrerende direktør

- Administrerende direktør har det overordnede ansvaret for ISP ved NIH
- Administrerende direktør er forskningsansvarlig ved NIH
- Administrerende direktør rapporterer til styret om arbeidet med ISP ved NIH.
- Er ansvarlig for NIHs Ledelsessystem
- Eier og er ansvarlig for informasjonssikkerhetsforumet ved NIH
- Leder IT styringsgruppe
- Skal sørge for at det avsettes tilstrekkelige ressurser til arbeidet med ISP i hele organisasjonen, herunder opplæring og kompetanseheving.
- Er ansvarlig for at det finnes en oversikt over de informasjonsverdiene som behandles av institusjonen
- Skal årlig gjennomgå status for arbeidet med ISP i virksomheten («Ledelsens gjennomgang»)
- Skal årlig rapportere til styret status for arbeidet med ISP
- Skal informere styret og rektor om spesielt alvorlige sikkerhetsbrudd
- Skal foreslå eventuelle endringer i Ledelsessystemet (sikkerhetsmål, sikkerhetsstrategi, akseptabel risiko og organisering) til styret

Ansvaret for daglige oppgaver innenfor ISP er delegert videre i organisasjonen, se presisering i hver enkelt rolle nedenfor.

Rektor

- Skal bistå administrerende direktør i oppfølging av ISP ved NIH
- Skal holde seg orientert om arbeidet med ISP
- Godkjenner mindre endringer i Ledelsessystemet på vegne av styret

Krisestab

- Rutine for Krisestab skal utarbeides/er i prosess

Instituttleder – forskningsansvarlig

- Har ansvar for at all behandling av personopplysninger ved avdelingen skjer i henhold til NIHs rutiner.
- Instituttleder er delegert ansvar for alle forskningsprosjekt ved sitt institutt.
- Forskningsansvarlig har ansvar for at alle instituttets forskningsprosjekt gjennomføres i henhold til NIHs rutiner.
- Instituttspesifikke rutiner for prosjektplanlegging/gjennomføring og avslutning av forskningsprosjekt skal utarbeides og vedlegges Ledelsessystemet.
- Alle institutt skal ha rutiner for:
 - o Formell overføring av prosjektlederansvar når forsker/veileder slutter
 - Sikker lagring av fysiske dokumenter slik at ISP ivaretas
 - o Personvernkonsekvensvurdering (DPIA) for forskningsprosjekt med høy ulempe og risiko for personvern
- Forskningsansvarlig kan delegere oppgaver knyttet til gjennomføring og oppfølging av forskningsprosjekt til leder for forskningssenter knyttet til sitt institutt.
- Skal ha oversikt over de informasjonsverdier og IT-løsninger enheten har ansvar for.
- Alle IT-løsninger som benyttes av ansatte på enheten ut over institusjonell programvare skal være godkjent av informasjonssikkerhetsrådgiver.
- Instituttleder utpeker tjenesteeier for hvert IT-system som enheten har ansvar for.
- Skal sørge for at alle administrative behandlinger av personopplysninger er registrert i Behandlingslisten
- Skal sørge for at egne ansatte og prosjektledere har kompetanse til å utføre sine oppgaver slik at informasjonssikkerhet og personvern blir ivaretatt.
- Skal sørge for at ansatte deltar i institusjonelle opplæringstiltak innenfor ISP.
- Har ansvar for at alle rutineavvik og sikkerhetsbrudd varsles og skal sørge for at alle brukere i sin enhet er kjent med rutiner for slike varslinger.
- Skal bistå ved gjennomføring av internkontroll innenfor ISP – se egen rutine.

Avdelingsledere

- Har ansvar for at all behandling av personopplysninger ved avdelingen skjer i henhold til NIHs rutiner.
- Skal ha oversikt over alle informasjonsverdier og IT-løsninger enheten har ansvar for.
- Alle IT-løsninger som benyttes av ansatte på enheten ut over institusjonell programvare skal være godkjent av informasjonssikkerhetsrådgiver.
- Avdelingsleder utpeker tjenesteeier for de IT-system som enheten har ansvar for.
- Skal sørge for at alle administrative behandlinger av personopplysninger er registrert i Behandlingslisten.

- Skal sørge for at egne ansatte og prosjektledere har kompetanse til å utføre sine oppgaver slik at informasjonssikkerhet og personvern blir ivaretatt.
- Skal sørge for at ansatte deltar i institusjonelle opplæringstiltak innenfor ISP.
- Har ansvar for at alle rutineavvik og sikkerhetsbrudd varsles og skal sørge for at alle brukere i sin enhet er kjent med rutiner for slike varslinger.
- Skal bistå ved gjennomføring av internkontroll innenfor ISP – se egen rutine.

Spesielt for IT-direktør

I tillegg til ansvar og oppgaver nevnt under Avdelingsledere (se ovenfor) er IT-direktør delegert et institusjonsovergripende ansvar for informasjonssikkerhet og personvern i all infrastruktur ved NIH.

- Skal sørge for at vedtatte sikkerhetsmål, kriterier for akseptabel risiko og sikkerhetsstrategi blir fulgt opp ved investeringer og i drift av alle IT-løsninger ved NIH.
- Har ansvar for å ajourføre oversikt over systemer, typer av data lagret i systemene, avhengighet mellom system, risikovurdering av systemer og oppfølging av risikovurdering.
- Har ansvar for IT-reglementet for NIH
- Har ansvar for klassifiserings- og lagringsguide.
- Har ansvar for at det finnes oppdaterte kontinuitetsplaner for sentrale system.
- Har ansvar for at det finnes relevante driftsrutiner, herunder rutiner for sikkerhetskopiering
- Har ansvar for at det inngås databehandleravtaler med eksterne aktører der dette er nødvendig (på institusjonsnivå)
- Skal etter forespørsel bistå enheter eller forskningsprosjekter ved risikovurderinger av teknisk sikkerhet.
- Skal bistå enheter eller forskningsprosjekt ved håndtering av tekniske sikkerhetsbrudd.
- Skal bistå rådgivere informasjonssikkerhet og personvern ved avvik der dette er aktuelt
- Er delegert ansvar for å lede informasjonssikkerhetsforum
- Innkaller IRT ved behov

Spesielt for Eiendomssjef

I tillegg til ansvar og oppgaver nevnt under Avdelingsledere (se ovenfor) er Eiendomssjefen delegert et institusjonsovergripende ansvar for fysisk sikring av bygninger og anlegg ved NIH.

Rådgivere informasjonssikkerhet og personvern

Er delegert ansvar for det løpende arbeidet med informasjonssikkerhet og personvern ved NIH.

Felles for begge rådgiverstillinger:

- Har ansvar for at Ledelsessystemet oppdateres og utvikles innenfor sine respektive områder.
- Deltar i informasjonssikkerhetsforum
- Skal bistå institusjons- og avdelingsledere med utvikling av og gjennomføring av opplæringstiltak innenfor ISP
- Skal løpende foreslå tiltak for å bedre ISP ved NIH
- Sørge for at oppdatert informasjon om rutiner og regelverk for ISP er tilgjengelig på hjemmesider og intranett
- Bidra til at spørsmål om ISP inkluderes i alle risikovurderinger
- Skal holde seg oppdatert på tiltak i sektoren innenfor informasjonssikkerhet og personvern
- Skal delta i relevante samlinger arrangert av Sikt, herunder CISO-forum
- Skal gjennomføre internkontroll – se egen rutine
- Etter forespørsel, bistå enhetene ved deres årlige risikovurderinger
- Forberede og delta i ledelsens årlige gjennomgang

Spesielt for rådgiver informasjonssikkerhet

Stillingen er plassert i IT-avdelingen

- Skal håndtere avvik på informasjonssikkerheten, inklusiv ha kontakt med og rapportere til Personvernombud og til Datatilsyn der dette er nødvendig
- Skal holde Administrerende direktør og IT-direktør oppdatert om informasjonssikkerhetsavvik
- Har det praktiske ansvar for utarbeidelse av IT-reglement
- Skal signere databehandleravtaler NIH inngår med andre aktører
- Skal godkjenne ikke-institusjonell programvare
- Stedfortreder for IT-direktør i Incident Response Team

Spesielt for rådgiver personvern:

Stillingen er plassert i HR.

- Skal håndtere brudd på personopplysningssikkerheten, inklusiv ha kontakt med og rapportere til Personvernombud og til Datatilsyn der dette er nødvendig.
- Skal holde administrerende direktør oppdatert om personvern avvik.
- Er kontaktperson for Sikt angående Institusjonsportalen (oversikt innmeldte forskningsprosjekter på NIH med personopplysninger)

- Har det praktiske ansvar for dokumentering av Ledelsens gjennomgang, årshjul/ tiltaksplan for ISP og oppdatering av Ledelsessystemet

Personvernombud

- skal kontrollere NIHs overholdelse av personvernlovgivningen
- skal involveres i håndteringen av avvik etter personvernlovgivningen
- skal opptre uavhengig og gi høgskolen råd som er objektive og kvalifiserte ut ifra personvern hensyn
- skal informere og gi råd til NIH sine ansatte og studenter om gjeldende forpliktelser etter personvernlovgivningen
- skal vurdere og gi råd i forbindelse med personvernkonsekvensvurderinger (DPIA) og kontrollere gjennomføringen av disse vurderingene
- skal utarbeide årlig rapport som skal tas inn som vedlegg til årsrapport for informasjonssikkerhet og personvern
- kan kontaktes direkte av de registrerte med spørsmål om NIHs behandling av deres personopplysninger, og om utøvelsen av sine rettigheter etter personvernforordningen (GDPR)

IT styringsgruppe

IT styringsgruppe har overordnet ansvar for oversikt over leveranser, prosjekter, brukertilfredshet og økonomi for IT ved NIH.

- Spesifikt har IT styringsgruppe ansvar for
- Å anbefale tiltak for å vedlikeholde og bedre informasjonssikkerhet
- Å holde oversikt over informasjonssikkerhetshendelser, hendelsesanalyser og tiltak
- Beslutte risikoanalyser for IT
- Beslutte anskaffelse av institusjonell programvare/IT-løsninger

Medlemmer

- Administrerende direktør – styringsgruppens leder
- Instituttleder IFP
- Instituttleder IIM
- Avdelingsleder HR
- Avdelingsleder Økonomi
- Avdelingsleder Studieadministrasjonen
- Avdelingsleder IT

Arbeidsgruppe for informasjonssikkerhet i forskningsprosjekter

Arbeidsgruppa skal sikre forankring i forskningsmiljøene for institusjonsovergripende tiltak inklusiv opplæring innenfor informasjonssikkerhet og personvern. Hvert institutt skal være representert. Medlemmene oppnevnes av instituttleder.

- Arbeidsgruppa ledes av administrerende direktør
- Medlemmene skal fungere som superbrukere innen sitt fagmiljø/institutt
- Gruppa innkalles etter behov

Brukere av NIHs informasjonssystemer

- Alle brukere skal sette seg inn i og overholde vedtatte rutiner og retningslinjer for sikker håndtering av informasjonsverdier og personopplysninger.
- Alle brukere skal rapportere eventuelle avvik fra vedtatte rutiner og brudd på ISP.

Spesielt om ansattes ansvar:

- Ansatte skal ved behov bistå ved planlegging, gjennomføring eller oppfølging av konkrete sikkerhetsoppgaver innenfor ISP.

5. Klassifisering av informasjon

En forutsetning for å kunne si noe om akseptabel bruk, samt behovet for sikkerhetstiltak, er at det er foretatt en klassifisering av informasjonen som behandles. Klassifiseringen ligger til grunn for hvilken grad av sikring (IT-teknisk, organisatorisk og fysisk) informasjonen skal underlegges. Videre vil klassifisering bidra til å oppnå en oversikt over hvilke informasjonsverdier NIH forvalter.

Klassifiseringen gir personer som skal behandle informasjonsverdier en konkret indikasjon og veiledning på hvordan denne skal håndteres og beskyttes.

6. Risiko- og sårbarhetsanalyser

Risikovurderinger skal avdekke mulige uønskede hendelser/trusler som kan føre til brudd på informasjonssikkerheten ved NIH. Vurderingene er derfor sentrale i arbeidet med å sikre trygg og sikker behandling av NIH sine informasjonsverdier. I tillegg til å avdekke hva som kan gå galt, skal den avdekke hva vi har gjort og hva vi ytterligere kan gjøre for å hindre at uønskede hendelser inntreffer, samt redusere konsekvensene dersom de likevel skjer.

Dersom risikoen for at en eller flere uønskede hendelser skjer er større enn det som anses som akseptabelt, må denne risikoen håndteres ved at forebyggende tiltak iverksettes.

Risikovurderinger skal foretas:

- ved etablering eller større endring av IT-systemer
- ved organisatoriske endringer som kan påvirke informasjonssikkerheten
- når trusselbildet endres

Alle risikovurderinger skal dokumenteres. Dersom risikovurderinger avdekker tilfeller som skal følges opp, skal det navngis hvem som har ansvar for å fastsette relevante tiltak og plan for oppfølging av disse. Risikovurderingen skal dokumenteres og tilgjengeliggjøres til informasjonssikkerhetsforum for etterkontroll.

7. Opplæring

Opplæring skal bidra til å bygge en god sikkerhetskultur ved NIH. Den skal bevisstgjøre ansatte og studenter om betydningen av informasjonssikkerhet og personvern, samt gjøre dem i stand til å etterleve IT-reglementet ved Norges idrettshøgskole i sitt daglige virke. Opplæring i informasjonssikkerhet og personvern må derfor tas inn som en naturlig del av opplæringen av studenter og ansatte på alle nivå i organisasjonen. Systemeiere er spesielt ansvarlig for opplæring i sine respektive systemer.

Ledere har et overordnet ansvar for at nødvendig informasjon blir gitt til de ansatte, og at det blir satt av tid og ressurser til opplæring. For å sikre at dette ansvaret blir ivaretatt skal informasjonssikkerhet og personvern inngå i NIHs lederopplæring.

Informasjon om informasjonssikkerhet og personvern ved NIH skal være lett tilgjengelig for alle via høgskolens nettsider og andre relevante kanaler.

Alle som er tildelt sentrale roller og oppgaver i sikkerhetsarbeidet skal gis spesiell opplæring ved behov. Eksterne kurs, seminarer og deltakelse i relevante nettverk er viktig for å sikre utveksling av informasjon og øke kompetansen hos denne gruppen ansatte.

8. Håndtering av hendelser og avvik

Avvik er brudd på lover, forskrifter eller interne bestemmelser ved NIH. Innmeldte avvik og håndteringen av disse er en sentral kilde for å både vurdere sikkerhetsnivået ved de enhetene der avvik inntreffer samt for NIH sett under ett. Oversikten over innmeldte avvik vil kunne avdekke behov for nye eller justere eksisterende sikringstiltak.

Avvikshåndtering handler om kvalitet og forbedring, i tillegg til skadebegrensning.

I denne sammenheng kan avvik og hendelser være av sikkerhetsmessig art, og/eller brudd på personvernlovgivningen.

Eksempler på hendelser og avvik:

- tyveri av datautstyr
- misbruk av IT-tjenester
- misbruk av passord
- fakturasvindel eller andre svindelforsøk
- dataangrep
- datalekkasje
- løsepengevirus
- svakheter i IT-systemer
- brudd på eller manglende rutiner ved NIH
- fortrolig informasjon på avveie
- uautorisert tilgang til opplysninger
- bruk av databehandler uten tilstrekkelig avtale
- innsamling av personopplysninger utover det man hadde legitim bruk for (brudd på dataminimeringsprinsippet)
- behandling av personopplysninger uten lovlig grunnlag, herunder viderebehandling til nye formål uten at man har lovlig adgang til dette

Melding og håndtering av hendelser og avvik

Den som oppdager, eller blir gjort oppmerksom på, hendelser og avvik (heretter «avvik») skal melde inn dette via høgskolens avvikssystem. Avvik meldes via e-post til adressen sikkerhetsavvik@nih.no

Ansvar for planlegging og gjennomføring av korrigerende tiltak vil variere ut fra avvikets karakter. Den enhet som har størst faglig nærhet til avviket vil normalt være ansvarlig for prosessen med å rette avviket. Ved IT-relaterte avvik skal IT-avdelingen alltid være ansvarlig for prosessen med å rette avviket. Større avvik skal håndteres av IRT-teamet.

Informasjonssikkerhetsforum kan bistå enheten med hvordan avviket bør håndteres.

Informasjonssikkerhetsforum skal føre en samlet oversikt over alle avvik som er meldt inn. Disse skal blant annet inngå i ledelsens gjennomgang, og benyttes for læring på tvers i organisasjonen for å hindre gjentakelse.

Melding til Datatilsynet

Ved avvik som innebærer brudd på personopplysningssikkerheten skal NIH som behandlingsansvarlig melde fra til Datatilsynet uten ugrunnet opphold og senest 72 klokke timer etter å ha fått kjennskap til avviket. Det er derfor svært viktig at avvik meldes så raskt som mulig.

Administrerende direktør beslutter om et avvik skal meldes Datatilsynet.

Orientering om slike saker skal alltid oversendes rektor.

Så langt som det er mulig, skal Personvernombudet bli orientert om saken og få tilgang til avviksmeldingen før den sendes. Hvis sakens art tilsier det skal Personvernombudet involveres direkte i håndteringen av avviket fra et så tidlig tidspunkt som mulig.

Personvernombudet har imidlertid alltid anledning til å aktivt involvere seg i håndteringen av alle avvik som innebærer brudd, eller mulige brudd, på personopplysningssikkerheten.

9. Internkontroll og sikkerhetsrevisjon

Det skal gjennomføres årlig internkontroll med informasjonssikkerhet og personvern. Informasjonssikkerhetsforum har det praktiske ansvar for gjennomføring. Hensikten er å avdekke mulige svakheter og risiko i organisasjonen. Internkontrollen skal også gi mulighet for ulike grupper ansatte å komme med tilbakemeldinger til arbeidet med ISP på NIH.

Administrative avdelinger:

Rådgivere informasjonssikkerhet og personvern skal gjennomføre intervjuer med et utvalg administrativt ansatte og avdelingsledere.

- Intervjuene gjennomføres etter et standard skjema.
- Informasjonssikkerhetsforum gjennomgår tilbakemeldingene.
- Oppsummering og forslag til oppfølging presenteres for AL

Prosjektledere forskningsprosjekt

Et utvalg prosjektledere skal rapportere om gjennomføring av sine forskningsprosjekt. Stipendiater er per definisjon ikke prosjektledere, men bør inkluderes i utvalget av opplæringshensyn.

- Rapportering skjer i henhold til et standard skjema.
- Stipendiater rapporterer på eget prosjekt på vegne av veileder.

I tillegg til selvrapportering skal det foretas stikkprøver av enkeltprosjekt på alle institutt. Gjennomgangen foretas rådgivere ISP i samarbeid med instituttledelse.

Faginstitutt og forskningssentre

Instituttledere/forskningsansvarlige skal rapportere til rektor om ISP i forskningsprosjekt på sitt institutt. Dersom instituttleder har delegert ansvar for oppfølging av forskningsprosjekt til senterleder, rapporterer senterleder separat.

- Rapportering skjer i henhold til et standard skjema.
- Informasjonssikkerhetsforum gjennomgår tilbakemeldingene, egenrapporter og stikkprøver.
- Oppsummering og forslag til oppfølging presenteres for Faglig Ledelse (FL)

Internrevisjon

Internrevisjon av ledelsessystemet for informasjonssikkerhet og personvern skal gjennomføres ved behov, og som hovedregel ikke sjeldnere enn hvert femte år.

10. Ledelsens gjennomgang

Ledelsens gjennomgang er et årlig møte der ledelsen vurderer ytelsen og effektiviteten av informasjonssikkerhets- og personverntiltak. Gjennomgangen er en viktig del av en organisasjons styringsprosess og hjelper med å sikre kontinuerlig forbedring.

Ledelsens gjennomgang skal omhandle:

- avvik og hendelser, herunder eventuelle trender som det bør rettes særskilt oppmerksomhet mot
- risikobildet for NIH
- resultater/oppfølging av kontrollaktiviteter
- resultater/oppfølging av internrevisjon, dersom aktuelt
- gjennomgang av personvernombudets rapport og ta stilling til foreslåtte tiltak fra denne
- resultater/oppfølging av eksterne revisjoner, dersom aktuelt
- tilstand for risikohåndtering ved NIH
- status på vedtatte tiltak fra forrige gjennomgang
- behov for justeringer av ledelsessystemet
- ressurs- og kompetansebehov, herunder om det foreligger særlige behov for kommende år

Årsrapport og årsplan

Innholdet som presenteres under ledelsens gjennomgang skal dokumenteres skriftlig i form av en årsrapport som oppsummerer året som har gått og oversikt over tiltak som planlegges gjennomført/oppdatert årshjul for informasjonssikkerhet og personvern. Denne leveres til ledelsen sammen med årsrapporten til personvernombudet.