# Retningslinjer for Informasjonssikkerhet

**Referanse:** ISMS DOC 5.2

**Organisasjon utgave nr:** HK_SOP_IT_SEC_V2.3

**Organisasjon utgave dato:** 13.01.2020

**Endringshistorikk**

| Versjon | Endret på | Endringsbeskrivelse | Dokument ID |
|---|---|---|---|
| Ver 1.0 | 07.06.2018 | Retningslinjer for Informasjonssikkerhet ble etablert. | |
| Ver 1.1 | 04.03.2019 | Sendt til godkjenning av ledergruppen. | |
| Ver 2.0 | 04.03.2019 | Godkjent av leddergruppen. | |
| Ver 2.1 | 13.01.2020 | Oppdateringer *ifm* ISO 27001-standarden. | *HK_SOP_IT_SEC_V_2.1* |
| Ver 2.2 | 15.01.2020 | Oppdateringer på *retningslinjer for epost*. | *HK_SOP_IT_SEC_V_2.2* |
| Ver 2.3 | 09.10.2020 | Oppdateringer på *Sanksjoner* som anbefalt av HR-avdelingen. | *HK_SOP_IT_SEC_V_2.3* |

*Høyskolen Kristiania* en stiftelse grunnlagt i 1914,
lokalisert ved
Prinsens gate 7-9,
0152 Oslo (Norge),

er forpliktet til å bevare konfidensialiteten, integriteten og tilgjengeligheten til alle fysiske og elektroniske aktivum i hele organisasjonen - for å bevare konkurransefortrinn, kontantstrøm, lønnsomhet, juridisk, forskriftsmessig og kontraktsmessig etterlevelse og kommersielt image. Informasjon- og informasjonssikkerhetskrav vil fortsette å være i tråd med *Høyskolen Kristianias* mål, og ISMS er ment å være en mekanisme som legger til rette for informasjonsdeling, elektronisk drift, e-handel og reduserer informasjonsrelatert risiko til akseptable nivåer.

1. Retningslinjene gjelder for alle brukere som benytter skolens IT-utstyr og informasjonssystemer, og/eller er i et partnerskap med skolen for sektorbasert samarbeid og/eller yter støttefunksjoner.
2. IT-utstyr består av datamaskiner, mobiltelefoner, nettverk, programvare, data, lagringsmedier og annet utstyr av lignende art som gjøres tilgjengelig av Høyskolen Kristiania.

3. Informasjonssystemer er alle former for fysiske eller digitale løsninger som oppbevarer enhver form for informasjon som gjelder Høyskolen Kristiania. Denne informasjonen kan være om studenter, ansatte, forretningspartnere eller selve skolen.
4. Brukere har alltid ansvaret for å gjøre seg kjent med innholdet i dette dokumentet før de bruker IT-utstyret og for holde seg informert om IT-forskriftene som er i bruk og eventuelle gjeldende tilleggsbestemmelser.
5. IT-forskrifter er tilgjengelig på http://kristiania.no/it for studenter og på intranett for skolens ansatte.
6. Kontaktinformasjon for IT-avdelingen finner du på http://kristiania.no/it.

Høyskolen Kristiania sin nåværende strategiske forretningsplan og risikostyringsrammeverk gir kontekst for å identifisere, vurdere, evaluere og kontrollere informasjonsrelaterte risikoer gjennom etablering og vedlikehold av et ISMS. Risikovurderingen, erklæringen om anvendelighet (*Statement of Applicability*) og tiltaksplanen identifiserer hvordan informasjonsrelaterte risikoer håndteres. CISO er ansvarlig for styring og vedlikehold av tiltaksplanen. Om nødvendig kan ytterligere risikovurderinger utføres for å utarbeide passende kontroller for spesifikke risikoer.

Spesielt er forretningskontinuitets- og beredskapsplaner, prosedyrer for sikkerhetskopiering av data, unngåelse av virus og hackere, tilgangskontroll til systemer og rapportering av informasjonssikkerhetshendelser fundamentale for denne forskriften. Kontrollmål for hvert av disse områdene er spesifisert i håndboken og støttes oppunder av spesifikke dokumenterte retningslinjer og prosedyrer.

Høyskolen Kristiania har ambisjon om å oppnå spesifikke, definerte mål for informasjonssikkerhet, som er utviklet i samsvar med forretningsmålene, organisasjonens kontekst, resultatene av risikovurderinger og tiltaksplanen.

Alle ansatte ved *Høyskolen Kristiania* og alle eksterne parter:

*i. ethvert universitet eller utdanningsinstitusjon som jobber i samarbeid med Høyskolen Kristiania for forsknings- eller utdanningsformål.*
*ii. enhver forretningspartner som yter støtte til høyskolen med utdannelsesformål eller som bransjepartner.*
*iii. enhver person eller organisasjon tilknyttet Høyskolen Kristiania for å yte støtte i prosjekter eller annen aktivitet knyttet til Høyskolen Kristianias virksomhet;*

forventes at overholder denne forskriften og ISMS som gjennomfører den.

Alle ansatte og eksterne parter vil motta en kopi av dette dokumentet dvs. *Høyskolen Kristianias Retningslinjer for Informasjonssikkerhet* på ansettelsestidspunktet (eller retrospektivt for nåværende ansatte).

Følgende retningslinjer må tas i betraktning ved bruk av informasjonssystemene (IT-systemene) tilhørende Høyskolen Kristiania.

**Retningslinjer for passord**
Passord er personlig og må ikke deles med andre. Når en bruker blir informert om å endre deres passord, skal han/henne velge et passord som ikke er enkelt å gjette (skal ikke inneholde personlig informasjon slik som eiers navn, fødselsdato, bilmerke osv.). Ved mistanke om røpt passord skal det umiddelbart endres.

**Uautorisert bruk**
Det er brukerens ansvar å forhindre enhver form for uautorisert tilgang til deres brukerkonto. Ved oppdagelse av uautorisert tilgang, forsøkt uautorisert tilgang eller ved mistanke om at uvedkommende kjenner til passordet ditt, skal dette umiddelbart rapporteres til IT-avdelingen.

Brukere er ansvarlig for alle handlinger utført fra deres brukerkonto.

**Uautorisert tilgang**
Brukeren skal ikke oppnå, eller forsøke å oppnå tilgang til systemer eller informasjon som han/henne ikke er ment tilgang til; gjennom skolens IT-systemer.
Dette gjelder også i sammenheng med undervisning eller forskning.

**Avlogging**
For å forhindre misbruk eller uautorisert tilgang, er det viktig at brukeren sikrer fysisk tilgang ved å logge av eller benytte seg av en passord-beskyttet skjermsparer når han/henne ikke er til stede. Uautoriserte personer kan ellers enkelt få tilgang til informasjon under brukerens fravær.

**Ondsinnet programvare**
Brukeren må forsikre seg om at installert programvare ikke er skadelig for datamaskinen eller tilkoblede IT-systemer (virus, skadevare, osv.). I hovedsak skal programvare som ønskes installert være forhåndsgodkjent av IT-avdelingen.

**Instruksjoner for bruk og rutiner**
Brukeren er forpliktet til å gjøre seg kjent med brukerhåndbøkene, rutinene eller saker av lignende art på en slik måte at brukeren reduserer muligheten for uvitenhet; skaper risiko for sårbarheter, driftsforstyrrelse eller tap av data.

**Bruk av digitalt innhold**
Brukeren må opptre med varsomhet ved åpning av ukjente filer, e-postvedlegg, filer fra ukjente minnepenner og lignende. Dette for å forhindre at utstyr blir

infisert med skadevare slik som virus, spionvare, trojanere og lignende. Skulle en hendelse oppstå, skal IT-avdelingen varsles så fort som mulig.

*Merk: IT-avdelingen står fritt til å blokkere tjenester etter eget skjønn, dersom de utgjør en sikkerhetsrisiko.*

**Bruk av ikke-standardiserte tjenester/løsninger**
Det er ikke tillatt å bruke tjenester (for eksempel over internett) som kan hindre eller forstyrre normal drift av skolens IT-systemer.

**Bruk av IT-utstyr**

- Brukeren må unngå bruk av IT-utstyr til aktiviteter som ikke er direkte relatert til skolens aktiviteter
- Brukeren må sørge for at skolens IT-systemer ikke brukes til aktiviteter som bryter med norsk lov.
- Det er ikke tillatt å koble fra eller flytte skolens stasjonære IT-utstyr uten avtale med IT-avdelingen. Dette gjelder ikke bærbare datamaskiner i bruk av de ansatte.

**Lagring, sikkerhetskopiering og oppbevaring av data (for ansatte)**

- Ansatte bør sørge for at arbeidsrelatert informasjon lagres på plattformene (lagringsløsningene) som tilbys av skolen.
- Data som tilhører skolen, skal lagres på en slik måte at de blir sikkerhetskopiert automatisk. Vær oppmerksom på at data lagret på de lokale datamaskinene ikke blir sikkerhetskopiert.
- Brukerne er ansvarlige for å sikkerhetskopiere data som er lagret på deres lokale datamaskin.

**Lagring, sikkerhetskopiering og oppbevaring av data (for studenter)**

- Studentene er selv ansvarlige for deres egen data. Imidlertid opprettholdes data i læringsportalen og i andre systemer som er gjort tilgjengelig av skolen; på samme måte som resten av dataene tilhørende skolen.
- Brukerne er ansvarlige for å sikkerhetskopiere data som er lagret på deres lokale datamaskin.

**Retningslinjer for e-post**

- E-postkontoer levert av Høyskolen Kristiania er skolens eiendom og må kun brukes til offisielle formål.
- Da *phishing* i disse dager er en veldig relevant og utbredt angrepsvektor, er det viktig at ethvert observert phishing-angrep rapporteres til IT-support. Hvis noen ved uhell blir offer for slike angrep, bør han/henne umiddelbart endre passordet sitt og kontakte IT-support for ytterligere assistanse.

- Ikke svar på forespørsler om personlig eller sensitiv informasjon via e-post, selv om e-posten ser ut til å være fra en troverdig kilde.
- Opptre diskre når du vurderer troverdigheten til en e-post.
- Under ingen omstendigheter skal e-post inneholde trusler, språk eller bilder relatert til rase, kjønn, alder, seksuell legning, pornografi, religiøs eller politisk tro, nasjonalitet eller funksjonshemning.
- Informasjon om personer eller virksomheter må oppbevares eller arkiveres på en tidsbundet måte og årsak for oppbevaring må kunne grunnes forskriftskrav.
- E-posten din må følge de grunnleggende protokollene til forretnings-e-post, slik som å unngå bruk av slang, må inneholde en signatur, kun svare til alle når det er nødvendig og svare på e-post innenfor en rimelig tidsramme.

**Opphavsrettsbeskyttet materiale og lisenser**

- Bruk eller deling av åndsverk skal kun gjøres i samsvar med Åndsverkloven.
- Nedlasting og/eller deling av opphavsrettsbeskyttet materiale uten eksplisitt godkjenning fra materialets eier er ikke tillatt.
- Det er ikke tillatt å kopiere programvare og andre rettsbegrensede eller lisensierte data (for eksempel font, bilder eller lignende) fra IT-utstyr eid av skolen.
- Programvare som skolen har gjort tilgjengelig for brukerne, skal alltid brukes i samsvar med lisensavtalen. Mange av lisensene er kun for utdanningsformål og kan dermed ikke brukes privat eller kommersielt. IT-avdelingen kan avklare lisensvilkår ved behov.

**Personvern**

- Bruk av personopplysninger må være i samsvar med personopplysningsloven. Skolens personvernansvarlige kan veilede i spørsmål knyttet til personvern.
- Registrering av personopplysninger skal kun gjøres etter avtale med IT-avdelingen. Dette gjelder uavhengig av formål (forskning, studier osv.).
- Lagringsmedier (som CD/DVD-plater, minnepinner, eksterne harddisker og papirdokumenter osv.) som inneholder personlig informasjon og/eller konfidensiell informasjon, skal håndteres og lagres på en sikker måte.
- Utskrifter som inneholder personlig informasjon og/eller konfidensiell informasjon som en ansatt ikke lenger har behov for, må makuleres. Forpliktelser i dette avsnittet supplerer taushetserklæringer for de som er bundet av dem.

**Bruk av privat IT-utstyr**

- Utstyret kobles opp mot skolens nettverk på egen risiko.
- Skolen kan ikke holdes ansvarlig for utstyr som blir infisert, stjålet eller på noen måte påvirket mens du bruker skolens nettverk eller lokaler.

- Brukerne er ansvarlige for å oppdatere antivirusprogramvare regelmessig og sørge for at alle applikasjoner/operativsystem er oppdatert med de siste sikkerhetsoppdateringene.

**Innsyn og utlevering av data**

- Brukere skal ikke utlevere informasjon om de ansatte eller data som tilhører en partner, med mindre norsk lov eller interne forskrifter er gjeldende.
- IT-avdelingen har rett til å søke tilgang til den enkelte brukers reserverte områder med det eneste motivet å 1) sikre funksjonaliteten til IT-systemet, eller 2) kontrollere at brukeren ikke bryter eller har brutt denne forskriften. Det antas at slik tilgang bare søkes når det er kritisk for skolens drift, eller på grunnlag av spesielle mistanker. Tillatelse for tilgang til elektronisk post skal søkes separat.
- Hvis IT-avdelingen søker slik tilgang, må tillatelse på forhånd oppnås fra direktøren for HR (for ansatte) eller direktøren for Studentadministrasjonen (for studenter).
- Hvis bruken av datamaskin, mobiltelefon eller annet sluttbrukerutstyr på grunnlag av driftssikkerhet eller av andre hensyn overvåkes av IT-avdelingen, skal dette angis med et merke på enheten eller på annen måte.
- IT-avdelingen har taushetsplikt med hensyn til informasjon de tilegner seg om brukeren eller brukerens aktivitet, med unntak av forhold som representerer brudd på denne forskriften.

**Sanksjoner**

- Ved brudd på, eller mistanke om brudd på disse retningslinjene, kan IT-avdelingen uten videre varsel oppheve brukerrettigheter i opptil 5 dager.
- Brudd på retningslinjene kan få konsekvenser for ansettelsesforholdet for ansatter, og studentstatus for studenter.
- Direktøren for HR (for ansatte) og direktøren for Studentadministrasjonen (for studenter) kan oppheve brukerrettighetene permanent.
- Andre sanksjoner kan benyttes i samsvar til andre retningslinjer for skolen eller i henhold til norsk lov.

Skulle det være tvetydighet i bestemmelsene, skal det gis passende avklaringer og nødvendige endringer vil bli gjort i forskriften, periodisk og etter behov.

Konsekvensene av å bryte *Retningslinjene for Informasjonssikkerhet* er beskrevet i organisasjonens disiplinærforskrift, og i kontrakter og avtaler med tredjeparter. ISMS er underlagt kontinuerlig, systematisk gjennomgang og forbedring. Høyskolen Kristiania har etablert en styringsgruppe på toppnivå kalt *Advisory Board*, ledet av administrerende direktør (CEO) eller et delegert organ i samarbeid med sjef for informasjonssikkerhet (CISO) og inkluderer andre

ledere/spesialister/risikospesialister, for å støtte oppunder ISMS-rammeverket og periodisk gjennomgå sikkerhetsforskriften.

Høyskolen Kristiania har som mål å oppnå sertifisering av ISMS til ISO27001: 2013.

Denne forskriften vil bli gjennomgått for å reflektere eventuelle endringer i risikovurderingen eller tiltaksplanen, minst på årlig basis.

I denne forskriften er `informasjonssikkerhet´ definert som:

**Bevare**
Dette betyr at ledelse, heltids- eller deltidsansatte, underleverandører, prosjektkonsulenter og eventuelle eksterne parter har og vil bli gjort oppmerksom på; sitt ansvar (som er definert i deres stillingsbeskrivelser eller kontrakter) for å bevare informasjonssikkerheten, å rapportere sikkerhetsbrudd (i tråd med retningslinjene og prosedyrene identifisert i avsnitt 16 i håndboken og å handle i samsvar med kravene i ISMS. Alle ansatte vil få informasjonssikkerhetsopplæring og mer spesialiserte ansatte vil få passende spesialisert informasjonssikkerhetsopplæring.

**tilgjengeligheten,**
Dette betyr at informasjon og tilknyttet aktivum skal være tilgjengelig for autoriserte brukere når det behøves og fysisk sikret. Datanettverket må være motstandsdyktig og Høyskolen Kristiania må kunne forhindre, overvåke, identifisere og reagere raskt på hendelser (slik som virus og annen skadevare) som truer den fortsatte tilgjengeligheten av aktivum, systemer og informasjon. Planer for videre drift må være utarbeidet (BCP). Skulle det være en sikkerhetshendelse som truer tilgjengeligheten av informasjonssystemene, kan disse systemene hentes ut og gjenopprettes ved hjelp av sikkerhetskopiløsningene.

**konfidensialiteten,**
Dette innebærer å sikre at informasjonen bare er tilgjengelig for de som er autorisert til å få tilgang til den, og dermed forhindre både bevisst og utilsiktet uautorisert tilgang til Høyskolen Kristianias informasjonsaktivum (all informasjon som oppbevares digitalt eller på papir) og systemer; inkludert, men ikke begrenset til nettverk, nettsted(er), ekstranett, kvalitetssikringssystem, ERP-system dvs. Business Central, HRM system etc.

i. Brukere skal ikke utlevere informasjon om de ansatte eller data som tilhører en partner, med mindre norsk lov eller interne forskrifter er gjeldende.

ii. IT-avdelingen har rett til å søke tilgang til den enkelte brukers reserverte områder med det eneste motivet å 1) sikre funksjonaliteten til IT-systemet, eller 2) kontrollere at brukeren ikke bryter eller har brutt denne forskriften. Det antas at slik tilgang bare søkes når det er kritisk for skolens drift, eller på grunnlag av spesielle mistanker. Tillatelse for tilgang til elektronisk post skal søkes separat.
iii. Hvis IT-avdelingen søker slik tilgang, må tillatelse på forhånd oppnås fra direktøren for HR (for ansatte) eller direktøren for Studentadministrasjonen (for studenter), med mindre spesielle forhold krever umiddelbare inngrep. Imidlertid må slike spesielle forhold dokumenteres etter prosedyren.
iv. Hvis bruken av datamaskin, mobiltelefon eller annet sluttbrukerutstyr på grunnlag av driftssikkerhet eller av andre hensyn overvåkes av IT-avdelingen, skal dette angis med et merke på enheten eller på annen måte.
v. IT-avdelingen har taushetsplikt med hensyn til informasjon de tilegner seg om brukeren eller brukerens aktivitet, med unntak av forhold som representerer brudd på dette dokumentet.

**og integriteten**
Dette innebærer å sikre nøyaktigheten og fullstendigheten av informasjon og behandlingsmetoder, og krever derfor å forhindre bevisst eller utilsiktet, delvis eller fullstendig, ødeleggelse eller uautorisert modifisering av både fysiske aktivum og elektroniske data. Det må være hensiktsmessig beredskap rundt; inkludert, men ikke begrenset til nettverk, nettsted(er), ekstranett, kvalitetssikringssystem, ERP-systemer dvs. Business Central, HRM system etc. og planer for sikkerhetskopiering av data og rapportering av sikkerhetshendelser.

Høyskolen Kristiania må overholde alle relevante datarelaterte lovgivninger i de jurisdiksjonene den opererer innenfor.

**av de fysiske aktivum**
Høyskolen Kristianias fysiske aktivum; inkludert, men ikke begrenset til, datamaskinvare, datakabler, telefonsystemer, arkivsystemer, fysiske datafiler og informasjonsaktivum.

**og informasjonsaktivum**
Dette inkluderer informasjon som er trykt eller skrevet på papir, sendt med post, vist i filmer, sagt i samtaler, samt informasjon som er lagret elektronisk på servere, nettside(r), ekstranett, intranett, PC-er, bærbare datamaskiner, mobiltelefoner og PDA-er, samt på CD-ROM, disketter, USB-pinner, sikkerhetskopibånd og andre digitale eller magnetiske medier, og annen informasjon som på noen måte overføres elektronisk. I denne sammenheng inkluderer `data´ også settene med instruksjoner som forteller systemer

hvordan man kan manipulere informasjon (dvs. programvaren; operativsystemer, applikasjoner, verktøy osv.).

**tilhørende Høyskolen Kristiania**
Høyskolen Kristiania, og alle eksterne parter dvs.:

i. ethvert universitet eller utdanningsinstitusjon som jobber i samarbeid med Høyskolen Kristiania for forsknings- eller utdanningsformål.
ii. enhver forretningspartner som yter støtte til høyskolen med utdannelsesformål eller som bransjepartner.
iii. enhver person eller organisasjon assosiert med Høyskolen Kristiania for å gi støtte i prosjekter eller andre aktiviteter som har tilknytning til Høyskolen Kristianias virksomhet og har akseptert våre retningslinjer for informasjonssikkerhet og ISMS.

ISMS er styringssystemet for informasjonssikkerhet som denne forskriften, informasjonssikkerhetshåndboken (håndboken) og annen støttende og/eller relatert dokumentasjon er en del av, og er utformet i samsvar med spesifikasjonen i ISO27001:2013.

Et sikkerhetsbrudd er enhver hendelse eller aktivitet som forårsaker, eller kan forårsake, et brudd i tilgjengeligheten, konfidensialiteten eller integriteten til Høyskolen Kristianias fysiske eller elektroniske informasjonsaktivum.

**Eier av dokumentet og godkjenning**
CISO er eier av dette dokumentet og er ansvarlig for å holde det oppdatert. Den gjeldende versjonen av dette dokumentet er tilgjengelig for HR-avdelingen, informasjonssikkerhetsjef (CISO), ledelsen og *Advisory Board*.

Etter godkjenning skal dette dokumentet være tilgjengelig for alle ansatte og studenter, og være bindende - før bruk Høyskolen Kristianias IT-utsyr. Dokumentet er publisert på intranett og kvalitetssikringssystemet - *Compilo*.