Sikkerhetsinstruks
for ansatte ved NMH

INNHOLD

Forord

I dag spiller informasjonssystemene en viktig rolle i alle deler av samfunnet. Det finnes flere lover som stiller viktige krav til NMH i forvaltning av informasjonen. Samtidig har teknologi bidratt til at informasjon lagres og deles i et omfang som er stadig økende.

Den effektiviseringen i informasjonsbehandlingen som teknologien muliggjør, må skje i tråd med de grunnleggende rettigheter som vårt samfunn er bygget på. Lover som Personopplysningsloven stiller strenge krav til bruk av informasjon.

Nye krav til behandling av personopplysninger styrker ansattes, studenters og søkeres rettigheter og stiller nye krav til oss som organisasjon. Vi må sette studenter og ansattes rettigheter i førersete og styrke vårt internkontrollarbeid for å få dette til.

Ved NMH har direktøren et overordnet ansvar for at forvaltningen av informasjon skjer i tråd med gjeldende lover og regler (behandlingsansvarlig). Videre har den enkelte medarbeider som benytter informasjonen i ulike behandlinger, et operativt ansvar for å følge de regler og retningslinjer for personvern og informasjonssikkerhet som her er beskrevet. Denne veilederen inneholder de viktigste regler hver enkelt ansatt må følge, for at vi sammen skal redusere risikoen for brudd på sikkerhetsbestemmelsene.

Med hilsen

Tove T Blix (Direktør)

1 Innledning

Dette dokument er rettet mot de ansatte ved NMH.

Studenter har «IKT reglementet» som veileder å forholde seg til.

Dette dokumentet beskriver NMHs regelverk for behandling av informasjon generelt og personopplysninger spesielt.

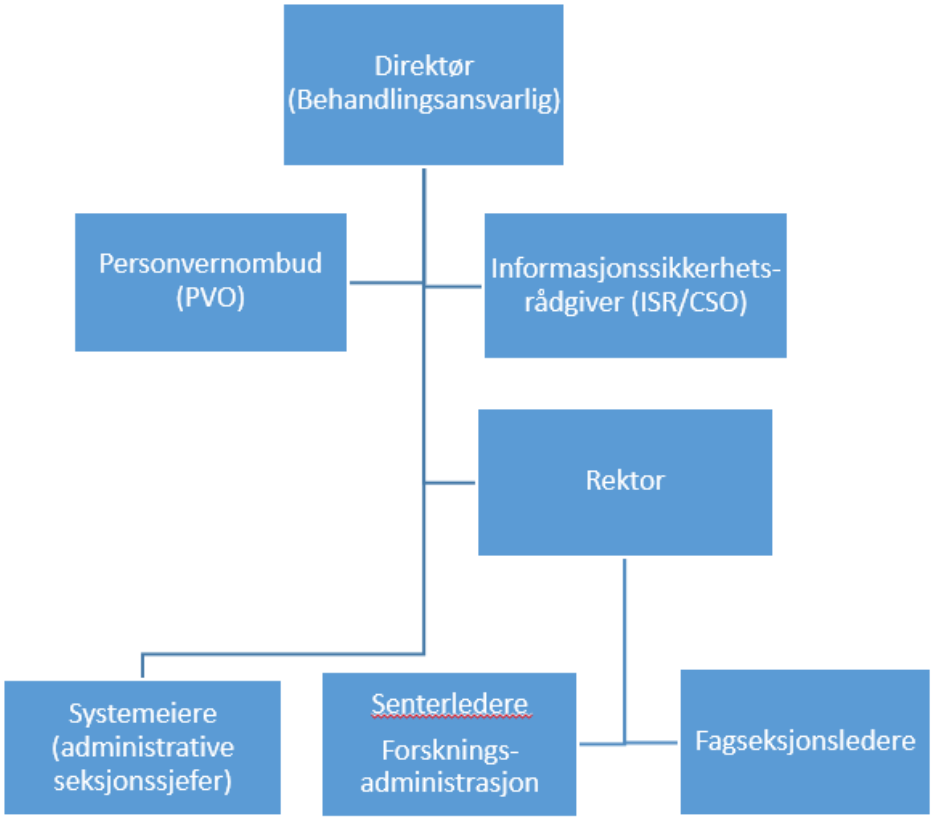
Det er ditt ansvar å bli kjent med og etterleve regelverket. Begrepene som brukes i dokumentet er definert under kapittelet ordforklaringer.

Se følgende relaterte dokumenter:

- ✓ Taushetserklæring
- ✓ Sikresiden.no
- ✓ Ledelsesinformasjonssystem for sikkerhet (LSIS)
- ✓ IKT reglementet

2 Organisering av personvern

Direktøren er ansvarlig for alle behandlinger av personopplysninger og er ansvarlig for personvern og informasjonssikkerhet.



Alle ledere har et ansvar for personvern i sin seksjon.

Det operative ansvaret for personvern og informasjonssikkerhet er delegert til de seksjonslederne som har ansvar for et eller flere systemer (systemeiere).

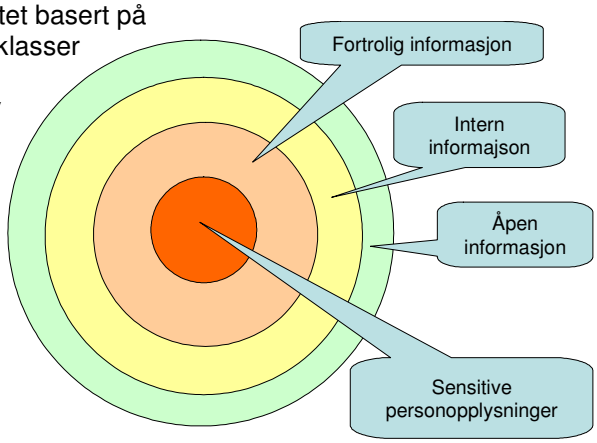
Ansatte og studenter har ansvar for å følge det etablerte regelverk og rapportere avvik fra dette.

3 Informasjonshåndtering

NMH klassifiserer informasjonens konfidensialitet basert på gjeldende lovverk. De forskjellige informasjonsklasser er beskrevet under "Ordforklaringer". Det er i tillegg til åpen informasjon, tre hovedklasser av beskyttet informasjon:

- ✓ Åpen informasjon
- ✓ Intern informasjon (Lav)
- ✓ Fortrolig informasjon (Medium)
- ✓ Sensitive informasjon (Høy)

Lav, Medium og Høy tilsvarer skalaen i klassifiseringen av konfidensialitet.



3.1 Åpen informasjon:

Dette er informasjon publisert på åpne sider på internett, som studieplaner, informasjons-materiell, ansattoversikter, pressemeldinger, kursinvitasjoner etc.

Behandling:

- ✓ Informasjon som publiseres på Internett eller trykkes gjennom NMHs utgivelser, skal være kvalitetssikret.
- ✓ Opplysninger om enkeltpersoner som publiseres skal være godkjent av den enkelte.

3.2 Intern informasjon:

Dette er informasjon som ikke skal utenfor NMH sine lokaler eller lukkede informasjonssystemer.

Behandling av elektronisk informasjon:

- ✓ Skal begrenses kun til ansatte med brukerkonto.
- ✓ Beskyttes med godkjente mekanismer, dersom informasjonen sendes ut av NMH sitt domene/område.

Papirdokumenter med Intern informasjon:

- ✓ Beskyttes (fysisk sikring / låsing) dersom informasjonen tas med ut av kontorsoner (f.eks ut av kontoret, ut av administrasjonen eller ut av NMH).

3.3 Fortrolig informasjon:

Dette er for eksempel personopplysninger om studenter og ansatte, som dokumenter rundt ansettelse, personalsaker, lønnsbehandling og -forhandlinger, samt interne fortrolige notater.

Behandling av elektronisk informasjon:

- ✓ Tilgang skal begrenses til grupper internt.
- ✓ Mobile enheter (mobiltelefoner, nettbrett osv.) med NMH e-post skal sikres med kode.

Papirdokumenter med Fortrolig informasjon:

- ✓ Låses inn når de ikke er i bruk (låst kontor eller skap)
- ✓ Kun skrivere som har utskriftskontroll benyttes
- ✓ Kun kastes i godkjente sikkerhetsdunker eller makuleres

3.4 Sensitive opplysninger:

Sensitive personopplysninger defineres som:

- ✓ Opplysninger om helse-, kriminelle-, seksuelle-, politiske- og fagforeningsforhold
- ✓ Se for øvrig link (datatilsynet)

I tillegg kan følgende informasjon defineres som sensitiv:

- ✓ Risikovurderinger, konkurransestrategier

Behandling av elektronisk informasjon:

- ✓ Tilgang skal begrenses til kun de som har saklig behov
- ✓ Ikke sendes ut av det lokale nettverk uten godkjent kryptering eller andre godkjente sikkerhetstiltak (som Digipost eller tjenester for pakking med kryptering og passordbeskyttelse (ZIP verktøy)
- ✓ Mobile enheter med e-post skal sikres iht NMHs regler for mobile enheter.

Papirdokumenter med sensitive opplysninger skal:

- ✓ Låses inn når de ikke er i bruk (låst kontor eller skap)
- ✓ Kun skrivere som har utskriftskontroll benyttes
- ✓ Kun kastes i godkjente sikkerhetsdunker eller makuleres

3.5 Personvern generelt

Det er nye og strengere krav til behandling av personopplysninger fra juni 2018. Ansattes rettigheter og kontroll over egne personopplysninger styrkes. NMH kan få høye bøter dersom vi bryter personvernreglene.

Informasjon som kan knyttes til en ansatt (og studenter) er personopplysninger. Det stilles strenge krav til konfidensialitet for sensitive personopplysninger og de må ikke komme på avveie.

NMH ønsker å være en «åpen skole», som betyr at studenter og andre (også uvedkommende) lett kan komme inn i administrasjonsområdet. Det betyr at vi må sikre personopplysningen godt på PC, mobil og på papir.

3.5.1 Prinsipper for behandling av personopplysninger

Personopplysninger skal i behandles etter følgende prinsipper: [1]

> *a) behandles på en lovlig, rettferdig og gjennomsiktig måte med hensyn til ansatte, studenter og søkere («lovlighet, rettferdighet og gjennomsiktighet»),*

[1] All tekst i kursiv er hentet direkte fra Personopplysningsloven. 3 punktum markerer at noe lovtekst er utelatt for lesbarhetens skyld.

b) *samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene … («formålsbegrensning»),*

c) *være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»),*

d) *være korrekte og om nødvendig oppdaterte… («riktighet»),*

e) *lagres slik at det ikke er mulig å identifisere ansatte, studenter og søkere i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for; … («lagringsbegrensning»),*

f) *behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og fortrolighet»).*

Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at prinsippene *overholdes («ansvar»).* Alle ledere og ansatte har ansvar for å oppfylle kravene.

3.5.2 Ansatte, studenter og søkere sine rettigheter

Videre har ansatte, studenter og søkere en rekke rettigheter som vi må ta stilling til når vi behandler personopplysninger, som retten til å:

- ✓ få vite hvordan personopplysninger behandles på NMH gjennom personvern-erklæringer på nmh.no
- ✓ få innsyn i egne personopplysninger
- ✓ få rettet og slettet personopplysninger (innen visse grenser gitt av andre lover f.eks arkivloven)
- ✓ Link til personvernerklæring

Det er videre en del andre rettigheter som håndteres av sikkerhetsorganisasjonen.

Ta kontakt med informasjonsinformasjonssikkerhetsrådgiver (ISR) dersom du har spørsmål rundt behandling av personopplysninger.

3.6 Lagring og sletting av personopplysninger

Personopplysninger lagres på godkjente lagringsområder (som Box.com og felles filområder). Alle filområder eies av avdelingens leder, som har det overordnede ansvar for informasjonen, vedlikehold og sletting. Det er viktig å ha avklart hvor lenge informasjonen skal «leve».

Det er definert regler for sletting for alle behandlinger av personopplysninger. Når personopp-lysninger skal slettes, skal de slettes på samtlige lagringsplattformer, for eksempel dedikerte informasjonssystemer, Box, filområder, epost (husk slettede elementer også) og på papir (i skuffer, arkivskap, arkiver og fjernarkiver). Vurder tiltak for dataminimering og anonymisering.

Arkivverdig informasjon skal lagres i arkivsystemet med nødvendig beskyttelse.

4 Informasjonssikkerhet

4.1 Fysisk sikring

Manglende fysisk sikring kan være årsak til sikkerhetsbrudd. Følg disse enkle reglene for å redusere risikoen for tap av informasjon og teknisk utstyr.

- ✓ Ikke slipp inn personer uten autorisert adgang i adgangskontrollerte kontorsoner uten tillatelse fra en ansatt ved NMH.
- ✓ Oppbevar adgangskort eller nøkler sikkert og utilgjengelig for uvedkommende. Dersom du mister adgangskort eller nøkler skal du orientere drift/sentralbord umiddelbart.

- ✓ Ikke gi dine personlige passord / adgangskoder til andre.
- ✓ Ikke låne bort adgangskort inklusiv personlige pin kode til andre

4.2 Brukeridentifikasjon og autentisering

Datasystemer benytter et brukernavn og passord for å sikre at kun autoriserte personer bruker systemet.

- ✓ Beskytt dine passord godt og la aldri noen andre bruke din konto
- ✓ Skriv ikke ned ditt passord eller lagre det elektronisk i klartekst.
- ✓ Logg ut eller bruk en passordbeskyttet skjermlås (Windows L / ctrl+alt+del) når du forlater arbeidsplassen og logg alltid ut på slutten av dagen.

4.3 Mobile enheter

Bærbar klienter (PC/MAC), iPad, mobiltelefoner, ekstern lagringsenhet og minnebrikker, kan lett bli stjålet og informasjon kan komme uvedkommende i hende.

- ✓ Mobile enheter med NMH e-post skal sikres med kode.
- ✓ Sensitive opplysninger skal ikke lagres på mobile enheter som Pad, ekstern lagrings-enhet og minnebrikker uten kryptering.
- ✓ Lås alltid PCen når du forlater den (Windows L)
- ✓ Alle klienter (PC/MAC) og andre mobile enheter for ansatte tilknyttet NMHs ansatt-nettverk, skal være innkjøpt, forvaltet og konfigurert av IT-avdelingen. Alle PC/MAC skal ha antivirus programvare installert. Ansatte kan benytte egen maskin på NMHs gjeste-nettverk.
- ✓ Brukere (gjester) som ikke benytter godkjente klienter, vil automatisk bli koblet til gjestenettet.
- ✓ Rapporter tyveri av bærbart utstyr umiddelbart til IKT-avdelingen. Standard prosedyre ved tap av klient er endring av NMH/FEIDE-passord.
- ✓ Det blir tatt sikkerhetskopier av all informasjon på NMHs sentrale datasystemer og tjenester (for eksempel e-post, fillagring). Lagrer du data på lokale disk eller minnebrikker er du selv ansvarlig for sikkerhetskopiering.

4.4 Digitale tjenester

Krav til aktsomhet i forhold til Internett:

- ✓ Ta utgangspunkt i at du aldri er anonym på nettet og at all kommunikasjon på nettet kan spores tilbake til maskinen du sitter med på NMH.
- ✓ Det at du er ansatt ved NMH forplikter i forhold til god etikk. Den enkelte skal derfor ha et reflektert forhold til hvilke søk, og hvilke nedlastinger av materiale som foretas.
- ✓ NMH overvåker ikke den enkeltes bruk av Internett eller private filer. Det forutsettes at bruken skjer i samsvar med de retningslinjer som er gitt. Vær klar over at:
    - o Sikkerhetslogger kan inneholde informasjon om trafikk knyttet til enkeltpersoner. Disse sikkerhetsloggene kan gjennomgås av sikkerhetsleder. Ved mistanke om sikkerhetsbrudd vil sikkerhetslogger kunne inngå som grunnlag for å vurdere sikkerhetsbruddet eller hærverk

- NMH kan i visse situasjoner ha en saklig begrunnelse til å gå gjennom den enkeltes e-post eller filområde, f. eks. ved lang tids sykefravær eller ved mistanke om grove brudd på regelverk. Se egne regler for samtykke og innsyn (Personvernerklæring).
- Ved innsyn i personopplysninger i logger, skal rutinen for innsyn i e-post følges (jf. arbeidsmiljøloven).

- ✓ Hvis du har behov for programvare utover det som er standard, kontakt IKT-drift.
- ✓ Å legge ut fortrolig informasjon eller sensitive personopplysninger ansees som et alvorlig brudd på sikkerhetsbestemmelsene.
- ✓ Bruk ikke bilder og tekster du finner på nettet i NMH publikasjoner og dokumenter uten først å sjekke opphavsrett og regler for gjenbruk (copyright / Creative Commons (CC)). Det kan påløpe store bøter ved misbruk.
- ✓ Gjør deg kjent med regler for programvare og tjenester som benyttes ved NMH
- ✓ Ikke søk eller last ned materiale fra nettsider du er kjent med, eller burde være kjent med inneholder ulovlig materiale. Er du i tvil, sjekk med ISR.

4.5 E-post og meldingstjenester

Ukryptert e-post er relativt lett tilgjengelig for uvedkommende når det sendes ut av NMH-domenet.

- ✓ Sensitive personopplysninger skal sendes til og fra eksterne med sikker kommunikasjon (Digipost eller tjenester for pakking med kryptering og passordbeskyttelse (ZIP verktøy)
- ✓ E-post må alltid vurderes i forhold til om det inneholder arkivverdig materiale som skal registreres og arkiveres i saksbehandlingssystemet.
- ✓ Vedlegg til, eller lenker i e-post skal ikke åpnes, med mindre forsendelsen kommer fra en avsender det er rimelig å forvente saklig kontakt med NMH.
- ✓ Den enkelte er ansvarlig for fortløpende å rydde i sin e-post ved å slette elementer som det ikke er behov for å lagre. Se spesielt på personopplysninger.
- ✓ E-post er først forsvarlig slettet når den er slettet fra e-post systemets ”søppelkasse”.
- ✓ E-post skal i utgangspunktet kun brukes i jobb-sammenheng og eies av NMH.

4.6 Sosiale medier

- ✓ Ikke lagre fortrolig eller sensitiv informasjon på sosiale medier.
- ✓ Når det opprettes grupper i sosiale medier av NMH, må det finnes en redaksjonsvarlig som holder øye med aktivitet og modererer gruppen.
- ✓ Samtykke skal innhentes for alle personopplysninger (inkludert bilder) som legges ut.

4.7 Chat

Ved bruk av chatte funksjonalitet skal man være oppmerksom på:

- ✓ Ikke oppgi sensitiv informasjon, logger kan lagres og komme på avveie.

4.8 Risikovurderinger

Ved større endringer i organisasjonen, innføring av nye digitale tjenester, når man tar i bruk ny teknologi eller ved inngåelse av større kontrakter skal Informasjonssikkerhetsrådgiver

(ISR) kontaktes og bistå med å gjennomføre risikovurderinger for å avklare hvilke personvern og informasjonssikkerhetstiltak som er fornuftige og tilstrekkelige.

4.9 Hendelsesrapportering (Avvikshåndtering)

Rapportering om sikkerhetshendelser begrenser konsekvensene av et sikkerhetsbrudd.

Rask rapportering er viktig for å oppfylle krav til eventuell melding til Datatilsynet og eventuelt til de ansatte, studenter og søkere det gjelder innen gitte frister.

Rapporter betydelige avvik i informasjonssikkerhet eller gjeldende sikkerhetsbestemmelser til informasjonssikkerhetsrådgiver (eller nærmeste overordnede) umiddelbart gjennom avviksrapporteringssystemet (Meld avvik). Eksempler på betydelige avvik er:

- ✓ Brudd på personvern
- ✓ Uautorisert tilgang til datasystem
- ✓ Sensitiv informasjon og passord på avveie
- ✓ Feil utsendelse av sensitiv informasjon (inkl. via e-post)
- ✓ Tap eller tyveri av bærbart utstyr
- ✓ Sikkerhetshull i IT-system
- ✓ Fysisk eller elektronisk ubeskyttet transport av sensitiv informasjon
- ✓ Uautorisert endring av informasjon
- ✓ Bruk av uautorisert programvare
- ✓ Sabotasje eller hærverk som berører informasjonstilgang
- ✓ Virusangrep
- ✓ Phishing

5 Ordforklaringer

Begrep	**Forklaring**	
Informasjons-sikkerhet	Beskyttelse av informasjon mot handlinger som kan føre til brudd på:	
	Konfidens-ialitet	dvs. sikkerhet for at kun autoriserte får tilgang til informasjonen.
	Integritet	dvs. sikkerhet for at informasjonen er fullstendig, nøyaktig og gyldig.
	Tilgjenge-lighet	dvs. sikkerhet for at informasjonen er tilgjengelig ved behov.
Bruker	Enhver som har tilgang til informasjon ved NMH.	
Medarbeider	Enhver som jobber ved NMH, enten som ansatt eller som innleid.	
Behandling	Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, etc.	
Behandlings-ansvarlig	en … som … bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes…	
Personopplysninger	Personvernforordningen Artikkel 4 definerer personopplysninger som: ”*Opplysninger og vurderinger som kan knyttes til en enkeltperson.”* Eksempler på ikke sensitive personopplysninger er personnummer, fødselsdato, adresse, telefonnummer, yrke og arbeidssted, IP adresser, bilder, video etc,.	
Sensitive person-opplysninger	Personvernforordningen Artikkel 9 definerer sensitive personopplysninger som: *Opplysninger om:* ✓ rasemessig eller etnisk opprinnelse, ✓ politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, ✓ samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, ✓ helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering	

ISR - Informasjonssikkerhetsrådgiver
LSIS - Ledelsessystem for informasjonssikkerhet