

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 1 av 20

Innhold

1	INNLEDNING	2
1.1	Risikostyring	2
1.2	Krav til Ledelsessystem for informasjonssikkerhet	3
2	AVGRENSNING	4
3	SIKKERHETSMÅL	5
3.1	Overordnet mål for sikkerhet ved HiMolde	5
3.2	Mål for ulike sikkerhetsområder	5
4	KRITERIER FOR AKSEPTABEL RISIKO	6
4.1	Åpen informasjon	6
4.2	Intern informasjon	6
4.3	Sensitiv informasjon	7
4.4	Akseptabel risiko for materielle verdier	8
5	SIKKERHETSSTRATEGI	9
5.1	Risikovurderinger	9
5.2	Opplæring og kompetanseheving	9
5.3	Lederansvar	10
5.4	Informasjon til brukere	10
5.5	Fjerndrift og utkontraktering	10
5.6	Andre overordna prioriteringer	10
6	SIKKERHETSORGANISASJON	11
6.1	Høgskolestyret	11
6.2	Høgskoledirektøren	11
6.3	CSO (Chief Security Officer)	12
6.4	Informasjonssikkerhetsforum:	14
6.5	Avdelingsledere	15
6.6	Forskningsansvarlig og prosjektledere i forskningsprosjekter:	16
6.7	IT-leder:	19
6.8	Brukerne (ansatte, studenter, gjester, osv.):	20

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 2 av 20

1 INNLEDNING

Kjernevirksomheten til Høgskolen i Molde (heretter kalt HiMolde) er (a) å tilby forskningsbasert utdanning av internasjonal kvalitet både innenfor satsningsområdene logistikk, sport og event management og helse/sosialfag, og innenfor fagområder som skal støtte den faglige spissingen og (b) bidra til kunnskapsutvikling, innovasjon og verdiskapning gjennom formidling, utdanning, faglig utviklingsarbeid og forskning.

Det betyr at HiMolde i stor grad lever av å forvalte, foredle og formidle ikke-materielle verdier. Derfor er det også avgjørende at all informasjon som HiMolde forvalter i administrasjon, forskning, undervisning og offentlig formidlingsarbeid er tilfredsstillende sikret mot brudd på:

- **Konfidensialiteten:** Informasjon og informasjonssystemer skal bare være tilgjengelig for de som skal ha tilgang
- **Integriteten:** Informasjon og informasjonssystemer skal være korrekte, gyldige og fullstendige
- **Tilgjengeligheten:** Informasjon og informasjonssystemer skal være tilgjengelige innenfor fastsatte tilgjengelighetskrav

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

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 3 av 20

informasjonssikkerhetsarbeid er derfor å forutse og forebygge uønskede hendelser og avvik før de oppstår.

Vårt risikostyrte informasjonssikkerhetsarbeid er forankret i høgskolens toppledelse.

Arbeidet utføres av en sikkerhetsorganisasjon med egne mål, strategier, arbeidsmetodikk/redskaper og ressurser. Medarbeiderne som utgjør sikkerhetsorganisasjonen blir utpekt av høgskoledirektøren.

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 HiMolde. I tillegg inneholder andre lovverk, blant annet offentlighetsloven og arkivloven, bestemmelser som har betydning for arbeidet med sikring av informasjon ved HiMolde.

I Kunnskapsdepartementets (KD) tildelingsbrev til Høgskolen i Molde kreves det innføring av et Ledelsessystem for informasjonssikkerhet (SSIS) bygget på grunnprinsippene i anerkjente sikkerhetsstandarder.¹ For å bistå oss i dette arbeidet har KD gitt UNINETT i mandat å opprette Sekretariatet for informasjonssikkerhet i UH-sektoren. HiMolde skal rapportere til KD hvordan vi bruker denne interne tjenesten.

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

¹ Tildelingsbrevet 2016 tilgjengelig på

<https://www.regjeringen.no/contentassets/d5cc2f23a57040b792ab06100f57f0f0/tildelingsbrev-him-2016---l997733.pdf>

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 4 av 20

2 AVGRENSNING

Styringssystemet for informasjonssikkerhet ved HiMolde omfatter

- alle ansatte, registrerte studenter, alt innleid personell og gjester
- alle lokasjoner hvor HiMolde har aktivitet; Molde, herunder Høgskolesenteret i Kristiansund og andre steder der medarbeidere utfører arbeid for HiMolde
- alle informasjonsverdier som høgskolen håndterer, for eksempel personopplysninger, forskningsdata- og registre, manuelle registre osv.
- alle materielle og tekniske verdier, for eksempel IT-systemer, teknisk og fysisk infrastruktur og bygninger som eies eller leies av Høgskolen i Molde

HMS-arbeidet omfattes ikke av styringssystem for informasjonssikkerhet. Økonomi- og personalavdelinga har systemansvar for helse-, miljø- og sikkerhetsarbeidet ved HiMolde.

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 5 av 20

3 SIKKERHETSMÅL

Følgende mål for arbeidet med informasjonssikkerhet gjelder ved Høgskolen i Molde

3.1 Overordnet mål for sikkerhet ved HiMolde

- Sikkerhetsarbeidet skal bidra til god kvalitet på undervisning, forskning, formidling og administrasjon. Arbeidet skal også bidra til å sikre robust drift av høgskolen.
- Lov og myndighetskrav skal være oppfylt

3.2 Mål for ulike sikkerhetsområder

3.2.1 Informasjonssikkerhet

- Høgskolens informasjon skal være tilgjengelig, korrekt og ikke komme på avveie.
- Rettighetene og personvernet til studenter, tilsatte, forskningsobjekter og eventuelt andre som høgskolen mottar informasjon om skal ivaretas.

3.2.2 IKT-sikkerhet

- Høgskolens IKT-løsninger skal være tilfredsstillende fysisk og logisk sikret.
- IKT-angrep skal avdekkes og håndteres slik at skadeomfang begrenses og normaltilstand gjenopprettes raskt.

3.2.3 Fysisk sikring

Høgskolens verdier skal være tilfredsstillende sikret mot brann, tyveri og skadeverk og lokalene skal være sikret mot uautorisert adgang.

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 6 av 20

4 KRIITERIER FOR AKSEPTABEL RISIKO

For å oppnå tilfredsstillende informasjonssikkerhet skal arbeidet baseres seg på kriterier for akseptabel risiko. Arbeidet med informasjonssikkerhet skal sørge for at informasjonsverdiene ved HiMolde 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

Åpen informasjon er informasjon som ikke skal skjermes mot offentligheten. Integriteten og tilgjengeligheten til informasjon som skal være offentlig tilgjengelig skal prioriteres. Integriteten til informasjonen skal vektlegges foran hensynet til tilgjengeligheten.

Eksempler på åpen informasjon er publiserte forskningsresultater, generell informasjon om studietilbudet eller annen informasjon som er tilgjengelig på www.himolde.no

4.2 Intern informasjon

Intern informasjon er informasjon med et beskyttelsesbehov som gjør at den ikke skal være åpent tilgjengelig for offentligheten. Er beskyttelsesbehovet sterkt i forhold til integritet og/eller konfidensialitet, kalles informasjonen sensitiv (se neste punkt).

Konfidensialiteten og integriteten til informasjon som benyttes i intern administrasjon og saksbehandling eller i pågående eller planlagt forskning/studentforskning skal prioriteres høyt. For intern informasjon aksepteres

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 7 av 20

ikke brudd på konfidensialiteten. Kortere avbrudd i informasjonens tilgjengelighet kan normalt aksepteres.

Eksempler på intern informasjon er 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.

4.3 Sensitiv informasjon

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

Eksempel på sensitiv informasjon er konfidensielle forskningsdata, opplysninger om enkeltpersoner (personopplysninger²) eller forslag/tekster til eksamensoppgaver.

- Det aksepteres ikke brudd på konfidensialiteten eller integriteten til personopplysninger. Dette gjelder i særlig grad for sensitive personopplysninger.³ Kortere avbrudd i personopplysningers tilgjengelighet aksepteres. Eksempler på sensitive personopplysninger er skikkethets- og fuskesaker, forskningsdata som inneholder sensitive personopplysninger, disiplinærsaker, saker vedrørende oppfølging av sykdom, varslingsaker, politiattestsaker, utestengningssaker.
- Det aksepteres ikke brudd på konfidensialiteten og integriteten til konfidensielle forskningsdata som ikke er godkjent for

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

³ 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.

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 8 av 20

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.
- Det aksepteres ikke brudd på integriteten eller tap av informasjon om karakterer og vitnemål.
- Det aksepteres ikke brudd på integriteten på opptaksgrunnlag og resultater, tilsetningsgrunnlag eller på økonomiske transaksjoner.
- Det aksepteres ikke brudd på integriteten i autentiseringsgrunnlag for tilganger til sensitiv informasjon eller avlåste lokaler.

4.4 Akseptabel risiko for materielle verdier

Det aksepteres ikke at spesialrom eller eiendeler med høy verdi ikke er tilfredsstillende sikret. Eksempler på dette er:

- Serverrom
- Rom med verdifullt spesialutstyr som øvingsavdelingen
- Verdifull kunst

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 9 av 20

5 SIKKERHETSSTRATEGI

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

5.1 Risikovurderinger

Vårt arbeid med informasjonssikkerhet skal basere seg på risikovurderinger. Normalt skal sikringstiltak, uavhengig av om de er tekniske, organisatoriske, fysiske eller personalmessige, ikke 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 jevnlig, ved behov og i forbindelse med vesentlige endringer. Valg av sikringstiltak skal basere seg på ISO-standarder og anbefalinger/veiledninger fra Uninett og norske forvaltningsorganer på området.

5.2 Opplæring og kompetanseheving

Ledelsen ved HiMolde vil bevilge nødvendige ressurser til opplæring og kompetanseheving for ledere og ansatte som er delegert ansvar for informasjonssikkerheten ved høgskolen 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.

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 10 av 20

5.3 Lederansvar

Ledere 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.

5.4 Informasjon til brukere

Alle brukere skal gis informasjon om rutiner for sikker håndtering av informasjonsverdier og trusler mot informasjonsverdiene. De skal også informeres om avviksmeldingssystemet som beskrives i gjennomførende del. I tillegg skal de informeres om hensikten med og viktigheten av at avvik/sikkerhetsbrudd rapporteres.

5.5 Fjerndrift og utkontraktering

Fjerndrift av HiMolde 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 av drift og forvaltning av informasjon med særskilte sikkerhetskrav, for eksempel sensitive personopplysninger eller konfidensielle forskningsdata, kan bare skje etter en spesielt grundig vurdering.

5.6 Andre overordna prioriteringer

Arbeidet med informasjonssikkerhet ved høgskolen skal til enhver tid basere seg på anbefalte og anerkjente standarder for styring av informasjonssikkerhet i offentlig sektor.

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

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 11 av 20

6 SIKKERHETSORGANISASJON

HiMoldes sikkerhetsorganisasjon består av:

6.1 Høgskolestyret

Myndighet:

- Behandler og vedtar Ledelsessystemet for informasjonssikkerhet ved HiMolde og vesentlige endringer i Ledelsessystemet.
- Kan stille krav til arbeidet med informasjonssikkerhet ved HiMolde

Rapportering:

- Skal i årsrapporten informeres om arbeidet med informasjonssikkerhet av høyskoledirektøren
- Skal informeres om spesielt alvorlige sikkerhetsbrudd av høyskoledirektøren.

6.2 Høgskoledirektøren

- Har det overordnede ansvaret for informasjonssikkerheten ved HiMolde.
- Oppnevner medlemmer av informasjonssikkerhetsforumet ved HiMolde.
- Kan delegere ansvaret for utøvelsen av daglige oppgaver til CSO.
- Skal inngå avtaler med eksterne aktører (databehandlere) som behandler personopplysninger på vegne av HiMolde.
- Skal sørge for at Ledelsessystemet for informasjonssikkerhet blir innført, satt i drift og vedlikeholdt.

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 12 av 20

- 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 HiMolde (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 meddele rektor alvorlige brudd på konfidensialiteten til personopplysninger til Datatilsynet.

6.3 CSO (*Chief Security Officer*)

- Utøver det daglige ansvaret for informasjonssikkerhet HiMolde.
- Skal planlegge og lede arbeidet i informasjonssikkerhetsforumet ved HiMolde.
- Skal ha oversikt over informasjonsverdier som behandles og IT-løsninger som benyttes ved HiMolde.

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 13 av 20

- Skal holde seg orientert om informasjonssikkerhetstilstanden ved HiMolde, herunder motta avviksmeldinger fra avdelingene, forskningsprosjekter og individuelle brukere (ansatte, studenter, gjester, osv.).
- Skal sørge for at det gis opplæring i praktisk informasjonssikkerhetsarbeid til ledere, administrativt og vitenskapelige ansatte.

Byggsikkerhet :

- Skal sørge for at vedtatte sikkerhetsmål og kriterier for akseptabel risiko blir fulgt opp ved nybygg eller bygningsmessige endringer som har betydning for informasjonssikkerheten.
- 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.

Revisjoner og rapporter:

- Skal sørge for at det gjennomføres revisjoner av arbeidet med informasjonssikkerhet.
- Skal utarbeide rapport om informasjonssikkerhetsarbeidet til høgskoleledelsens årlige gjennomgang.
- Skal rapportere alvorlige brudd på informasjonssikkerheten og andre vesentlige avvik til høgskoledirektøren.

Opplæring, informasjon og bistand:

- Skal bistå avdelinger og forskningsprosjekter ved planlegging, gjennomføring og oppfølging av konkrete sikkerhetsoppgaver, spesielt risikovurderinger,

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 14 av 20

iverksetting av sikringstiltak og inngåelser av avtaler med betydning for informasjonssikkerheten (SLA (tjenesteavtaler) og liknende).

- Skal sørge for at brukerne informeres om trusler mot informasjonssikkerheten.

6.4 Informasjonssikkerhetsforum:

- 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 HiMolde 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.

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 15 av 20

- Skal foreslå konkrete mål for arbeidet med informasjonssikkerhet for neste periode (budsjettår) i forkant av ledelsens gjennomgang.

6.5 Avdelingsledere

- Skal 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.
- 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.

Kartlegging, risikovurderinger og tiltak:

- Skal ha oversikt over hvilke informasjonsverdier og IT-løsninger enheten er ansvarlige for, inkludert hvilke forskningsdata som behandles.
- Skal gjennomføre risikovurderinger og iverksette tiltak der det er nødvendig for å ivareta informasjonssikkerheten.
- Skal sørge for at sikringstiltak blir iverksatt dersom risikovurderingene viser at informasjonssikkerheten ikke er tilfredsstillende.
- Skal rapportere resultat fra risikovurderinger til CSO.
- 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.

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 16 av 20

- Skal sørge for at alle avvik og sikkerhetsbrudd i sin enhet blir lukket, herunder be om assistanse fra IT- eller ØP ved håndtering av tekniske eller fysiske sikkerhetsbrudd dersom det er nødvendig.

6.6 Forskningsansvarlig og prosjektledere i forskningsprosjekter:

6.6.1 Forskningsansvarlig (rektor)

- Rektor er forskningsansvarlig og har det overordnede ansvaret for informasjonssikkerheten i forskningsprosjekter.
- Rektor delegerer utøvelsen av sitt ansvar for informasjonssikkerheten i forskningsprosjekter til faglig ledelse ved avdelingene (dekan).
- Rektor skal ha oversikt over hvilke forskningsprosjekter som gjennomføres ved HiMolde.
- Skal sørge for at vedtatte sikkerhetsmål, kriterier for akseptabel risiko og sikkerhetsstrategi blir fulgt opp i forskningsprosjekter.

6.6.2 Prosjektledere i forskningsprosjekter

- Skal sørge for at vedtatte sikkerhetsmål, kriterier for akseptabel risiko og sikkerhetsstrategi blir ivaretatt.
- Skal, dersom det er nødvendig, melde forskningsprosjekter til Personvernombudet for forskning.
- Skal ha oversikt over hvilke informasjonsverdier og IT-løsninger som behandles eller benyttes i forskningsprosjekter.

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 17 av 20

- 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 drøfte tekniske og fysiske sikringstiltak fra IT- og ØP.
- 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.

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 18 av 20

6.6.3 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.⁴
- Skal følge anbefalingene i *Personvern og informasjonssikkerhet i forskningsprosjekter innenfor helse- og omsorgssektoren*, spesielt med hensyn til sikring av forskningsdata/forskningsfiler, koblingsnøkler og nøkkelfiler.⁵

⁴ Jf. <https://www.etikkom.no/>.

⁵ Tilgjengelig på http://www.helsedirektoratet.no/lover-regler/norm-for-informasjonsikkerhet/dokumenter/veiledere/Documents/veileder_personvern-og-informasjonsikkerhet-i-forskningsprosjekter-v11.pdf.

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 19 av 20

6.7 IT-leder:

- IT-leder har det samme ansvaret for informasjonssikkerheten innenfor sin avdeling/ansvarsområde som øvrige avdelingsledere, se over.
- 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.

I tillegg

- Skal registrere og dokumentere autorisert og forsøk på uautorisert bruk av HiMoldes IT-løsninger som inneholder personopplysninger.
- Skal registrere og dokumentere alle sikkerhetshendelser/brudd som gjelder HiMoldes IT-løsninger.
- Skal bistå avdelinger og forskningsprosjekter ved risikovurderinger av teknisk sikkerhet (interne og eksterne IT-løsninger).
- Skal bistå avdelinger og forskningsprosjekter ved utforming og iverksetting av IT-tekniske sikringstiltak.
- Skal bistå avdelinger og forskningsprosjekter ved håndtering av tekniske sikkerhetsbrudd.

Byggsikkerhet:

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

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET Styrende dokumenter	Godkjent dato: 14.12.2016 Versjon: 1.00
STYRENDE DEL		Side 20 av 20

6.8 Brukerne (ansatte, studenter, gjester, osv.):

- Alle brukere skal overholde de rutiner og retningslinjer som til enhver tid gjelder for sikker håndtering av informasjonsverdier og personopplysninger.
- Alle brukere skal rapportere avvik fra vedtatte rutiner/retningslinjer og brudd på informasjonssikkerheten.

Dokumentref: 16/00802-10	Dokumentansvarlig: Randi Gammelsæter
Filnavn: Styrende del	