Ledelsessystem for informasjonssikkerhet (LSIS) ved Høgskolen i Innlandet

Versjon: 1.0

Dato: 22.11.18

Basert på ISO/IEC 270001/02: 2013

Dokumentref: 18/02185-3	**Dokumentansvarlig: GT**
Filnavn: LSIS_Hinn.docx	

Revisjoner:

Versjon	Dato	Beskrivelse/ kommentar	Utført av
0.01	Aug -2018	Etablering av dokument	Gunnar
0.02	23/08/18	Innspill fra forskningsadministrasjonen	Anne Sofie/Gunnar
0.03	25/09/18	Justeringer og utbygging av systemeierrollen samt presisering av CSO	Gunnar
0.004	12/10/18	Høringsrunde og innspill fra Innkjøp	Gunnar
1.0	22/11/18	Vedtatt av styret	

Innhold

1 Innledning

Kjernevirksomheten til Høgskolen i Innlandet er (a) å samle inn og bearbeide informasjon/data ved bruk av vitenskapelige metoder og (b) produsere og formidle kunnskap av høy internasjonal kvalitet.[1] Det betyr at Høgskolen i Innlandet i stor grad lever av å forvalte, foredle og formidle ikke-materielle verdier. Derfor er det også avgjørende at all informasjon som Høgskolen i Innlandet forvalter i administrasjon, forskning, undervisning og offentlig formidlingsarbeid er tilfredsstillende sikret mot brudd på:

- **Konfidensialiteten**: hindre at uvedkommende får tilgang til konfidensiell eller sensitiv informasjon,
- **Integriteten**: hindre uønsket endring, sletting eller manipulering av informasjon og
- **Tilgjengeligheten**: sikre brukere tilgang til informasjon når de har behov for det.

1.1 *Risikostyring*

Informasjonssikkerhet handler om risikostyring. Risikostyring innebærer at hendelser som kan føre til uautorisert tilgang, endring, tap eller skade på informasjonen skal identifiseres og vurderes. Deretter skal de iverksettes tiltak for å unngå uønskede hendelser som vurderes å ha størst risiko. Hensikten med risikostyrt informasjonssikkerhetsarbeid er derfor å forutse og forebygge uønskede hendelser og avvik før de oppstår.

Risikostyrt informasjonssikkerhetsarbeid skal forankres i toppledelsen. Arbeidet skal utføres av en sikkerhetsorganisasjon med egne mål, strategier, arbeidsmetodikk/redskaper og ressurser.

[1] Se særlig kapittel 1 i lov om universiteter og høyskoler (http://lovdata.no/dokument/NL/lov/2005-04-01-15).

1.2 *Krav til Ledelsessystem for informasjonssikkerhet*

Personopplysningsloven med forskrift, forvaltningsloven med forskrift (e-forvaltningsforskriften) og helseforskningsloven med forskrift stiller krav til innføring av Ledelsessystem for informasjonssikkerhet. Disse kravene gjelder også for Høgskolen i Innlandet. I tillegg inneholder andre lovverk, blant annet offentlighetsloven og arkivloven, bestemmelser som har betydning for arbeidet med sikring av informasjon ved Høgskolen i Innlandet.

I Kunnskapsdepartementets (KD) tildelingsbrev til Høgskolen i Innlandet kreves det innføring av et Ledelsessystem for informasjonssikkerhet (LSIS) bygget på grunnprinsippene i anerkjente sikkerhetsstandarder.[2] For å bistå oss i dette arbeidet har KD gitt UNINETT i mandat å opprette Sekretariatet for informasjonssikkerhet i UH-sektoren. Høgskolen i Innlandet skal rapportere til KD hvordan vi bruker denne interne tjenesten.

Ledelsessystemet for informasjonssikkerhet ved Høgskolen i Innlandet ivaretar de kravene som lovverket og Kunnskapsdepartementet stiller til arbeidet med informasjonssikkerhet i UH-institusjoner.

[2] Tildelingsbrevet til institusjone 2014 (tilgjengelig på http://www.regjeringen.no/nb/dep/kd/dok/andre/brev/utvalgte_brev/2014/tildelingsbrev-til-universiteter-og-hoys.html?id=747533).

2 Avgrensning av ledelsessystemet

Nedenfor følger en uttømmende oversikt over hvilke deler av organisasjonen ved Høgskolen i Innlandet som inngår i styringssystemet for informasjonssikkerhet:

2.1 *Geografiske lokasjoner:*

- Studiested Elverum
- Studiested Lillehammer
- Studiested Hamar
- Studiested Rena
- Studiested Blæstad
- Studiested Evenstad
- Desentralisert studiested Oslo
- Desentralisert studiested Kongsvinger

2.2 *Organisatoriske enheter*

2.2.1 Ledelsen

- Rektor
- Viserektor
- Prorektor Utdanning
- Prorektor Forskning
- Prorektor innovasjon og samfunnskontakt
- Økonomidirektør
- HR-direktør
- Direktør for digitalisering og infrastruktur
- Dekan – ALB
- Dekan – AMEK
- Dekan – DNF

- Dekan – HHS
- Dekan – HSV
- Dekan - LUP

2.2.2 Administrative enheter

- Rektors stab
- Kommunikasjons- og markedsavdelingen
- Senter for livslang læring
- Studieavdelingen
- Høgskolebiblioteket
- Seksjon for lønn
- Seksjon for regnskap
- Seksjon for innkjøp
- Seksjon for økonomistyring
- IT-avdelingen
- Eiendomsavdelingen
- Seksjon for dokumentasjon- og informasjonsforvaltning
- Forskningsadministrasjonen

2.2.3 Faglige avdelinger

- Fakultet for anvendt økologi, landbruksfag og bioteknologi
- Fakultet for audiovisuelle medier og kreativ teknologi
- Den norske filmskolen
- Handelshøgskolen Innlandet – fakultet for økonomi og samfunnsvitenskap
- Fakultet for helse- og sosialvitenskap
- Fakultet for lærerutdanning og pedagogikk

2.3 *Informasjonsverdier*

2.3.1 Hovedtyper digitale data

- Personlige dokumenter
- Økonomiske data som regnskap, prosjektstyring og innkjøp.
- Juridiske dokumenter som kontrakter, avtaler, protokoller, referater, opptaksbrev, vitnemål, klagesaker osv.
- Forskningsdata, herunder ting som omfattes av helseforskningsloven
- Strategiske og kommersielle data som planer, kundeinformasjon og statistikker.
- E-post og talepost
- Databaser av forskjellige typer. De viktigste er:
    - studentregister
    - personalregister
    - regnskap
    - prosjekter
    - biblioteksdata
    - publiseringsdata
    - Forskningsdatabaser
- Personlige og delte harddisker
- Sikkerhetskopier og digitale arkiver
- Krypteringsnøkler

2.3.2 Varige (arkiverte) informasjonsverdier

- Personlige dokumenter
- Økonomiske dokumenter
- Juridiske dokumenter
- Forskningsdata
- Strategiske og kommersielle data
- E-postarkiv

- Mikrofilm og andre backup-medier
- Nøkler til safe / kontorer andre medier og lagerrom,
- Tidsskrifter, magasiner og bøker

2.4 *Aktører*

Alle ansatte i forsknings- undervisnings- og administrative stillinger (faste og midlertidige), alle studenter som er registrert ved institusjonen, alle gjester ved institusjonen (for eksempel gjesteforskere), alt innleid personell (for eksempel personer som utfører renhold, vedlikehold, driftsoppgaver, og liknende) og alle eksterne behandlere av informasjonsverdier (for eksempel databehandlere: USIT, UNINETT eller kommersielle virksomheter).

2.5 *Tekniske ressurser*

Alle tekniske systemer og datanettverk som anvendes til behandling av institusjonens informasjonsverdier, for eksempel IT-systemer, interne og eksterne datanettverk, databaser/-registre, manuelle personregistre, osv.

3 Sikkerhetsmål

Følgende mål for arbeidet med informasjonssikkerhet gjelder ved Høgskolen i Innlandet:

1. Arbeidet med informasjonssikkerhet skal bidra til høy kvalitet på forvaltningen av all informasjon som benyttes i administrasjon, forskning, undervisning og formidlingsaktiviteten ved Høgskolen i Innlandet.

2. Arbeidet med informasjonssikkerhet skal bidra til at Høgskolen i Innlandet ivaretar sine plikter som offentlig forvaltningsorgan og respekterer rettighetene til ansatte, studenter og deltakere i forskningsprosjekter.

3. Arbeidet med informasjonssikkerhet skal til enhver tid være i tråd med de krav som stilles i lover og forskrifter som gjelder for Høgskolen i Innlandet, og følge opp de kravene som Kunnskapsdepartementet stiller til informasjonssikkerheten.

4. Arbeidet med informasjonssikkerhet skal ivareta grunnleggende personvernhensyn, herunder privatlivets fred, den personlige integriteten og opplysningskvaliteten, ved all elektronisk behandling av personopplysninger.

5. Arbeidet med informasjonssikkerhet skal bidra til at alle skal kunne ha tillit til kvaliteten på den informasjonen som kommuniseres og formidles av Høgskolen i Innlandet, uavhengig av hvilke kanaler som benyttes.

6. Arbeidet med informasjonssikkerhet skal bidra til at Høgskolen i Innlandet ivaretar sitt omdømme som et profesjonelt og kompetent forvaltningsorgan.

4 Kriterier for akseptabel risiko

Arbeidet med informasjonssikkerhet skal sørge for at informasjonsverdiene ved Høgskolen i Innlandet til enhver tid er tilfredsstillende sikret mot brudd på konfidensialiteten, integriteten og tilgjengeligheten. For å oppnå tilfredsstillende informasjonssikkerhet skal arbeidet basere seg på følgende kriterier for akseptabel risiko:

4.1 *Åpen informasjon*

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

4.2 *Intern og begrenset 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.

4.3 *Sensitiv, Fortrolig og Strengt fortrolig informasjon.*

Konfidensialiteten og integriteten til informasjon som er spesielt beskyttelsesverdig eller som er underlagt særskilt rettslig regulering, for eksempel konfidensielle forskningsdata, opplysninger om enkeltpersoner (personopplysninger[3]) eller forslag/tekster til eksamensoppgaver, skal prioriteres særlig høyt.

[3] I personopplysningsloven § 2 defineres personopplysninger som opplysninger og vurderinger som kan knyttes til en enkeltperson.

- Det aksepteres ikke brudd på konfidensialiteten eller integriteten til personopplysninger. Dette gjelder i særlig grad for sensitive personopplysninger.[4] 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.

[4] I personopplysningsloven § 2 defineres sensitive personopplysninger som opplysninger om rasemessig eller etnisk bakgrunn; politisk, filosofisk eller religiøs oppfatning; at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling; helseforhold; seksuelle forhold eller medlemskap i fagforeninger.

5 Sikkerhetsstrategi

For å realisere sikkerhetsmålene og sørge for tilfredsstillende informasjonssikkerhet, skal arbeidet med informasjonssikkerhet ved Høgskolen i Innlandet basere seg på følgende hovedprioriteringer:

Alt arbeid med informasjonssikkerhet skal basere seg på risikovurderinger. Ingen sikringstiltak, uavhengig av om de er tekniske, organisatoriske, fysiske eller personalmessige, skal gjennomføres uten at risikovurderinger viser at det er behov for tiltakene. Risikovurderinger av IT-systemer og -tjenester, datanettverk og infrastruktur, arbeidsprosesser og fysiske forhold skal gjennomføres hvert annet år. Valg av sikringstiltak skal basere seg på tiltaksoversikten i ISO/IEC 27001: 2013 Annex A, jf. ISO/IEC 27002: 2013.

Ledelsen ved Høgskolen i Innlandet vil bevilge nødvendige ressurser til opplæring og kompetanseheving for ledere og ansatte som er delegert ansvar for informasjonssikkerheten ved Høgskolen i Innlandet eller som er pålagt å utføre konkrete arbeidsoppgaver. Opplæringen og kompetansehevingen skal i særlig grad fokusere på arbeidsmetodikken i risikostyrt informasjonssikkerhetsarbeid og praktisk bruk av konkrete arbeidsredskaper.

Ledere ved Høgskolen i Innlandet som er delegert ansvaret for informasjonssikkerheten skal sørge for at ressurser bevilges til planlegging, gjennomføring og oppfølging av pålagte arbeidsoppgaver innenfor deres ansvarsområder. Dette inkluderer iverksetting av sikringstiltak som er nødvendige for å oppnå tilfredsstillende informasjonssikkerhet.

Alle brukere av informasjonsverdiene til Høgskolen i Innlandet skal gis informasjon om rutiner for sikker håndtering av informasjonsverdier og trusler mot informasjonsverdiene. De skal også

informeres om avviksmeldingssystemet ved Høgskolen i Innlandet. I tillegg skal de informeres om hensikten med og viktigheten av at avvik/sikkerhetsbrudd rapporteres.

Fjerndrift av Høgskolen i Innlandet sine informasjonsverdier, for eksempel bruk av nettbaserte tjenester eller andre typer databehandlere, kan bare skje dersom risikoen for sikkerhetsbrudd er innenfor kriteriene for akseptabel risiko, og dersom de nødvendige avtaler er inngått og blir fulgt opp. Utkontraktering (eng.: outsourcing) av drift og forvaltning av informasjon med særskilte sikkerhetskrav, for eksempel sensitive personopplysninger eller konfidensielle forskningsdata, kan bare skje etter en spesielt grundig vurdering. Se KD's anbefaling om felles løsninger i sektøren.

Arbeidet med informasjonssikkerhet ved Høgskolen i Innlandet skal til enhver tid basere seg på anbefalte og anerkjente standarder for Ledelsessystemer for informasjonssikkerhet i offentlig sektor, jf. DIFIs referansekatalog versjon 3.1, punkt 2.16 (tilgjengelig på http://standard.difi.no/forvaltningsstandarder/referansekatalogen-html-versjon).

UNINETT og Sekretariatet for informasjonssikkerhet i UH-sektoren skal benyttes til rådgiving og bistand når det er nødvendig.

6 Sikkerhetsorganisasjon

I sikkerhetsorganisasjonen til Høgskolen i Innlandet inngår følgende roller:

- Høgskolestyret.
- Rektor.
- Digitaliseringsdirektør.
- CSO.
- Informasjonssikkerhetsforum.
- Hendelseshåndteringsteam (IRT).
- Fakultets-, avdelings-, enhets- og prosjektledere:
    - Avdelingsledere/direktører i sentraladministrasjonen.
    - Fakultetsledelsen, ledere i sentraladministrasjonen og andre ledere i fagavdelinger.
    - Ledere ved andre organisatoriske enheter (for eksempel forskningssentre).
    - Forskningsansvarlig og ledere i forskningsprosjekter.
- IT-direktør.
- Eiendomsdirektør.
- Brukere (ansatte, studenter, gjester).

Nedenfor følger en gjennomgang av hvilket ansvar og hvilke arbeidsoppgaver de ulike rollene i sikkerhetsorganisasjonen er pålagt å ivareta.

6.1 *Høgskolestyret*

Myndighet:

- Behandler og vedtar Ledelsessystemet for informasjonssikkerhet ved Høgskolen i Innlandet og vesentlige endringer i Ledelsessystemet. Spesielt gjelder dette endringer i sikkerhetsmål og kriterier for akseptabel risiko.
- Kan stille krav til det videre arbeidet med informasjonssikkerhet ved Høgskolen i Innlandet.

Rapportering:

- Skal informeres årlig om arbeidet med informasjonssikkerhet av Digitaliseringsdirektøren.
- Skal informeres om spesielt alvorlige sikkerhetsbrudd av Digitaliseringsdirektøren.

6.2 *Digitaliseringsdirektøren*

Myndighet og delegasjon:

- Digitaliseringsdirektøren har det overordnede daglige ansvaret for informasjonssikkerheten ved Høgskolen i Innlandet.
- Digitaliseringsdirektøren oppnevner medlemmer av informasjonssikkerhetsforumet ved Høgskolen i Innlandet.
- Digitaliseringsdirektøren kan delegere ansvaret for utøvelsen av daglige oppgaver til CSO, herunder også oppnevnelse av medlemmer til informasjonssikkerhetsforum.
- Digitaliseringsdirektøren skal undertegne avtaler med eksterne leverandører av digitale systemer.
- Digitaliseringsdirektøren skal undertegne avtaler med eksterne aktører (databehandlere) som behandler personopplysninger på vegne av Høgskolen i Innlandet.
- Godkjenner mandat for Høgskolen i Innlandet sitt hendelseshåndteringsteam (IRT).

Drift og ressurser:

- Skal sørge for at Ledelsessystemet for informasjonssikkerhet blir innført, satt i drift og vedlikeholdt.
- Skal sørge for at det avsettes tilstrekkelige ressurser til arbeidet med informasjonssikkerhet, herunder opplæring og kompetanseheving.

Kontroll og rapportering:

- Skal ha oversikt over de informasjonsverdiene som behandles av institusjonen, spesielt behandlingen av personopplysninger.
- Skal holde seg orientert om arbeidet med informasjonssikkerhet.
- Skal årlig gjennomgå status for arbeidet med informasjonssikkerhet ved Høgskolen i Innlandet (ledelsens gjennomgang).
- Skal årlig rapportere status for arbeidet med informasjonssikkerhet til høgskolestyret og informere styret om spesielt alvorlige sikkerhetsbrudd.
- Skal, dersom det er nødvendig, foreslå endringer i Ledelsessystemet (sikkerhetsmål, sikkerhetsstrategi, akseptabel risiko og organisering) til høgskolestyret.
- Skal godkjenne varslinger av brudd på sikkerheten ved behandling av personopplysninger til Datatilsynet.
- Skal godkjenne varslinger av brudd på sikkerheten ved behandling av personopplysninger til de registrerte.
- Rådføre seg med Høgskolen i Innlandet sin personvernrådgiver i spørsmål knyttet til informasjonssikkerhet i personvernsammenheng.

6.3 *CSO*

Myndighet og ansvar:

- Skal i det daglige utøve høgskoleledelsens ansvar for informasjonssikkerheten ved Høgskolen i Innlandet.
- Skal planlegge og lede arbeidet i informasjonssikkerhetsforumet ved Høgskolen i Innlandet.

Tilstand og oversikt:

- Skal ha oversikt over informasjonsverdier som behandles og IT-løsninger som benyttes ved Høgskolen i Innlandet.
- Skal holde seg orientert om informasjonssikkerhetstilstanden ved Høgskolen i Innlandet, herunder motta avviksmeldinger fra fakulteter, avdelinger, andre enheter, forskningsprosjekter og individuelle brukere (ansatte, studenter, gjester, osv.).
- Ajourføre en overordnet oversikt over sikkerhetstiltak ved Høgskolen i Innlandet i henhold rapportering fra ledere med ansvar for gjennomføring av risikovurderinger og etablering av sikringstiltak.

Revisjoner og rapporter:

- Skal sørge for at det gjennomføres revisjoner av arbeidet med informasjonssikkerhet ved fakulteter, avdelinger, andre enheter og forskningsprosjekter.
- Skal utarbeide rapport om informasjonssikkerhetsarbeidet til høgskoleledelsens årlige gjennomgang.
- Skal rapportere alvorlige brudd på informasjonssikkerheten og andre vesentlige avvik til Digitaliseringsdirektøren.

- Skal varsle Datatilsynet og de registrerte ved sikkerhetsbrudd som berører personopplysninger (etter godkjenning fra Digitaliseringsdirektøren).

Opplæring, informasjon og bistand:

- Skal sørge for at det gis opplæring i praktisk informasjonssikkerhetsarbeid til ledere, administrativt og vitenskapelige ansatte, prosjektledere og prosjektdeltakere i forskningsprosjekter dersom det er nødvendig.
- Skal bistå fakulteter, avdelinger og forskningsprosjekter ved planlegging, gjennomføringen og oppfølging av konkrete sikkerhetsoppgaver, spesielt risikovurderinger, iverksetting av sikringstiltak og inngåelser av avtaler med betydning for informasjonssikkerheten (SLA og liknende).
- Skal sørge for at brukerne informeres om trusler mot informasjonssikkerheten.
- Rådføre seg med Høgskolen i Innlandet sin personvernrådgiver i spørsmål knyttet til informasjonssikkerhet i personvernsammenheng.

6.4 *Informasjonssikkerhetsforum*

Myndighet og ansvar:

- Skal gi råd til høgskoleledelsen om tiltak/initiativ som fremmer informasjonssikkerheten, herunder ressursbehov.
- Skal koordinere planleggingen og gjennomføringen av tiltak/initiativ på informasjonssikkerhetsområdet som omfatter hele institusjonen.

Ledelse og sammensetning:

- Arbeidet planlegges og ledes av CSO.
- Forumet består for øvrig av vitenskapelige og administrative ledere/ansatte.
- Forumet møtes minst én gang hvert semester eller ved behov.

Øvrige oppgaver:

- Skal holde seg orientert om tilstanden på informasjonssikkerhetsområdet, herunder nye trusler mot Høgskolen i Innlandet sine informasjonsverdier.
- Skal gjennomgå meldte avvik og sikkerhetshendelser.
- Skal gjennomgå resultater fra sikkerhetsrevisjoner.
- Skal behandle eventuelle forslag til endringer i sikkerhetsmål, sikkerhetsstrategi, akseptkriterier og sikkerhetsorganisering i forkant av ledelsens gjennomgang.
- Skal foreslå konkrete mål for arbeidet med informasjonssikkerhet for neste periode (budsjettår) i forkant av ledelsens gjennomgang.

6.5 *Hendelseshåndteringsteam (IRT)*

Myndighet og delegasjon:

- Myndighet til selvstendig å iverksette nødvendige tiltak for å beskytte nettverk og IT-ressurser i forbindelse med IT sikkerhetshendelser.
- Monitorerer nettverksaktivitet for å forebygge, avdekke og håndtere tekniske sikkerhetsbrudd.

Primæroppgaver:

- Oppdage uregelmessigheter i nettet ved hjelp av egne alarmsystemer eller pålitelig varsling fra eksterne aktører.
- Vurdere alvorligheten av alarmer og varsler.
- Sørge for raskest mulig håndtering av alvorlige hendelser og effektiv håndtering av de mindre alvorlige.
- Bistå med å få oversikt over et oppdatert trusselbilde.
- Følge beste praksis for å beskytte seg, samt i noen utstrekning avdekke brudd på god praksis.
- Opprettholde en god og åpen kontakt med andre sikkerhetsteam i inn- og utland, samt relevante myndighetsinstanser.
- Informere IT-direktør og CSO om tekniske sikkerhetsbrudd ved behandling av personopplysninger som skal varsles til Datatilsynet og de registrerte.

6.6 *Fakultetsledelsen, ledere i sentraladministrasjonen og andre enhetsledere (forskningssentre, biblioteker, osv.)*

Myndighet og delegasjon:

- Skal, etter delegasjon fra Digitaliseringsdirektøren, utøve det daglige ansvaret for informasjonssikkerhet innenfor sine ansvarsområder, herunder IT-systemer/tjenester som de har eierskapet til.
- Skal sørge for at vedtatte sikkerhetsmål, kriterier for akseptabel risiko og sikkerhetsstrategi blir fulgt opp innenfor sine ansvarsområder.
- Kan delegere utøvelsen av det daglige ansvaret for informasjonssikkerheten til én eller flere ansatte ved fakultetet, avdelingen eller enheten.

Kartlegging, risikovurderinger og tiltak:

- Skal ha oversikt over hvilke informasjonsverdier og IT-løsninger enheten er ansvarlige for, inkludert hvilke forskningsdata som behandles.
- Skal sørge for at det jevnlig (hvert annet år) blir gjennomført risikovurderinger av:
  - IT-systemer/tjenester som enhetene har eierskap til.
  - Bruk av eksterne IT-systemer/tjenester (fjerndrift).
  - Bruk av IT-utstyr.
  - Arbeidsprosesser (forskning, undervisning, formidling og administrasjon).
  - Fysiske forhold som har betydning for informasjonssikkerheten.
  - Anskaffelse av IT-løsninger.
  - Ved vesentlige endringer i arbeidsprosesser, IT-løsninger eller fysiske forhold.

- Skal sørge for at sikringstiltak blir iverksatt dersom risikovurderingene viser at informasjonssikkerheten ikke er tilfredsstillende, herunder bestille tekniske og fysiske sikringstiltak fra IT- eller Eiendomsavdelingen.
- Rapportere plan for risikohåndtering (tiltaksplan) til CSO.

Informering og opplæring:

- Skal sørge for at administrativt og vitenskapelige ansatte med ansvar for konkrete sikkerhetsoppgaver og prosjektledere/deltakere har kompetanse til å utføre sine informasjonssikkerhetsoppgaver.
- Skal sørge for at alle brukere i sin enhet er kjent med de rutiner som til enhver tid gjelder for behandling av informasjonsverdier i administrasjon, undervisning, forskning og formidling.

Avviksmelding og avvikshåndtering:

- Skal sørge for at alle brukere i sin enhet er kjent med de prosedyrer som til enhver tid gjelder for melding av rutineavvik og sikkerhetsbrudd.
- Skal sørge for at alle avvik og sikkerhetsbrudd i sin enhet blir lukket, herunder be om assistanse fra IT- eller Eiendomsavdelingen ved håndtering av tekniske eller fysiske sikkerhetsbrudd dersom det er nødvendig.
- Skal informere CSO om sikkerhetsbrudd ved behandling av personopplysninger som skal varsles til Datatilsynet eller de registrerte.

Anskaffelser, avtaler og revisjoner:

- Skal sørge for at CSO får nødvendig bistand ved gjennomføring av sikkerhetsrevisjoner.
- Skal sørge for at krav til innebygd informasjonssikkerhet ivaretas ved anskaffelser av IT-løsninger.
- Skal sørge for at det inngås databehandleravtaler eller andre avtaler med eksterne aktører for å ivareta informasjonssikkerheten (for eksempel SLA), herunder kontrollere at avtalevilkårene respekteres.

6.7 *Forskningsansvarlig og prosjektledere i forskningsprosjekter*

6.7.1 Forskningsansvarlig

Myndighet og delegasjon:

- Prorektor for forskning er forskningsansvarlig og har det overordnede ansvaret for informasjonssikkerheten i forskningsprosjekter og har det juridiske ansvaret for behandling av personopplysninger i forskningsprosjekter.
- Prorektor for forskning delegerer utøvelsen av sitt ansvar for informasjonssikkerheten i forskningsprosjekter til faglig ledelse ved fakulteter eller tilsvarende enheter (dekan eller prodekan for forskning).
- Prorektor for forskning skal årlig gjennomgå status for arbeidet med informasjonssikkerhet i forskningsprosjekter ved Høgskolen i Innlandet (ledelsens gjennomgang).[5]

Oversikt og oppfølging:

- Skal ha som minimum ha en oversikt over hvilke forskningsprosjekter som behandler personopplysninger og som gjennomføres ved Høgskolen i Innlandet.
- Skal sørge for at vedtatte sikkerhetsmål, kriterier for akseptabel risiko og sikkerhetsstrategi blir fulgt opp i forskningsprosjekter.

[5] Prorektors gjennomgang av informasjonssikkerheten i forskningen bør koordineres med Digitaliseringsdirektørens årlige gjennomgang av institusjonens arbeid med informasjonssikkerhet. Dersom forskningsansvaret legges på fakultetsnivå, er det dekan/prodekan som har ansvaret for gjennomgangen av informasjonssikkerhet i forskningen på sitt fakultet. Resultatene fra gjennomgangen rapporteres til rektor.

6.7.2 Prosjektledere i forskningsprosjekter

Myndighet og ansvar:

- Skal sørge for at vedtatte sikkerhetsmål, kriterier for akseptabel risiko og sikkerhetsstrategi blir ivaretatt.
- Skal rapportere forskningsprosjekter til forskningsansvarlig ved Høgskolen i Innlandet.
- Skal, dersom det er nødvendig, melde forskningsprosjekter til lokalt personvernombud eller til Norsk Senter for Forskningsdata.

Kartlegging, risikovurderinger og tiltak:

- Skal ha oversikt over hvilke informasjonsverdier og IT-løsninger som behandles eller benyttes i forskningsprosjekter.
- Skal sørge for at det gjennomføres risikovurderinger ved oppstart av forskningsprosjekter og jevnlig ved langvarige prosjekter. Risikovurderingene bør omfatte prosjektets bruk av:
  - IT-systemer/tjenester – interne og eksterne – som anvendes i prosjektene.
  - IT-utstyr.
  - Fysiske forhold som har betydning for informasjonssikkerheten i forskningsprosjekter.
  - Anskaffelse av IT-løsninger i forskningsprosjekter.
  - Ved vesentlige endringer i forskningsprosjektet og endringer i IT-løsninger eller fysiske forhold.

- Skal sørge for at sikringstiltak blir iverksatt dersom risikovurderingene viser at informasjonssikkerheten i prosjektene ikke er tilfredsstillende, herunder bestille tekniske og fysiske sikringstiltak fra IT- og Eiendomsavdelingen.
- Rapportere plan for risikohåndtering (tiltaksplan) til CSO.

Informering og opplæring:

- Skal sørge for at prosjektdeltakere (ikke respondenter) har kompetanse til å utføre sine sikkerhetsoppgaver, for eksempel ved å be CSO om bistand til opplæring/kompetanseheving.
- Skal sørge for at alle prosjektdeltakerne er kjent med de rutiner som til enhver tid gjelder for behandling av informasjonsverdier i forskning.

Avviksmelding og avvikshåndtering:

- Skal sørge for at alle prosjektdeltakerne er kjent med de prosedyrer som til enhver tid gjelder for melding av rutineavvik og sikkerhetsbrudd.
- Skal sørge for at alle avvik og sikkerhetsbrudd blir lukket, herunder be om assistanse fra IT- eller Eiendomsavdelingen ved håndtering av tekniske eller fysiske sikkerhetsbrudd dersom det er nødvendig.
- Skal informere CSO om sikkerhetsbrudd ved behandling av personopplysninger som skal varsles til Datatilsynet eller de registrerte.

Anskaffelser, avtaler og revisjoner:

- Skal sørge for at CSO får nødvendig bistand ved gjennomføring av sikkerhetsrevisjoner av forskningsprosjekter.

- Skal sørge for at krav til innebygd informasjonssikkerhet ivaretas ved anskaffelser av IT-løsninger.
- Skal sørge for at det inngås databehandleravtaler eller andre avtaler med eksterne aktører i forskningsprosjekter for å ivareta informasjonssikkerheten (for eksempel SLA), herunder sikre at avtalevilkårene respekteres.

6.7.3 Spesielt for prosjektledere i medisinske eller helsefaglige forskningsprosjekter

- Skal følge de særskilte godkjennings- og saksbehandlingsreglene som gjelder ved oppstart, gjennomføring og avslutning av medisinske og helsefaglige forskningsprosjekter.[6]
- Skal følge anbefalingene i *Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren*, spesielt med hensyn til sikring av forskningsdata/forskningsfiler, koblingsnøkler og nøkkelfiler.[7]
- Skal foreta en risikovurdering og rådføre seg med HINNs personvernombud; NSD og Personvernombudet fro forskning og/eller REK hvis det skal foretas en vurdering av personvernkonsekvenser etter personvernforordning artikkel 34.

[6] Jf. https://helseforskning.etikkom.no/.

[7] Tilgjengelig på http://www.helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/dokumenter/veiledere/Documents/veileder_personvern-og-informasjonssikkerhet-i-forskningsprosjekter-v11.pdf

6.8 *IT-direktør*

Myndighet og delegasjon:

- IT-leder har det samme ansvaret for informasjonssikkerheten innenfor sin avdeling/ansvarsområde som øvrige ledere i sentraladministrasjonen, se instruks for fakultetsledelsen, ledere i sentraladministrasjonen og andre enhetsledere ovenfor.
- IT-leder skal sørge for at vedtatte sikkerhetsmål, kriterier for akseptabel risiko og sikkerhetsstrategi blir fulgt opp ved investeringer i og drift av IT-løsninger.

Registrering og dokumentasjon:

- Skal registrere og dokumentere autorisert og forsøk på uautorisert bruk av Høgskolen i Innlandet sine IT-løsninger som inneholder personopplysninger.
- Skal registrere og dokumentere alle sikkerhetshendelser/brudd som gjelder Høgskolen i Innlandet sine IT-løsninger.

Ekstern bistand og avtaler:

- Skal bistå enheter eller forskningsprosjekter ved risikovurderinger av teknisk sikkerhet (interne og eksterne IT-løsninger) når de blir bedt om å gi slik bistand.
- Skal bistå enheter eller forskningsprosjekter ved utforming og iverksetting av IT-tekniske sikringstiltak.
- Skal bistå enheter og forskningsprosjekter ved håndtering av tekniske sikkerhetsbrudd.
- Skal informeres om sikkerhetsbrudd som avdekkes av hendelseshåndteringsteamet (IRT) og som enten skal varsles til Datatilsynet eller de registrerte.

- Skal sørge for at det inngås databehandleravtaler eller andre avtaler med eksterne aktører som har betydning for informasjonssikkerheten (for eksempel SLA), herunder kontrollere at avtalevilkårene respekteres.

6.9 *Eiendomsdirektør*

Myndighet og delegasjon:

- Eiendomsdirektør har det samme ansvaret for informasjonssikkerheten innenfor sin avdeling/ansvarsområde som øvrige ledere i sentraladministrasjonen, se instruks for fakultetsledelsen, ledere i sentraladministrasjonen og andre enhetsledere ovenfor.
- Skal sørge for at vedtatte sikkerhetsmål og kriterier for akseptabel risiko blir fulgt opp ved nybygg eller bygningsmessige endringer som har betydning for informasjonssikkerheten.

Fysisk sikkerhet:

- Skal sørge for at sikring av tilgang til bygninger, rom og områder er i tråd med kriterier for akseptabel risiko.

Bistand og avtaler:

- Skal bistå enheter og forskningsprosjekter ved risikovurderinger av fysisk sikkerhet og ved gjennomføring av nødvendige fysiske sikringstiltak.
- Skal bistå enheter og forskningsprosjekter ved håndtering av fysiske sikkerhetsbrudd.
- Skal informere CSO om fysiske sikkerhetsbrudd som berører personopplysninger og som skal varsles til Datatilsynet eller de registrerte.
- Skal sørge for at det inngås databehandleravtaler eller andre avtaler med eksterne aktører som har betydning for informasjonssikkerheten (for eksempel SLA med vaktselskaper), herunder sikre at avtalevilkårene respekteres.

6.10 *Systemeier rollen*

6.10.1 Formål

Denne del av dokumentet definerer systemeiers ansvar ved høgskolen, og definerer forholdet til IT-avdelingen.

6.10.2 Hvem er systemeier

Rektor er den overordnede systemeier for alle IT-systemer ved institusjonen. Ettersom ansvaret for institusjonens prosesser og forvaltningsområder via en delegasjonsstruktur er delegert til avdelinger, fakulteter og enheter, er det naturlig at også systemeierskapet følger samme struktur.

I praksis vil det derfor være avdelingsdirektører, dekaner og enhetsledere som utøver systemeierskapet for det enkelte system. I dette dokumentet vil begrepet «systemeier» brukes om denne gruppa.

Systemeierskapet plasseres i linjeledelsen på laveste felles brukernivå. Systemeier er normalt øverste leder for den avdeling / enhet som bruker systemet, og har det overordnede juridiske og økonomiske ansvaret for et IKT-system.

Ansvaret for høgskolens fellessystemer er plassert i de ansvarlige stab-/støttefunksjoner. Økonomidirektør er for eksempel systemeier for institusjonens økonomisystem.

Systemeier kan utpeke navngitte operative representanter (kalt **systemansvarlige**) som ivaretar saksområdet i det daglige, og som gjerne har detaljert innsikt i systemet eierskapet omfatter.

For enkelte IT-systemer kan det i tillegg til systemansvarlig, være aktuelt å ha **superbrukere**. Superbrukere er spesielt dyktige brukere av et IT-system som hjelper den systemansvarlige med å ivareta opplæring og brukerstøtte.

6.10.3 Hva er systemeiers ansvar

Systemeier har overordnet ansvar for et IT-systems innhold og bruk i organisasjonen, herunder:

- Ansvar for at aktuelt forvaltningsområdes behov løses gjennom anvendelse av systemet. Det er påkrevd at systemeier har systemansvarlige som kjenner systemet godt og kan ivareta oppgaven med å få systemet til å løse oppgavene som tilligger det enkelte fagområdet.
- Vurdere faglige behov for, vurdere nytte av, realisere gevinster ved, samt fastsette retningslinjer for bruk av systemer innen eget ansvarsområde.
- Fastsette krav til systemfunksjonalitet og vurdere behov for funksjonelle endringer. Herunder nødvendig datautveksling med andre systemer.
- Ansvar for å sikre nødvendig datakvalitet i systemet.
- Ansvar for feil i systemet som ikke skyldes feil i teknisk infrastruktur, samt rapportering og oppfølging i forhold til leverandør.

- Oppfølgning av avtaler om anskaffelse/utvikling, vedlikehold og brukerstøtte. Systemeier har hovedkontakten med leverandøren og er ansvarlig for å holde dialogen med leverandør på de saker som måtte være aktuelle.
- Ansvar for opplæring i bruk og rutiner, samt organiseringen av dette.
- Ansvar for informasjonssikkerhet, med fokus på de organisatoriske sidene av sikkerhetsarbeidet. Iverksette rutiner i forhold til internkontrollsystem for informasjonssikkerhet, herunder risikovurderinger, avvikshåndtering, sikkerhets- og driftsrutiner. Systemeier ivaretar rollen «databehandlingsansvarlig» definert i Personopplysningsloven.
- Brukerstøtte av ikke-teknisk art.
- Ansvar for oppfyllelse av lovverk, forskrifter, retningslinjer og annen regelverk knyttet til bruk av systemet innenfor det aktuelle forvaltningsområdet.
- Ansvar for å beslutte hvilke brukere som skal ha tilgang og hvilken tilgang disse skal ha.
- Økonomisk ansvar for innkjøps-, vedlikeholds-, brukerstøtte-, konsulent- og prosjektkostnader. Dette kan også omfatte kostnader til infrastruktur der behovet er lokalt eller spesialisert og som går utover det som IT-avdelingen normalt håndterer.
- Ansvar for å avklare arkivfaglige forhold for systemet med Arkivleder.
- Ansvar for forretningskontinuitet ved at aktuelle tjenester kan drives videre, som regel gjennom manuelle rutiner, ved eventuelle feil på IT-løsning.
- Bistå i tvilstilfeller med å avklare hvorvidt det er feil i infrastruktur eller i systemet.
- Samarbeid med andre systemeiere. Delta i Hinn's systemeierforum.
- Innordne seg etter overordnede IT-styringsstrukturer besluttet av Digitaliseringsdirektøren/Rektor. Eksempler på slike rammebetingelser kan være arkitektur, datadefinisjoner, integrasjoner, informasjonssikkerhetspolicy og annet.

6.10.4 Hva gjør IT-avdelingen

IT-avdelinger er ansvarlig for den tekniske driften av IT-systemet i de tilfeller hvor driften ikke er satt bort til tredjepart / ekstern leverandør. Teknisk driftsansvar omfatter:

- Ansvar for drift av IT-teknisk infrastruktur. Dette innebærer også ansvaret for feil og
- feilkorrigering i infrastrukturen.
- Ansvar for oppgraderinger etter avtale med systemeier i de tilfeller hvor IT-avdelingen har kompetanse på dette.
- Ansvar for høyest mulig grad av kontinuerlig oppetid.
- Ansvar for at kompetent personell er tilgjengelig i feil-situasjoner og ved systemarbeid.
- Ansvar for sikkerhetskopiering. Systemeier kan ha krav om dette som avtales i hvert enkelt tilfelle.
- Ansvar for IT-teknisk brukerstøtte.
- Bistå i tvilstilfeller med å avklare hvorvidt det er feil i infrastruktur eller i systemet.
- IT-teknisk støtte med tekniske vurderinger og råd der dette er naturlig i hele prosessen fra planlegging og kravspesifikasjon til avvikling og utfasing av et system. Dette inkluderer kostnadsberegninger av teknisk infrastruktur uavhengig av hvem som finansierer dette.
- Støttefunksjon i leverandørkontakten og kan der det er hensiktsmessig også følge opp saker og deler av dialogen i forståelse med systemeier.
- Teknisk implementering av løsninger, som installasjoner, oppgraderinger og tilpasninger.
- Ansvar for teknisk informasjonssikkerhet. Ivaretar rollen som «databehandler» definert i Personopplysningsloven. Bidra ved gjennomføring av risikovurderinger.
- Ansvar for å gjennomgå ansvar og oppgaver for systemforvaltning med nye systemeiere og systemansvarlige.

6.11 *Brukerne (ansatte, studenter, gjester, osv.)*

Ansvar:

- Alle brukere skal overholde de rutiner og retningslinjer som til enhver tid gjelder for sikker håndtering av informasjonsverdier og personopplysninger.

Oppgaver:

- Alle brukere skal rapportere avvik fra vedtatte rutiner/retningslinjer og brudd på informasjonssikkerheten.
- Ansatte skal bistå ved planlegging, gjennomføring eller oppfølging av konkrete sikkerhetsoppgaver dersom de blir bedt om det.