NHH	**STYRINGSSYSTEM FOR INFORMASJONSSIKKERHET** Styrende dokumenter		Gradering: Åpen
	Versjon: 1.1	**Godkjent dato:** 19.06.2020	**Dokumentref:**
Tittel: IT-reglement			
Gjelder for: NHH		**Dokumentansvarlig:** IT-avdeling	

1 Formål

Formålet med IT-reglementet er å regulere bruken av IT-systemer og -utstyr ved Norges Handelshøyskole (NHH)

2 Virkeområde

Med IT-systemer menes her all programvare, datasystemer, infrastruktur og utstyr som benyttes til digital informasjons- og databehandling, samt informasjon og data som lagres i disse. Digital kommunikasjon knyttet til disse inngår også samt IT-systemer som inngår i annen infrastruktur og utstyr.

Med IT-systemer ved NHH menes IT-systemer som finnes på NHH, eies eller disponeres av NHH, eller som stilles til rådighet for NHHs brukere fra eksterne parter, leverandører eller andre på oppdrag, avtale eller i forståelse med NHH, og som benyttes av NHHs brukere eller samarbeidspartnere til formål knyttet til NHHs virksomhet.
Reglementet gjelder for:

- For ansatte, studenter, gjester og andre som er gitt tilgang til IT-systemer ved NHH heretter kalt brukere.
- All bruk av NHHs IT-systemer.

I tillegg gjelder reglementet for

- Brukernes og annen tredjeparts IT-systemer, i den utstrekning de benyttes til å utføre oppgaver knyttet til NHHs virksomhet, uavhengig av om anlegget er plassert på NHHs område eller ikke.
- Privat og annet tredjeparts IT-utstyr som er koblet til NHHs IT-infrastruktur (f.eks. nettverk) uavhengig av hvilket formål det brukes til.

3 Tilgang til NHHs IT-tjenester og -systemer

Som student eller ansatt ved NHH skal du ha en brukerkonto hos NHH som gir tilgang til IT-systemer.

Andre kan gis tilgang til NHH sine IT-systemer etter tjenstlig behov. Tilgang til de ulike systemer og tjenester autoriseres av systemeier.

4 Avslutning av ansettelsesforhold eller studier, mv.

I god tid innen opphør av ansettelsesforhold eller avslutning av studier ved NHH, skal du som bruker rydde din konto. Filer som tilhører saker du som ansatt har hatt til behandling, skal forelegges din overordnede for vurdering. Slike filer skal ikke slettes før aktuell enhet har godkjent dette. Du som ansatt skal sørge for at filer som kan tenkes å ha betydning for NHH sin virksomhet, men som ikke tilhører bestemte saker, forelegges nærmeste overordnede som avgjør om filene skal slettes eller eventuelt arkiveres.

4.1 Avslutning av brukerkonto og epostkonto mv.:

Studenters brukerkonto sperres tre måneder etter at studieretten opphørte.

Ansattes brukerkonto sperres ved avslutning av ansettelsesforholdet. Ansattes e-postkasse avsluttes ved arbeidsforholdets opphør, med mindre det foreligger særskilt behov for å holde e-postkontoen åpen i en kort periode etter opphøret.

Som pensjonist ved NHH kan du søke om å få beholde din brukerkonto med endrede tilganger. Dette skal på forhånd godkjennes av leder ved den enheten hvor du sist var ansatt.

Andre brukere sin brukerkonto ved NHH sperres når tilknytningen til NHH opphører, eller godkjent tidsperiode utløper.

Data knyttet til en brukerkonto slettes automatisk seks måneder etter at brukerkontoen ble sperret. Data kan bli lagret i backup-systemer ut over denne perioden, men ikke lenger enn ett år.

Ved en brukers dødsfall blir brukerkontoen sperret umiddelbart. Brukerkontoen slettes etter seks måneder med mindre det er krevd innsyn eller gjort gjeldende rett til materiale som beskrevet i dette reglementet.

4.2 Tilbakelevering av utstyr, programvare og lisenser

IT-utstyr og lisenser tilhørende NHH skal leveres tilbake. Alle kopier av programvare, dokumentasjon og data eid av, eller utlånt fra NHH, skal slettes fra privat utstyr.

5 Bruk av NHHs IT-tjenester og -systemer

NHHs IT-systemer skal brukes til å utføre oppgaver knyttet til NHHs virksomhet. Din bruk av NHHs IT-tjenester og -systemer må ikke stride mot lov, forskrift eller NHHs regler.

Du skal hindre at andre får tilgang til din brukerkonto. Du skal heller ikke søke å skaffe deg tilgang til andres brukerkonto.

Du skal hindre at uønskede personer får tilgang til NHHs IT-systemer.

Du skal ikke uten tillatelse endre eller modifisere NHHs IT-systemer, eller på annen måte forårsake at de virker på en annen måte enn forutsatt.

Du plikter å respektere opphavsrett og lignende rettigheter til programvare, data og annen digital informasjon som publikasjoner, bilder, musikk, film etc.

Du skal påse at den enkeltes personvern overholdes og ikke krenkes.

Du skal unngå bruk av IT-systemer som kan utsette NHH for vesentlig tap av omdømme.

Du plikter straks å rapportere forhold som kan ha betydning for IT-sikkerheten og personvern ved NHH til IT-avdelingen (hjelp@nhh.no).

6 Aktivitetslogg og kontroll

NHHs IT-systemer er tilrettelagt med løsninger for registrering av aktiviteter (logging) og sikkerhetskopiering. Disse skal blant annet kunne brukes til å dokumentere lovbrudd eller avvik fra interne regler og rutiner, og avdekke/oppdage brudd på sikkerheten i IT-systemene.

IT-avdelingen ved IT-leder har hovedansvar for kontroll med tilgang til NHHs nettverk og generelle IT-systemer, samt for bærbart utstyr og utstyr som benyttes utenfor NHH, og har myndighet til å utøve denne kontrollen i henhold til NHHs styringssystem for informasjonssikkerhet og personvern.

7 Arbeidsgivers innsyn

7.1 Virkeområde for forskrift om arbeidsgivers innsyn

NHH har på visse vilkår rett til innsyn i arbeidstakers e-postkasse m.v., jfr. arbeidsmiljøloven § 9-5 og forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale. Forskriften gjelder både nåværende og tidligere arbeidstakere.

Med e-postkasse menes e-postkasse arbeidsgiver har stilt til arbeidstakerens disposisjon til bruk i arbeidet. Reglene gjelder tilsvarende for arbeidsgivers adgang til gjennomsøkning av og innsyn i arbeidstakerens personlige område i virksomhetens datanettverk, IT-systemer eller annet elektronisk utstyr som arbeidsgiver har stilt til arbeidstakerens disposisjon til bruk i arbeidet. Bestemmelsene gjelder tilsvarende for innsyn i opplysninger som er slettet fra de nevnte områdene, men som finnes på sikkerhetskopier eller tilsvarende.

7.2 Vilkår for innsyn

NHH har bare rett til innsyn i opplysninger som er lagret på områder nevnt under punkt 7.1

a) når det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten, eller
b) ved begrunnet mistanke om at arbeidstakerens bruk av e-postkasse eller annet elektronisk utstyr medfører grovt brudd på de plikter som følger av arbeidsforholdet eller kan gi grunnlag for oppsigelse eller avskjed.

NHH har ikke rett til å overvåke arbeidstakerens bruk av elektronisk utstyr, herunder bruk av Internett, med mindre formålet med overvåkingen er

a) å administrere virksomhetens datanettverk eller
b) å avdekke eller oppklare sikkerhetsbrudd i nettverket.

7.3 Prosedyrer ved innsyn

Du som arbeidstaker skal så langt som mulig varsles og få anledning til å uttale deg før NHH gjennomfører innsyn. I varselet skal NHH begrunne hvorfor vilkårene for innsyn anses å være oppfylt og orientere deg om dine rettigheter ved innsyn.

Du som arbeidstaker har innsigelsesrett etter personvernforordningens artikkel 21.

Du skal så langt som mulig gis anledning til å være til stede under gjennomføringen av innsynet og har rett til å la deg bistå av tillitsvalgt eller annen representant.

Er innsyn foretatt uten forutgående varsel eller uten at du som arbeidstaker var til stede, skal du gis skriftlig underretning om dette så snart innsynet er gjennomført. Underretningen skal, i tillegg til opplysninger om hvorfor NHH anså vilkårene for innsyn som oppfylt, inneholde opplysninger om hvilken metode for innsyn som ble benyttet, hvilke e-poster eller andre dokumenter som ble åpnet samt resultatet av innsynet.

Unntakene fra rett til informasjon i personopplysningsloven § 16 gjelder tilsvarende.

Innsyn må så langt som mulig gjennomføres på en slik måte at opplysningene ikke endres og at frembrakte opplysninger kan etterprøves.

Åpnede e-poster, dokumenter eller tilsvarende som det viser seg at ikke er nødvendige eller relevante for formålet med innsynet, skal straks lukkes. Eventuelle kopier skal slettes.

Begjæring om innsyn fremmes av øverste leder ved enheten i samråd med HR-avdelingen og systemeier. Beslutning om innsyn fattes av rektor.

Ved dødsfall kan rektor beslutte at det skal foretas innsyn

- når det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten, eller
- når dødsboet har gjort gjeldende rett til materiale

Begjæring om slikt innsyn fremmes av øverste leder ved enheten i samråd med HR-avdelingen og systemeier.

Anmodning eller begjæring om innsyn i informasjon, logger og sikkerhetskopier fra offentlige myndigheter når dette har hjemmel i lov eller forskrift, samt ved beslutning av retten, behandles av rektor.

8 Sanksjoner

Brudd på IT-reglementet og/eller underliggende politikkdokument, retningslinjer, prosedyrer og rutiner kan føre til disiplinærtiltak mot deg som bruker av NHHs systemer og tjenester.

NHH kan uten opphold fjerne utstyr eller programvare som:

- forårsaker skade på NHHs IT-infrastruktur, eller
- forårsaker skade på NHHs eller andre brukeres informasjon/data, eller
- skaper forstyrrelser i NHHs IT-infrastruktur eller
- på annen måte hindrer oppnåelse av NHHs formål med IT-infrastrukturern

Overtredelse av reglementets bestemmelser kan føre til at du nektes tilgang til hele eller deler av NHHs IT-systemer. I tillegg kan det medføre sanksjoner etter andre regler, så som disiplinærreaksjoner etter statsansatteloven, advarsel eller utestenging fra studier og eksamen etter universitets- og høyskoleloven, erstatningsansvar, straffeansvar o.a.

Midlertidig utestenging i inntil 14 virkedager kan besluttes av øverste leder ved enheten (institutt, fakultet eller avdeling i sentraladministrasjonen) etter samråd med systemeier. HR-avdelingen skal straks varsles dersom utestengingen gjelder en arbeidstaker. Utestenging ut over 14 virkedager besluttes av rektor.

Midlertidig utestenging kan skje ved berettiget mistanke om at

- du har gjort deg skyldig i alvorlige overtredelser, eller at
- du eller ditt IT-utstyr utgjør en vesentlig trussel for informasjonssikkerheten.

I vurderingen skal det legges vekt på overtredelsens grovhet, om du tidligere har overtrådt reglementet, hvilke følger en utestenging vil få for deg som bruker og forholdene ellers.

Klage på vedtak truffet med hjemmel i statsansatteloven, universitets- og høyskoleloven og forvaltningsloven følger disse lovenes regler om klage.