



# POLITIHØGSKOLEN

## Instruks for IKT

NORWEGIAN POLICE UNIVERSITY COLLEGE

Vår ref: 201400125  
Utgitt: 15.08.2005  
Opphever: IKT-instruks for Politihøgskolen 2005  
Revidert: 21.11.2013  
Ansvarlig: IKT seksjonen



### 1 Hensikt og omfang

Politihøgskolens IKT-instruks angir retningslinjer for bruk av skolens samlede IKT ressurser. Hensikten er å ivareta den sikkerhet som kreves ved bruk av nettverk, anlegg og informasjon som Politihøgskolens ansatte/kursdeltaker/studentene og innleide gis tilgang til ved Politihøgskolens lokasjoner.

#### 1.1 Hvem gjelder den for

IKT-instruksene gjelder for ansatte, studenter, kursdeltakere, alt innleid personell og andre som gis tilgang til Politihøgskolens IKT-utstyr, i eller utenfor Politihøgskolens lokaler og lokasjoner. Instruksene gjelder også bruk av Politihøgskolens IKT-utstyr gjennom oppkobling, med privat IKT-utstyr, når og dersom det er tillatt.

Instruksene er en del av arbeidsavtalen for ansatte. Studenter skal også gjøre seg kjent med instruksene.

#### 1.2 Definisjoner

##### 1.2.1 IKT-utstyr

Med "IKT-utstyr" menes datamaskiner, Pc-er, skjermer, nettverk, programmer, skannere, sluttbrukerutstyr, tilleggsutstyr, skrivere, kameraer, fotoapparater, AV-utstyr (projektorer, video, TV, konferansesystem og musikk-anlegg) som stilles til disposisjon av høgskolen, inklusive lokale, nasjonale og internasjonale nettverk eller andres anlegg, som man får tilgang til gjennom slike ressurser.

##### 1.2.2 Brukere

Brukere er, ansatte, studenter, kursdeltakere, alt innleid personell og andre som har et fast eller midlertidig kontraktsforhold til høgskolen, og som får tilgang til IKT-utstyret. Dette gjelder også felles brukerkontoer og gjestekontoer.

##### 1.2.3 Helpdesk IKT

Ved Politihøgskolen vil det være en eller flere ansatte, på samtlige lokasjoner, som har ansvar for høgskolens IKT-utstyr. I denne instruksene er disse kalt Helpdesk IKT.

##### 1.2.4 Personlig epostkasse/filområde

Epostkasse/filområde tilknyttet til en enkelt bruker. Kan inneholde virksomhetsrelatert (informasjon relatert til virksomheten som det er behov å begrense tilgangen til) og privat informasjon. Eksempelvis så er H: personlig filområde til skolens ansatte/studentene.

##### 1.2.5 Felles e-postboks/Fellesområder

E-postboks/felles filområde som flere har tilgang til, og som flere brukere er tilknyttet. Privat innhold e-post/private filer skal ikke lagres her. Nettverksplasseringene I: og P: er fellesområder for hele Politihøgskolen. Lokasjonene kan ha noen i tillegg til disse.

### **1.2.6 Virksomhetsrelatert**

E-post, filer, dokumenter etc. som er knyttet til gjennomføring av arbeidsoppgaver for Politihøgskolen.

### **1.2.7 Privat e-post/private filer**

E-post og filer med innhold av privat art, så som e-post til personlige kontakter, hilsener, e-post sendt til og fra fagforening, tillitsvalgte og helsetjeneste, e-post mapper/e-post merket med "Privat" og mapper og innholdet til disse/filnavn på filserver merket "Privat"

### **1.2.8 Malware**

Malware er satt sammen av de engelske ordene "Malicious" og "Software" og er en fellesbetegnelse på ondsinnet programvare.

Eksempler på malware er (eksemplene er ikke utfyllende) datavirus, ormer, trojanere og keyloggere.

## **2 Gjennomføring**

### **2.1 Tilgang**

En bruker som skal ha tilgang til IKT-utstyret, skal ha et brukernavn, kalt brukerkonto, og et personlig passord. For at brukere skal få tildelt brukerkonto, må det foreligge en gyldig arbeidsavtale. Brukerkontoer opprettes automatisk, med unntak av korttidsinnbeordrede og timelønnede. Studenter får gyldig brukerkonto når det foreligger godkjent studieplass og aktivt studieprogram.

### **2.2 Trådløst nett**

Politihøgskolen tilbyr et gjestenett som er tilgjengelig for alle, og som er adgangskontrollert. Dette forutsetter at gjester som bruker dette nettet er blitt kjent med INSTRUKSEN.

Helpdesk IKT forbeholder seg retten til, uten varsel, å slå av gjestenett når forholdene krever det.

### **2.3 Rettigheter**

Med en brukerkonto følger det rett til å bruke de tilganger som brukeren er gitt tillatelse til i høgskolens eller politiets nettverk.

### **2.4 Opplæring**

Enhver bruker skal ha gjennomgått nødvendig opplæring. Enhver bruker har selv ansvaret for å melde fra om manglende opplæring (f.eks. hvor ligger skolens maler og hvordan skal disse brukes, hvordan brukes MinTid) til nærmeste leder.

## **3 Ansvar, plikter og brukerstøtte**

Enhver bruker er selv ansvarlig for å følge de regler og bestemmelser som gjelder for bruk av de forskjellige IKT-systemene og for behandling/makulering av konfidensiell informasjon (på papir eller elektronisk medium).

Rektor, nærmeste leder eller Helpdesk IKT kan til enhver tid kreve utlevert utstyr returnert.

### **3.1 Passord**

Brukernavn og passord (brukeridentitet) er strengt personlig og skal ikke oppgis eller lånes til andre.

### **3.2 Låse/overlate arbeidsstasjon**

Lås arbeidsstasjonen din hver gang du forlater plassen. Logg alltid av maskinen før du overlater arbeidsstasjonen til andre.

### **3.3 Beskytt innsyn og tilgang**

Beskytt skjermen slik at uvedkommende ikke får innsyn fra vinduer og korridorer. Lås dører til rom som ikke er under oppsikt.

### 3.4 IKT-utstyr som kan kobles til nettverk

Utstyr som ikke er tildelt av IKT, skal ikke tilkobles nettverket (eks. pc, printer, skanner, hubber). Forespørsel om slik tilkopling skal rettes til Helpdesk IKT. Unntak fra dette gjelder tilkobling til skolens trådløse gjestenett, se "2.2 Trådløst nett".

### 3.5 Brukerstøtte

- Brukerstøtte gis kun til IKT-utstyr som Helpdesk IKT har anskaffet.
- I noen grad vil Helpdesk IKT være behjelpelig med studenters maskiner. Dette vil Helpdesk IKT opplyse om.
- Brukerstøtte til privat formål og behov ytes ikke.

#### 3.5.1 Tap, skade, feil, mangler, problemer, uansvarlig og uaktsom bruk

Utlevert IKT-utstyr er brukerens ansvar og skal beskyttes mot skade, hærverk, tyveri og misbruk. Det er ikke tillatt å forlate utstyret uten tilfredsstillende sikring. Brukeren har vanlig aktsomhetsansvar.

Ved tap eller skade på IKT utstyr skal dette meddeles Helpdesk IKT umiddelbart.

Defekt IKT utstyr skal ikke repareres selv, men meddeles Helpdesk IKT umiddelbart.

### 3.6 Bruk av skolens IKT-utstyr

Før skolens utstyr tas i bruk plikter brukeren (og ansvarlige for innleid personell, foredragsholdere etc.) å sette seg inn i brukerdokumentasjon eller sikre seg opplæring for å unngå feil bruk og ødeleggelse av utstyr som kan medføre risiko for driftsforstyrrelser eller tap av data, programvare eller utstyr.

#### 3.6.1 Bruk av fellesområdet

Data som produseres for, eller på annen måte tilhører Politi­høgskolen (virksomhetsrelatert), skal lagres på fellesområdene, der det tas sikkerhetskopi. Informasjon som er lagret på lokale disk­er, eksterne skyløsninger, minnepenner osv. tas ikke sikkerhetskopi av, og kan i enkelte tilfeller også få andre eiendomsforhold (spesielt ved lagring i eksterne skyløsninger).

#### 3.6.2 Bruk av privat e-postboks/filområde

Enhver brukers private hjemmeområdet er ikke ment for arkivering av privat informasjon, men for informasjon relatert til virksomheten som det er behov å begrense tilgangen til. Allikevel, åpenbar personlig og privat informasjon kan lagres i mapper merket «PRIVAT».

#### 3.6.3 Avmontering/flytting

Det er ikke tillatt å koble fra IKT-utstyr, uten at det er avtalt med Helpdesk IKT.

#### 3.6.4 Tilkobling av enheter

Eksterne lagringsenheter, f.eks. minnepinner, som ikke er ens egne eller som blir funnet forlatt, skal ikke under noen omstendigheter kobles til skolens IKT-utstyr. Forlatt utstyr overleveres Helpdesk IKT. Egne lagringsenheter skal ikke ukritisk lånes bort til eksterne aktører (eller 3. part) for å unngå å få Malware på skolens IKT-utstyr.

#### 3.6.5 Bruk av skolens data- og undervisningsrom

Det er ikke tillatt for andre enn høgskolens ansatte, studenter, kursdeltagere og andre autoriserte brukere å benytte skolens datarom og IKT-utstyret som finnes der. Det er heller ikke adgang for andre enn nevnte brukere, til disse rommene.

#### 3.6.6 Bruk av mobilt bredbånd/oppkobling i utland

Det kan oppstå betydelige kostnader som følge av (uaktsom) tilkobling i utlandet. Alternativt, bruk hotellets/vertens internett-tilgang om mulig.

#### 3.6.7 Hacking/kartlegging/annen uautorisert tilgang

Forsøk på å hacke eller kartlegge nettverket på Politi­høgskolen, eller andres nettverk, er ikke tillatt.

#### 3.6.8 Utenforliggende formål

Enhver bruker skal påse at Politi­høgskolens IKT-utstyr ikke brukes til virksomhet som er i strid med norsk lov eller alminnelig sømmelighet for Politi­høgskolen.

### **3.6.9 Ulovlig kopiering**

Det er ikke adgang til å kopiere datamaskinprogrammer ved hjelp av Politihøgskolens IKT-utstyr utover det som følger av avtaler om disposisjonsrett (lisensavtaler).

### **3.6.10 Spill/underholdning**

Spill og underholdnings-programvare skal unngås, fordi det kan beslaglegge ressurser som går utover skolens drift. Dette gjelder også lagring av ikke virksomhetsrelaterte multimedia-filer på skolens på skolens IKT-utstyr.

## **3.7 Installasjon av programmer**

Enhver bruker skal ikke installere programvare som ikke er godkjent av Helpdesk IKT.

### **3.7.1 Uønsket programvare**

Enhver bruker skal bidra til at Politihøgskolens anlegg holdes fritt for malware (skadevare).

## **3.8 Arkivverdig e-post**

Arkivverdige e-poster som mottas i personlig epostkasse, skal videresendes arkivet for journalføring og arkivering.

## **3.9 Straffbare forhold**

For å sikre samt utlevere bevis, kan personlig epostkasse og hjemområde med mer, bli speilkopiert (behovet skal dokumenteres).

## **4 Sikkerhet og personvern**

Enhver bruker plikter å gjøre seg kjent med de regler som særlig gjelder for lagring og bruk av personopplysninger.

### **4.1 Logging**

All aktivitet knyttet til din brukerkonto logges og er gjenstand for sporing, både på Politihøgskolen, Politinett og ikke minst internett. All kommunikasjon på nettet kan spores tilbake til maskinen du sitter på.

### **4.2 Etisk bevissthet og aktsom nettbruk**

Som ansatt og student ved Politihøgskolen, forplikter den enkelte seg til å ha et reflektert forhold til hvilke søk og hvilke nedlastinger av materiale som foretas. Du må også være spesielt aktsom med hensyn til hva som kommuniseres til omverdenen. Se for øvrig etiske retningslinjer for statstjenesten og Politidirektoratets innføring i etikk for ansatte i politi- og lensmannsetaten.

### **4.3 Privat bruk av internett/e-post**

Politihøgskolen tillater begrenset privat bruk av internett/e-post, og forutsetter aktsom opptreden. Hvis omfanget av privat bruk tiltar i løpet av arbeidstiden, vil skolen uten videre varsel begrense bruken, for å sikre virksomhetsrelatert kommunikasjon. Det oppfordres til at bruker oppretter og bruker en privat e-post adresse til private formål.

### **4.4 Sikkerhetsprogramvare**

Det er ikke tillatt, helt eller delvis, å slå av/bytte ut sikkerhetsprogramvare/sikkerhetsinnstillinger på skolens IKT-utstyr.

### **4.5 E-post**

Den enkelte skal bruke elektronisk post med tilstrekkelig aktsomhet. E-post er normalt ukryptert, og kan sammenlignes med et postkort; enhver som ønsker det kan lese hva som er skrevet.

### **4.6 Informasjonssikkerhet**

Enhver bruker må vurdere om informasjon som inneholder personopplysninger eller sensitive opplysninger skal håndteres/avhendiges/makuleres særskilt, i tråd med lovgivning. Gradert informasjon skal ikke behandles på utstyrt som ikke er godkjent ihht. Sikkerhetsloven.

#### **4.7 Mobiltelefon**

Ikke ta mobiltelefonen med inn i rom der det diskuteres sensitive eller sikkerhetsgradert informasjon. Be andre møtedeltakere om å legge fra seg mobiltelefonene før møtet starter.

#### **4.8 Nettsamfunn/Sosiale medier/Informasjonskanaler**

Det er ikke uvanlig at informasjon fra ulike sider ved ulike nettsamfunn misbrukes. Denne informasjonen, satt sammen med informasjon fra andre kilder som verken bruker eller Politihøgskolen har ansvar for, kan gi informasjon som samlet sett er sensitivt eller i verste fall gradert. Vær varsom med informasjon og opplysninger som deles, og still spørsmål om det er nødvendig å dele disse.

#### **4.9 Personvern**

Alle behandlinger av personopplysninger krever et gyldig og saklig behandlingsgrunnlag.

Det er den til enhver tid gjeldende lov og forskrift om personopplysninger som ligger til grunn for personvern.

##### **4.9.1 Personers oppholdssted/annet**

Generelle spørsmål om personer ved Politihøgskolen, og deres ansettelsesforhold eller studentforhold, skal ikke besvares over telefon.

#### **4.10 Bilder av ansatte, studenter, skole eller "Politi-installasjoner"**

Uten samtykke og uten at det foreligger tjenstlige behov, skal ikke bilder av ansatte, studenter, skole eller "Politi-installasjoner" legges ut på nettsamfunn eller andre informasjonskanaler/sosiale medier som f.eks. Facebook, LinkedIn, XING, blogger osv. (listen er ikke uttømmende).

#### **4.11 Innsyn**

Enhver bruker skal være med på å motvirke behov for innsyn av arbeidsgiver, ved å etterkomme krav om arkivering samt lagring av virksomhetsrelaterte dokumenter der det er naturlig.

Ved planlagte fravær over lengre tid, er det brukerens ansvar å sørge for at e-post som er virksomhetsrelatert ikke blir liggende uåpnet, f.eks. ved hjelp av fraværsassistent som sier noe om stedfortreder.

## **5 Unntak fra denne instruks**

### **5.1 IKTs rett til å søke tilgang til reserverte områder**

#### **5.1.1 Overvåkning av bruk av IKT-utstyret**

Hvis bruken av arbeidsstasjon, terminal eller annet sluttbrukerutstyr på grunn av driftssikkerhet eller av andre hensyn må overvåkes av driftspersonalet, skal dette opplyses om, der det er hensiktsmessig.

#### **5.1.2 Skanning**

Helpdesk IKT vil uregelmessig foreta skanning av alt IKT-utstyr for å avdekke uautorisert eller ulisensiert programvare, underholdningsfiler (musikk, video etc.), uønsket eksekverbar kode (malware) og annet innhold som ikke er i tråd med IKT-instruks eller som ikke er virksomhetsrelatert.

#### **5.1.3 Taushetsplikt for Helpdesk IKT**

Helpdesk IKT har taushetsplikt med hensyn til opplysninger, personlige eller andre forhold om brukeren eller brukerens virksomhet. Unntak når forhold representerer brudd på denne instruks og/eller norsk lov.

#### **5.1.4 Særskilt om ansvar for krimteknisk lab AV-utstyr:**

Ansvar for krimteknisk lab og dens utstyr er lagt til Etter- og viderutdanningsavdelingen.

## **6 Utlevering av innhold, lovbrudd og brudd på skolens IKT-instruks**

### **6.1 Utlevering av personlig epostkasse/hjemmeområde**

Ved skriftlig henvendelse fra Politi eller påtalemyndighet, skal innhold av en navngitt brukers personlige epostkasse/hjemmeområde sikres ved kopi. Kopi utleveres ved forevisning av skriftlig beslutning fra kompetent myndighet.

### **6.2 Spesielt for eksterne brukere**

For eksterne brukere (ikke studenter/ansatte), vil brudd på disse reglene kunne medføre at oppdraget faller bort, uten noen form for erstatning.

Politihøgskolen forbeholder seg retten til å kreve erstatning for tap/skade i henhold til punkt "6.3 Følger av brudd".

### **6.3 Følger av brudd**

Ved brudd på, eller mistanke om brudd på høgskolens IKT-instruks, kan Helpdesk IKT inndra/utestenge brukerrettigheter til IKT-systemer.

Sjefen for Politihøgskolen eller den myndighet som har rekvirert brukerkontoen, kan inndra brukerrettighetene permanent.

## **7 Annet**

### **7.1 Erstatningsansvar.**

Politihøgskolen fraskriver seg ansvar for økonomisk tap som følge av feil eller mangler i programmer, data, bruk av opplysninger fra tilgjengelige databaser eller andre opplysninger innhentet gjennom nettet o.a.

### **7.2 Kassasjon/Avhending**

IKT-Utstyr som skal kasseres, skal returneres til Helpdesk IKT. Bruker skal ikke selv kassere eller sende til kassasjon.

### **7.3 Fratreden**

Enhver ansatt som slutter skal sørge for å orientere samarbeidspartnere og andre instanser, om hvem som overtar oppgaver og ansvar, henholdsvis henvise til leder slik at kommunikasjon (via epost/telefon) kan fortsette uten avbrudd.

Alt utlevert IKT-utstyr, også programvare, skal leveres tilbake, med mindre annet er avtalt med Helpdesk IKT. Virksomhetsrelatert informasjon skal være overlevert arkiv/nærmeste leder. Privat epostkasse/filområde slettes umiddelbart etter siste arbeidsdag.

### **7.4 Dødsfall**

Ved dødsfall slettes e-post og hjemmeområde, med mindre det tydelig fremgår av innhold at det er virksomhetsrelatert. Før sletting finner sted, vil innsyn foretas. Automatisk videresending til nærmeste leder eller automatisk svar til avsender, aktiveres ikke.

Overlevering av innhold som bilder og epost-veksling, som er tydelig merket «PRIVAT» eller ligger i en mappe merket «PRIVAT» til nærmeste pårørende, finner ikke sted.

Unntaksvis kan vi bistå etterlatte, dersom det kan gi svar som f.eks. i tilfeller det er snakk om selvmord, jmf. Datatilsynet.

### **7.5 Varsling/Meldeplikt/Medansvar**

Alle uønskede hendelser i form av brudd på denne instruks samt gjeldende lovgivning, skal varsles til Helpdesk IKT uten ugrunnet opphold.

Enhver bruker har et medansvar med å sikre at tilgangen til IKT-systemene er i henhold til faktiske behov, og at avvik meddeles Helpdesk IKT og leder umiddelbart.

## 8 Referanse

### 8.1 Relevante formularer/lister

- IKT-instruksen skal, sammen med taushetserklæring, underskrives av brukere før tilgang til skolens IKT-utstyr gis.
- Taushetserklæring for ansatte/eksterne: [Taushetserklæring ansatte.docx](#)
- Taushetserklæring for studenter: [Taushetserklæring student.docx](#)

### 8.2 Relevante lover/forskrifter

- Straffelovens §§ 121, 145 annet og fjerde ledd, 145b.
- Personopplysningsforskriften kapittel Kapittel 9. Innsyn i e-postkasse mv.
- Fra datatilsynets merknader til forskriften:
  - *De pårørende etter dødsfall har ikke uten videre krav på innsyn i den avdødes e-post mv. Det samme gjelder dødsboet. Dette må vurderes konkret etter §§ 8, 9 og 11. Hensynet til eventuelle tredjepersoner skal veie tungt.*
  - [http://datatilsynet.no/Global/05\\_regelverk/epostforskriften\\_merknader.pdf](http://datatilsynet.no/Global/05_regelverk/epostforskriften_merknader.pdf)

### 8.3 Relevante retningslinjer

- Etske retningslinjer for statstjenesten  
[http://www.regjeringen.no/upload/FAD/Vedlegg/Arbeidsgiverpol/Etske\\_retningslinjer\\_r ev2012.pdf](http://www.regjeringen.no/upload/FAD/Vedlegg/Arbeidsgiverpol/Etske_retningslinjer_r ev2012.pdf)
- Grunnleggende verdier, moral og etikk – en innføring i etikk for ansatte i politi- og lensmannsetaten [https://www.politi.no/vedlegg/rapport/Vedlegg\\_1939.pdf](https://www.politi.no/vedlegg/rapport/Vedlegg_1939.pdf)