

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET	Godkjent dato: 08.03.2018 Versjon: 1.00
GJENNOMFØRENDE DEL		Side 1 av 7

Innhold

1	HØGSKOLENS INFORMASJONSVERDIER	2
1.1	Våre informasjonsverdier	2
1.2	Klassifisering av informasjon ved HiMolde	2
1.3	Kartlegging.....	3
2	ÅRSPLAN – INFORMASJONSSIKKERHET	4
2.1	Faste aktiviteter som gjennomføres årlig	4
2.2	Aktiviteter 2017 – 2018.....	5
3	RISIKOVURDERING.....	5
3.1	Innledning.....	5
3.2	Metodikk	6
3.3	Når skal risikovurdering gjennomføres.....	6
3.4	Dokumentasjon.....	6
3.5	Kontroll og revisjon	6
4	RISIKOHÅNTERINGSPLAN - SIKRINGSTILTAK	6
4.1	Risikohåndteringsprosedyre	6
4.2	Tiltaksplan.....	7

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

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET	Godkjent dato: 08.03.2018 Versjon: 1.00
GJENNOMFØRENDE DEL		Side 2 av 7

1 HØYSKOLENS INFORMASJONSVERDIER

1.1 Våre informasjonsverdier

HiMolde forvalter svært store mengder informasjon. Mye av informasjonen er intern, og skal kun være tilgjengelig for de som har tilgangsstrettigheter. Eksempler på slik informasjon er personopplysninger og karakteropplysninger. Det vil kunne være til stor skade for høyskolen og de personer informasjonen gjelder om denne informasjonen blir kjent for uvedkommende.

HiMolde skal derfor til enhver tid ha god oversikt over den informasjon vi forvalter. Våre system og rutiner skal sikre at informasjonen blir behandlet og lagret i tråd med gjeldende regelverk og sikre informasjonen mot brudd på konfidensialitet, integritet og tilgjengelighet.

1.2 Klassifisering av informasjon ved HiMolde

Følgende klassifisering gjelder for HiMoldes informasjonsverdier:

KONFIDENSIALITET

Åpen informasjon – Informasjonen kan være tilgjengelig for alle uten særskilte tilgangsstrettigheter.

Intern informasjon – Informasjonen må ha en viss beskyttelse, men kan være tilgjengelig for både interne og eksterne brukere med kontrollerte tilgangsstrettigheter.

Fortrolig / Sensitiv informasjon – Informasjonen er særlig beskyttelsesverdig og skal ha de strengeste tilgangsstrettigheter.

INTEGRITET

Hvis informasjonen kun skal kunne endres av bestemte personer, må den sikres spesielt gjennom krav til pålogging, skrivebeskyttelse og/eller logging.

Ved HiMolde har vi følgende krav til beskyttelse av informasjonens integritet:

Strengt krav til integritet: En-faktor autentisering

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

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET	Godkjent dato: 08.03.2018 Versjon: 1.00
GJENNOMFØRENDE DEL		Side 3 av 7

Ekstra strengt krav til integritet: To-faktor autentisering, evt også logging, og/eller skrivebeskyttelse

Det er viktig at all informasjon som HiMolde står ansvarlig for er korrekt, men noen eksempler på informasjon der integriteten er spesielt viktig er søknadsfrister og karakterer.

TILGJENGELIGHET

Strengt krav – klasse 1

Informasjonen skal i utgangspunktet være tilgjengelig 24/7, hele året igjennom, men kortere avbrudd i tilgjengelighet (inntil 1 time mellom kl 08-16 på arbeidsdager) kan normalt aksepteres. Utenom dette tidsrommet kan også mer langvarige avbrudd i tilgjengelighet aksepteres. Dette gjelder ikke i spesielle perioder, som ved eksamensavvikling og i opptaksperioder, der avbrudd i tilgjengelighet utover 1 time likevel ikke kan aksepteres.

Mindre strengt krav – klasse 2

Informasjonen skal i utgangspunktet være tilgjengelig 24/7, hele året igjennom, men kortere avbrudd i tilgjengelighet (inntil 4 timer mellom kl 08-16 på arbeidsdager) kan aksepteres. Utenom dette tidsrommet kan også mer langvarige avbrudd i tilgjengelighet aksepteres.

Unntak fra kravene til tilgjengelighet kan være nødvendig ved planlagt vedlikehold, systemoppgradering eller i andre tilfeller. I slike tilfeller skal nedetid planlegges nøye og informasjon gis, slik at ulempene for brukerne blir så små som mulige.

1.3 Kartlegging

En kartlegging av informasjonsverdier innebærer å få en tilstrekkelig oversikt over informasjon som høyskolen håndterer. Særlig sentralt er det å ha oversikt over informasjon som er omfattet av spesielt regelverk for informasjonssikkerhet eller som er av så vesentlig betydning for virksomhetens mål for informasjonssikkerhet at de bør omfattes av risikovurderinger.

Vår kartlegging av informasjon tar utgangspunkt i Uninett sitt forslag til informasjonsklassifisering i «Retningslinjer for klassifisering av informasjon».

Oversikt over høyskolens informasjonsverdier finnes som vedlegg. Kartleggingen gjennomgås og oppdateres årlig av CSO.

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

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET	Godkjent dato: 08.03.2018 Versjon: 1.00
GJENNOMFØRENDE DEL		Side 4 av 7

2 ÅRSPLAN – INFORMASJONSSIKKERHET

Gjennomføring av aktivitetene som er satt opp i årsplanen skal understøtte HiMoldes overordnede sikkerhetsmål og sikkerhetsstrategi.

Gjennom faste tiltak og aktiviteter sikrer vi at medarbeidere og studenter har tilstrekkelig kompetanse, at risikovurderinger blir gjennomført og at arbeidet med informasjonssikkerhet blir prioritert i organisasjonen.

Årsplanen er et viktig arbeidsverktøy for den som til daglig utøver ledelsens ansvar for informasjonssikkerhet ved HiMolde.

I tillegg til institusjonens overordnede sikkerhetsmål og strategi, vil svakheter eller mangler ved ledelsessystemet avdekket under «Ledelsens gjennomgang» kunne påvirke innholdet i årsplanen.

2.1 Faste aktiviteter som gjennomføres årlig

Sikkerhetsmål (Styrende del)	Tiltak	Ansvar	Frist for gjennomføring
3.2.1 3.2.2 3.2.3	Opplæring - Opplæring av alle nytilsatte (som en del av introduksjon av nytilsatte) - Opplæring av nye studenter	CSO Studie-sjef	15.9 (i tillegg ved andre oppstartstids-punkt)
3.1 3.2.1 3.2.2	Risikovurdering - Årlig overordnet ROS – identifisere og vurdere overordnede risikoer. - Årlige system-/prosess ROS – minimum to risikovurderinger for å avdekke risikoer i informasjonssystem og/eller arbeidsprosesser	Direktør CSO	15.3 Fastsettes i årlig årsplan. Tidspunkt avhenger av praktiske forhold.

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

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET	Godkjent dato: 08.03.2018 Versjon: 1.00
GJENNOMFØRENDE DEL		Side 5 av 7

3.1	Informasjonstiltak Årlig delta på nasjonal sikkerhetsmåned og benytte opplæringsmaterieell fra denne	CSO	31.10.
3.1	Revisjon / ledelsens gjennomgang Årlig gjennomgang og revisjon av ledelsessystemet	Direktør	15.3

2.2 Aktiviteter 2018

Målsetting (Styrende del)	Tiltak	Ansvar	Frist for gjennomføring
3.2.1	Systemarbeid		
3.2.2	Etablering av gjennomførende og kontrollerende del av ledelsessystem for info.sikkerhet	Direktør	08.03.2018
3.2.2	Etablering av avvikssystem	CSO / IT-sjef	15.03.2018
3.2.2	Opplæring Opplæring av alle medarbeidere i bruk av avviksmelding	CSO	15.03.2018
3.2.1	Risikovurderinger		
3.2.2.	Sensur-/eksamensbehandling	CSO	01.03.2018
	Canvas – innføring		01.04.2018

3 RISIKOVURDERING

3.1 Innledning

Institusjonens arbeid med informasjonssikkerhet skal ha en risikobasert tilnærming. Se ledelsessystemets styrende del, punkt 5.1. Ledelsessystemets beskrivelse av sikkerhetsorganisasjonen, styrende del punkt 6, beskriver hvem som har ansvaret for at risikovurdering blir gjennomført.

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

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET	Godkjent dato: 08.03.2018 Versjon: 1.00
GJENNOMFØRENDE DEL		Side 6 av 7

3.2 Metodikk

Risikovurderinger skal gjennomføres ved bruk av felles metodikk og maler.

HiMolde bruker Uninett sitt rammeverk for gjennomføring av risikovurderinger.

[Informasjon til deg som skal delta i en risikovurdering](#)

[Risikovurderingsmatrise og verdier](#)

[Mal for risikovurderinger](#)

3.3 Når skal risikovurdering gjennomføres

Risikovurderinger skal gjennomføres før elektroniske tjenester eller systemer tas i bruk.

Risikovurderinger skal gjennomføres ved vesentlige endringer i elektroniske tjenester/systemer eller i bruken av dem.

Risikovurderinger av elektroniske tjenester eller systemer skal revideres ved større endringer, ellers hvert tredje år.

3.4 Dokumentasjon

Risikovurderinger skal dokumenteres og arkiveres i P360.

3.5 Kontroll og revisjon

Gjennomførte risikovurderinger evalueres ved ledelsens årlige gjennomgang.

4 RISIKOHÅNDTERINGSPLAN - SIKRINGSTILTAK

4.1 Risikohåndteringsprosedyre

Det følger av sikkerhetsorganiseringen ved HiMolde at avdelingsledere (dekaner og administrative ledere) og prosjektledere i forskningsprosjekter har ansvaret for å iverksette tiltak mot sikkerhetsbrudd.

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

 Høgskolen i Molde Vitenskapelig høgskole i logistikk	LEDELSESSYSTEM FOR INFORMASJONSSIKKERHET	Godkjent dato: 08.03.2018 Versjon: 1.00
GJENNOMFØRENDE DEL		Side 7 av 7

Følgende prosedyre gjelder ved iverksetting av sikringstiltak:

1. Sikringstiltak skal iverksettes dersom risikovurderingen avdekker at informasjonsverdier er utsatt for en uakseptabel høy risiko for brudd på konfidensialiteten, integriteten eller tilgjengeligheten, jf. kriterier for akseptabel risiko ved HiMolde.
2. Nødvendige sikringstiltak skal iverksettes uten ubegrunnet opphold etter at resultatet av risikovurderingen foreligger.
3. Vedkommende avdeling eller forskningsprosjekt som har gjennomført risikovurderingen bærer de kostnader som påløper ved iverksetting av nødvendige sikringstiltak.
4. Sikringstiltak skal rapporteres til CSO/personvernrådgiver så fort vedtak om iverksettelse er fattet. Malen under brukes.
5. CSO/personvernrådgiver rapporterer iverksatte sikringstiltak til ledelsen ved HiMolde i forbindelse med ledelsens gjennomgang.

4.2 Tiltaksplan

Risiko som skal reduseres	Ansvarlig for tiltak	Tiltak som skal iverksettes	Frist	Finansiering
Vurdere passordpolicy	Sikkerhetsforum	Vurdere innføring av tofaktor pålogging og tvungen skifte av passord	30.6.2018	

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