HØGSKULEN
I VOLDA

Styringssystem for informasjonssikkerhet ved

Høgskulen i Volda

Basert på ISO/IEC 270001/02: 2013

1 Innhold

Innledning

Fra strategiplanen for Høgskulen i Volda (heretter omtalt som HVO):

> ***VISJON***
> *Kompetanse for framtida.*
>
> ***IDENTITET OG VERDIAR***
> *Høgskulen i Volda (HVO) er tufta på ein lang folkeopplysningstradisjon frå 1700-talet – med lærarutdanning frå 1860-åra og distriktshøgskule frå 1970. Vi vil halde høgt verdiar som tillit, respekt, openheit, demokrati og ærleg framferd. HVO skal vere inkluderande, relevant og uavhengig.*
>
> ***PROFIL***
> *HVO er høgskulen for human- og samfunnsvitskapane i Møre og Romsdal, og dei nasjonale satsingsområda våre er:*
> *- Yrkesretta medieutdanning*
> *- Nynorsk i utdanning, forsking og formidling*
> *- Fleksible vidareutdanningstilbod*

HVO lever med andre ord i stor grad av å forvalte, foredle og formidle ikke-materielle verdier, og derfor er det også avgjørende at all informasjon som HVO forvalter i administrasjon, forskning, undervisning og offentlig formidlingsarbeid er tilfredsstillende sikret mot brudd på:

Konfidensialitet:	hindre at uvedkommende får tilgang til konfidensiell eller sensitiv informasjon,
Integritet:	hindre uønsket endring, sletting eller manipulering av informasjon og
Tilgjengelighet:	sikre brukere tilgang til informasjon når de har behov for det.

Personopplysningsloven med forskrift, forvaltningsloven med forskrift (e-forvaltnings-forskriften) og helseforskningsloven med forskrift stiller krav til innføring av styringssystem for informasjonssikkerhet (SFI). I tillegg inneholder andre lovverk, blant annet offentlighetsloven og arkivloven, bestemmelser som har betydning for arbeidet med sikring av informasjon ved HVO. I Kunnskapsdepartementets (KD) tildelingsbrev til HVO kreves det innføring av SFI bygget på grunnprinsippene i anerkjente sikkerhetsstandarder. SFI ved HVO ivaretar de kravene som lovverket og Kunnskapsdepartementet stiller til arbeidet med informasjonssikkerhet i UH-institusjoner.

2 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 det iverksettes tiltak for å unngå uønskede hendelser som vurderes å ha størst risiko. Risikostyrt informasjonssikkerhetsarbeid skal forankres i toppledelsen. Arbeidet skal ha egne mål, strategier, arbeidsmetodikk/redskaper, ressurser og forankres i den daglige driften ved HVO

2.1 Styringssystem for informasjonssikkerhet (SFI) ved HVO

Dette dokumentet beskriver de overordnede prinsippene for SFI, med beskrivelser av organisering av arbeidet, roller og ansvar samt oversikt over informasjonsverdier og retningslinjer.

Dokumentet beskriver systemets tre hovedelementer:

1. Styrende – overordnet policy, sikkerhetsmål og –strategi, roller og ansvar
2. Gjennomførende – risikovurderinger, rutiner og retningslinjer
3. Kontrollerende – internrevisjon, rapporter og ledelsesgjennomgang

3 Avgrensning av styringssystemet

SFI ved HVO omfatter

- alle ansatte, registrerte studenter, innleid personell og gjester ved HVO
- alle lokasjoner hvor HVO har virksomhet
- alle IT-systemer, teknisk og fysisk infrastruktur som eies eller leies av HVO
- alle informasjonsverdier, herunder også ev. manuelle registre

Med informasjonsverdier menes utstyr, prosesser eller data som er tilknyttet informasjon og som HVO anser som nødvendig å beskytte.

3.1 Sikkerhetsmål

Følgende mål for arbeidet med informasjonssikkerhet gjelder ved HVO:

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

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

3. Arbeidet med informasjonssikkerhet skal være i tråd med de krav som stilles i lover og forskrifter som gjelder for HVO, og følge opp 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 HVO, uavhengig av hvilke kanaler som benyttes.

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

3.2 Kriterier for akseptabel risiko:

Arbeidet med informasjonssikkerhet skal sørge for at informasjonsverdiene ved HVO 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 som 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, for eksempel konfidensielle forskningsdata, opplysninger om enkeltpersoner (personopplysninger[1]) eller forslag/tekster til eksamensoppgaver, - besvarelser, -karakterer og vitnemål skal prioriteres særlig høyt.

- Det aksepteres ikke brudd på konfidensialiteten eller integriteten til personopplysninger. Dette gjelder i særlig grad for sensitive personopplysninger.[2] Kortere avbrudd i personopplysningers tilgjengelighet aksepteres.

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

[2] 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.

- 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), eksamensbesvarelser, karakterer og vitnemål. 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 Sikkerhetsstrategi

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

- **Alt arbeid med informasjonssikkerhet skal basere seg på risikovurderinger.**
  Risikovurderinger av IT-systemer og -tjenester, datanettverk og infrastruktur, arbeidsprosesser og fysiske forhold skal gjennomføres hvert annet år, eller ved behov.

- **Ledelsen ved HVO skal bevilge nødvendige ressurser til opplæring og kompetanseheving for ledere og ansatte som er delegert ansvar for informasjonssikkerheten ved HVO eller som er pålagt å utføre konkrete arbeidsoppgaver.**
  Ledere ved HVO 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 HVO skal gis informasjon om rutiner for sikker håndtering av informasjonsverdier og trusler mot informasjonsverdiene.**
  De skal også informeres om avviksmeldingssystemet for brudd på informasjonssikkerhet ved HVO. I tillegg skal de informeres om hensikten med og viktigheten av at avvik/sikkerhetsbrudd rapporteres.

- **Fjerndrift av HVO sine informasjonsverdier 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.

- **Arbeidet med informasjonssikkerhet ved HVO skal til enhver tid basere seg på anbefalte og anerkjente standarder for SFI i offentlig sektor.**
  UNINETT og Sekretariatet for informasjonssikkerhet i UH-sektoren skal benyttes til rådgiving og bistand når det er nødvendig.

5 Sikkerhetsorganisasjon

Sikkerhetsorganisasjonen ved HVO består av:

5.1 Høgskulestyret

- Behandler og vedtar SFI ved HVO
- Kan stille krav til det videre arbeidet med informasjonssikkerhet ved HVO

5.2 Høgskuledirektør

- Har ansvaret for informasjonssikkerheten ved HVO.
- Har ansvar for at SFI implementeres og vedlikeholdes.
- Oppnevner medlemmer av sikkerhetsgruppen-IT/drift ved HVO.
- Kan delegere ansvaret til CSO

5.3 CSO (Chief Security Officer)

- Har fått delegert ansvar for informasjonssikkerhetssystem ved HVO.
- Skal ha oversikt over informasjonsverdier som behandles og IT-løsninger som benyttes ved HVO.
- Skal holde seg orientert om informasjonssikkerhetstilstanden ved HVO.

5.4 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.
- Skal motta avviksmeldinger fra fakulteter, avdelinger, andre enheter, forskningsprosjekter og individuelle brukere (ansatte, studenter, gjester, osv.)
- Skal registrere og dokumentere autorisert og forsøk på uautorisert bruk av HVOs IT-løsninger som inneholder personopplysninger.
- Skal bistå enheter eller forskningsprosjekter i sikkerhetsarbeidet.
- 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.

5.5 Sikkerhetsgruppen–IT/drift

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

- Skal holde seg orientert om tilstanden på informasjonssikkerhetsområdet, herunder nye trusler mot HVO 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.
- Ref. pkt. 3.3.3 i gjeldende sikkerhetspolicy for informasjon om gruppens sammensetning og mandat for øvrig.

5.6 Dekan/leder for enhet

- Er ansvarlig for å tilfredsstille krav til informasjonssikkerhet i egen avdeling/enhet
- Skal gjennomføre risikovurderinger og iverksette tiltak der det er nødvendig for å ivareta informasjonssikkerheten
- Skal rapportere resultat fra risikovurderinger med handlingsplan og avvik til CSO.
- Skal informere ansatte i avdelingen om gjeldende rutiner, retningslinjer og sørge for at kravene i SFI følges opp i avdelingen.

5.7 Brukere (ansatte og studenter)

- Plikter å gjøre seg kjent med og følge HVOs IT-reglement.

6 Risikovurdering

Risikovurderinger handler om to ting:

1. Identifisere uønskede hendelser, det vil si hendelser som kan føre til brudd på informasjonsverdienes konfidensialitet, integritet og tilgjengelighet.
2. Vurdere risikoen – sannsynlighet multiplisert med konsekvens – for hver uønsket hendelse som er identifisert.

Dersom risikoen (sannsynlighet/konsekvens) for én eller flere uønskede hendelser er høyere enn det institusjonen har definert som akseptabelt, må risikoen håndteres, for eksempel ved at forebyggende tiltak (sikringstiltak) iverksettes.

Risikovurderinger skal dokumenteres, og dersom tilfeller som skal følges opp avdekkes, skal dette rapporteres til CSO, sammen med tiltaksplan for behandling av avviket. I tiltaksplanen skal det framgå hvem som har ansvar for å gjennomføre tiltak(-ene).

Risikovurderinger skal foretas

- Ved oppstart av forskningsprosjekter
- Ved implementering av IT-systemer
    - Herunder også større endringer i eksisterende systemer
- Ved organisatoriske endringer som kan påvirke informasjonssikkerheten
- Når trusselbildet endres
    - CSO/Sikkerhetsgruppen-IT/drift kan pålegge organisasjonsledd å gjennomføre risikovurderinger

7 Opplæring

For å bygge en godt fungerende sikkerhetskultur ved HVO er opplæring avgjørende. Ansatte og studenter skal bevisstgjøres om viktigheten av informasjonssikkerhet. Opplæring i informasjonssikkerhet må derfor tas inn som en naturlig del av opplæringen av ansatte og studenter.

Ledere har et overordnet ansvar for å formidle relevant informasjon til de ansatte, og HVO skal inkludere informasjonssikkerhet i sin lederopplæring. Informasjon om HVOs arbeid, rutiner og retningslinjer for informasjonssikkerhet skal være lett tilgjengelig via HVOs nettsider og andre relevante kanaler.

Høgskuledirektøren skal sørge for at informasjonssikkerhet tas opp som tema i egnede lederfora minst en gang i året.

8 Sikkerhetsrevisjon

Hensikten med sikkerhetsrevisjon er å kontrollere at SFI innføres, driftes og vedlikeholdes ved HVO. Sikkerhetsrevisjoner skal gjennomføres årlig. Det er ikke nødvendigvis slik at hele organisasjonen skal gjennomgå revisjon hvert år.

Høgskuledirektøren eller CSO (dersom ansvaret er delegert) skal utarbeide revisjonsplan for informasjonsikkerhetsområde, samt ha oppsyn med at den gjennomføres i organisasjonen. I revisjonsplanen er det naturlig at det fremgår hvilke deler av institusjonen som skal revideres hvert år og hvilke områder som skal revideres.

9 Ledelsens gjennomgang (LG)

Hensikten med ledelsens gjennomgang er at høgskuledirektør blir orientert om og får grunnlag for styring av arbeidet med informasjonssikkerhet. LG skal føre til at det blir stilt krav til arbeidet med informasjonssikkerhet i neste periode. Sikkerhetsgruppen-IT/drift vedtar frekvens og omfang for LG, og utarbeider sluttrapport etter LG, som skal inneholde:

- Status på tiltak fra foregående LG
- Sikkerhetsmål og strategi
    - Vurdere om sikkerhetsmål og sikkerhetsstrategi fungerer som forutsatt.
    - Vurdere eventuelle forslag til endringer i sikkerhetsmål og sikkerhetsstrategi.
    - Vurdere økonomiske eller andre konsekvenser eventuelle endringer kan ha for institusjonen.
- Kriterier for akseptabel risiko
    - Vurdere endring av kriterier for akseptabel risiko basert på informasjonssikkerhetsarbeidet og trusselbildet
- Sikkerhetsorganisering
    - Vurdering av eksisterende organisering
    - Vurdere behov for endringer
- Avviksmeldinger
    - Gjennomgå de viktigste avvik i perioden.
    - Vurdere behov for sikringstiltak basert på gjentatte eller alvorlige avvik
- Sikkerhetsrevisjon
    - Gjennomgå status for arbeidet med informasjonssikkerhet i ulike deler i institusjonen
- Status på risikovurderinger
    - Hvilke risikovurderinger er gjennomført
    - Hovedfunn fra risikovurderinger
- Status på håndtering av risiko
    - Gjennomgå status på risikohåndteringen i institusjonen
    - Vurdere om risikohåndteringen er tilfredsstillende
- Ressurs- og kompetansebehov
    - Vurdere behov for økte ressurser til arbeidet med informasjonssikkerhet
    - Vurdere behovet for kompetanseheving (opplæring)