



INSTRUKS

NORWEGIAN POLICE UNIVERSITY COLLEGE

Vår ref: 201400125, 19/02697
Utgitt: 15.08.2005
Opphever: IKT-instruks for Politihøgskolen
Revidert: 21.11.2013, 21.08.2019
Ansvarlig: Rektor / Avdelingsleder Strategi og Virksomhetsstyring

IKT-instruks for Politihøgskolen

1 Hensikt og omfang

Politihøgskolens IKT-instruks angir retningslinjer for korrekt bruk av skolens IKT-ressurser. Hensikten er å ivareta den sikkerhet som kreves ved bruk av nettverk, anlegg og informasjon som Politihøgskolens brukere gis tilgang til ved Politihøgskolens lokasjoner, for å oppnå god informasjonssikkerhet ved at krav om konfidensialitet, integritet og tilgjengelighet overholdes.

1.1 Omfang

Denne instruksjonen baserer seg på lover, forskrifter og instruksjoner samt regelverk og policyer fastsatt av Justis- og beredskapsdepartementet (JD), Politidirektoratet (POD), Politiets IKT-tjenester (PIT), og behandlingsansvarlig.

Instruksjonen gjelder også bruk av Politihøgskolens IKT-ressurser gjennom oppkobling, med private IKT-ressurser (egen PC f.eks.), når og dersom det er tillatt.

1.2 Hvem gjelder den for

IKT-instruksjonen gjelder for brukere som gis tilgang til Politihøgskolens IKT-ressurser, i eller utenfor Politihøgskolens lokaler og lokasjoner, med mindre de reguleres av andre avtaler/instruksjoner, der avvikende eller utfyllende retningslinjer er nærmere beskrevet.

1.3 Definisjoner

Definisjonene er samlet i et eget vedlegg til instruksjonen «IKT-instruks 2019 – Definisjoner».

2 Gjennomføring

2.1 Tilgang – leders ansvar

Arbeidsgiver (leder) har ansvar for å sørge for at bruker har tilstrekkelig kjennskap til håndtering av beskyttelsesverdig informasjon, behandling av særskilte kategorier av personopplysninger (sensitive personopplysninger), og at det ved behov er undertegnet taushetserklæring.

En bruker som skal ha tilgang til IKT-ressurser, skal ha en brukerkonto. Det er nærmeste leders ansvar å gi en bruker tilgang. Brukeren kan ikke selv be om tilgang. Det er også nærmeste leders ansvar:

- Å vurdere tjenstlig behov
- Å vurdere om krav fra behandlingsansvarlig er oppfylt, f.eks. om det gis tilgang til informasjon som er underlagt politiregisterloven
- Å vurdere om informasjon er underlagt særskilt behov for tilgangsbegrensning, f.eks. om tilgang har betydning for sikkerheten

- d) Å sørge for at nødvendig opplæring er blitt gitt
- e) Å sørge for at nødvendig kunnskap om relevante instruks og rutiner blir gitt
- f) Å sørge for at brukers tilgangsnivå justeres når brukeren får endrede arbeidsoppgaver, slutter eller går ut i permisjon.
- g) Å sørge for at virksomhetsrelatert informasjon er ivarettatt/overlevert og at utleverte ITK-ressurser leveres tilbake, når brukeren får endrede arbeidsoppgaver, slutter eller går ut i permisjon, jfr. 3.9.10 Innlevering/kassasjon/avhending av IKT-ressurser. Unntak kan gjøres i samarbeid med IKT og forutsetter skriftlig avtale.

2.2 Tilgang til Trådløse nett

Politihøgskolen tilbyr et gjestenett «PHS Gjest» som er tilgjengelig for alle, mot at de registrerer seg med mobil-nummer og at gjeldende instruks for gjestenettet godkjennes før videre bruk.

Tilgang til trådløst nett «PHS» for ansatte, kan kun skje med PC-er/bærbare som er basert på Windows 10 og som er forvaltet av IKT.

Tilgang til trådløst nett «PHS» for studenter (Bachelor og Master), med private PCer, skjer med brukernavn og passord og under forutsetning av at «helsesjekk» gjennomføres og blir bestått. Dette gjelder kun for PCer som er basert på Windows eller Mac OS. Etter- og videreutdanningsstudenter får tilgang ved behov, og som ellers nevnt over.

eduroam¹ gir kun tilgang til internett, basert på brukernavn og passord, og for alle typer enheter uavhengig av hvem som er eier og hvilket operativsystem som er installert.

3 Ansvar, plikter og brukerstøtte

Enhver bruker er ansvarlig for å følge de regler og bestemmelser som gjelder for bruk av IKT-ressursene.

Dersom brukeren ikke har tilgang til skolens regelverk, uavhengig av årsak, er det nærmeste leder som har ansvaret med å formidle disse. Ved behov må det vurderes andre egnede måter å instruere om IKT-instruks og dokumentere at det er blitt gjort, samt innhente underskrevet taushetserklæring.

3.1 Varsling/Meldeplikt/Avvik/Medansvar

Alle uønskede hendelser i form av brudd på denne instruks samt gjeldende lovgivning, uregelmessigheter i systemer og nettverk, mistanke om virusangrep, tyveri av utstyr og tap eller kompromittering av utstyr eller passord, skal uten ugrunnet opphold varsles til Helpdesk IKT eller andre ansvarlige (nærmeste leder, informasjonssikkerhetsansvarlig, personvernombud, sikkerhetsleder, verneombud).

3.2 Krav til bruker om opplæring

Enhver bruker skal ha gjennomgått nødvendig opplæring, i tillegg til de opplæringene som gis som f.eks. Nano-læring i forbindelse med sikkerhetsmåned, eller andre opplæringsmoduler som Politihøgskolen, POD eller PIT iverksetter.

Enhver bruker må umiddelbart melde fra om manglende opplæring til nærmeste leder.

3.3 Krav til bruker om verdivurdering for behandling og avhending av informasjon

Enhver bruker plikter å gjøre seg kjent med de regler som gjelder for behandling av informasjon og personopplysninger, for å sikre korrekt behandling/avhending.

Det gjelder egne krav i forbindelse med forskning.

Spør nærmeste leder/veileder, informasjonssikkerhetsansvarlig eller personvernombud ved nærmere spørsmål.

¹ <https://eduroam.no/information/>

3.4 Brukerkonto

Brukerkonto er personlig og skal ikke oppgis, lånes bort, eller gjøres kjent for andre.

Studenter kan bruke <https://passord.phs.no> dersom det er behov for å bytte/nullstille glemt passord. For ansatte er det <https://ansatt.phs.no>

Passord som benyttes for tilgang til Politihøgskolens eller Politiets IKT-ressurser, må ikke gjenbrukes for pålogging på IKT-utstyr eller -tjenester som ikke er eid av Politihøgskolen eller Politiet.

3.5 Låse/overlate arbeidsstasjon

Lås arbeidsstasjonen din hver gang du forlater plassen. Ikke overlat den til andre uten oppsyn, dersom det er din bruker som benyttes. Du står ansvarlig for de handlinger som utføres i ditt navn.

3.6 Beskytt innsyn og tilgang

Beskytt skjermen/informasjonen slik at uvedkommende ikke får innsyn fra vinduer og korridorer eller tilgang til å lese/endre/slette informasjonen. Lås dører til rom som ikke er under oppsikt.

Dette gjelder uavhengig av hvor arbeidet gjøres fra, f.eks. på buss, tog, offentlige steder, osv.

3.7 IKT-ressurser som kan kobles til nettverk

IKT-ressurser som f.eks. privat PC, skriver, annet nettverksutstyr, osv., som ikke er tildelt av Helpdesk IKT, skal ikke kobles til skolens IKT-ressurser (som f.eks. nettverk).

Forespørsel om slik tilkopling skal rettes til Helpdesk IKT. Unntak fra dette gjelder tilkobling til skolens trådløse nett, se «2.2 Tilgang til Trådløse nett».

3.8 Brukerstøtte

Brukerstøtte gis kun til IKT-ressurser som Helpdesk IKT har anskaffet. I noen grad vil Helpdesk IKT være behjelpelig med studenters utstyr. Dette vil Helpdesk IKT opplyse om.

Brukerstøtte til privat formål og behov ytes ikke.

3.8.1 Tap, skade, feil, mangler, problemer, uansvarlig og uaktsom bruk

Utlevert IKT-ressurser er brukerens ansvar og skal beskyttes mot uønsket tilgang, skade, hærverk, tyveri og misbruk. Det er ikke tillatt å forlate utstyret uten tilfredsstillende sikring.

Dersom skade er forvoldt ved grov uaktsomhet eller forsett, vil Politihøgskolen kunne fremsette krav om erstatning for det tap som har oppstått, jfr. AML. § 14-15 andre ledd bokstav e.

Ved tap eller skade på IKT-ressurser skal dette meddeles Helpdesk IKT umiddelbart, uten ugrunnet opphold. Dersom defekt eller mangler på IKT-ressurser oppstår, ta kontakt med IKT Helpdesk for utbedring av feil/reparasjoner.

IKT-ressurser utlånt fra PHS regnes som PHS eiendom, og skal ikke lånes ut/brukes av andre enn den som har ansvaret for utstyret.

3.9 Bruk av skolens IKT-ressurser

Før IKT-utstyr tas i bruk plikter brukeren å ha gått igjennom nødvendig opplæring, der det er tilgjengelig. For øvrig gjelder 2.1 Tilgang – leders ansvar og 3.2 Krav til bruker om opplæring.

3.9.1 Dokumentsikkerhet

Virksomhetsrelatert informasjon (herunder epost) skal lagres på fellesområder eller i godkjente fagsystemer (FS, Canvas, Public 360 osv., jfr. Instruks for klassifisering av informasjon) umiddelbart.

Dersom det må lagres (midlertidig) på eksterne enheter, skal informasjonen snarest overføres til godkjent system, og makuleres (slette er ikke tilstrekkelig) fra opprinnelige enheter. Permanent behandling på ikke godkjente systemer/ekstern lagring skal ikke forekomme. Unntak gjelder for de tilfeller der Politihøgskolen har inngått avtaler med samarbeidspartnere og som evt. har behandlingsansvaret.

Forskning som inneholder personopplysninger og opplysninger fra reelle lovbrudd skal lagres på godkjente systemer, etter forutgående vurdering av personvernkonsekvenser og samtale med veileder/personvernombud/informasjonsikkerhetsansvarlig ved Politihøgskolen, i de tilfeller det er Politihøgskolen som er behandlingsansvarlig.

Arbeidskrav eller undervisningsopplegg som inneholder opplysninger fra reelle lovbrudd, inkludert, men ikke begrenset til personopplysninger, stedsnavn, åstedsbilder-/video/lyddopptak, skal anonymiseres/pseudonymiseres/avidentifiseres før de behandles (elektronisk og/eller analogt). Dersom det ikke er mulig, skal det ikke behandles på skolens eller personlig IKT-utstyr.

Informasjon som er lagret på PCer/arbeidsstasjoner, minnepinner, CD/DVD og skyløsninger som er utenfor Politihøgskolens/Politiets kontroll, tas det ikke sikkerhetskopi av og kan gå tapt.

Informasjon lagret på eksterne skyløsninger som Politihøgskolen/Politiet ikke har avtaler med kan i enkelte tilfeller også få andre eiendomsforhold, i tillegg til at de kan gå tapt.

Gradert informasjon skal kun behandles, og merkes, i henhold til sikkerhetsloven, på godkjente og merkede IKT-ressurser. Hverken Politinettet eller Politihøgskolens IKT-ressurser er godkjent for dette.

E-post er normalt ukryptert, og kan sammenlignes med et postkort; enhver som ønsker, og som tilegner seg (u)lovlig tilgang, kan lese innholdet. Kryptering av informasjon skal vurderes ut fra informasjonens behov for konfidensialitet og andre beskyttelsesbehov.

Dersom det er midlertidig behov for å transportere/lagre informasjon ved hjelp av ekstern lagring eller e-post, er brukeren ansvarlig for at gjeldende krav om konfidensialitet, integritet og tilgjengelighet er tilstrekkelig ivarettatt.

Ta kontakt med Helpdesk IKT ved behov for bistand.

3.9.2 Installasjon av programvare/uønskede programmer

Enhver bruker skal bidra til å holde IKT-ressursene fritt for skadevare, og skal ikke laste ned/installere programvare som ikke er godkjent av Helpdesk IKT.

Programvare som det er kjent kan påføre skade eller som kan utgjøre en sikkerhetstrussel, skal ikke lastes ned/installeres, med mindre det skjer i kontrollerte former og kontrollerte miljøer. Ta kontakt med informasjonssikkerhetsansvarlig for godkjenning.

Det kan forekomme at vedlegg i epost, eller innhold lastet ned fra internett, kan inneholde skadevare som ikke oppdages av viruskontroll. Ved mistanke om at det ikke er trygt, ta kontakt med Helpdesk IKT.

3.9.3 E-Post sikkerhet/Vedlegg i epost

Vær skeptisk til epost/vedlegg i epost fra ukjente avsendere. E-post kan inneholde skadelig programvare, forsøke å få deg til å trykke på lenke(r) som ber om informasjon du ellers ikke hadde gitt fra deg. Er du usikker på innholdet og/eller vedlegget, ta kontakt med avsender på telefon, henvend deg til Helpdesk IKT, eller slett meldingen.

Ved mistanke om skadelig programvare eller spam e-post, ta kontakt med Helpdesk IKT.

3.9.4 Bruk av IKT-ressurser til personlige formål

IKT-Ressursene skal kun benyttes til virksomhetsrelaterte aktiviteter, men Politihøgskolen tillater begrenset personlig bruk av internett/e-post/personlig filområde, og forutsetter aktsom opptreden.

Enhver brukers personlige e-post/hjemmeområde er ikke ment for arkivering/behandling av personlig informasjon, personlige bilder/filmer osv., men for informasjon relatert til virksomheten som det er behov å begrense tilgangen til i en kortere periode.

Personlig informasjon bør lagres i mapper merket «PRIVAT», henholdsvis merkes med «PRIVAT» i emneteksten på eposten.

Det er ikke lov til å benytte automatisk/manuell videresending av e-post til e-postkontoer utenfor Politihøgskolen, uten godkjenning av IKT Helpdesk og nærmeste leder.

Av sikkerhetsmessige årsaker bør brukere opprette og benytte personlig e-post adresse til personlige formål. Bruk for eksempel «ola.nordmann@hotmail.com» som pålogging til DropBox, Facebook, LinkedIn osv., ikke «olanor@phs.no» eller «ola.nordmann@politiet.no».

3.9.5 Avmontering/flytting

Det er ikke tillatt å koble fra IKT-ressurser som er koblet opp i fellesareal, møterom, tekniske rom osv. uten at det er avtalt med Helpdesk IKT.

3.9.6 Tilkobling av enheter

Eksterne lagringsenheter som ikke er personlige eller som blir funnet, skal ikke under noen omstendigheter kobles til skolens IKT-ressurser. Ta kontakt med Helpdesk IKT.

Eksterne lagringsenheter eller mobiltelefoner/nettbrett osv. bør ikke kobles til andre fremmede enheter for å unngå å få skadevare. Dersom det gjøres, sjekk alltid for skadevare.

3.9.7 Bruk av mobilt bredbånd/oppkobling i utland

Bruk av åpne nettverk anbefales ikke, det kan medføre risiko for å bli hacket. Slå av WiFi/Bluetooth (trådløst) når det ikke er i bruk.

En rekke leverandører av mobilt bredbånd i Norge tilbyr abonnement som inkluderer bruk av data i hele EU/EØS uten at det påløper (betydelige) ekstra kostnader, eller at gjeldende abonnement kan utvides mot en ekstra kostnad, som da inkluderer bruk av data i det landet du oppholder deg. Sjekk hvilket abonnement du har før du reiser.

Dersom du allikevel kobler til åpne nettverk, ikke lagre nettverket for automatisk tilkobling og sjekk at tilkoblinger til nettsteder er sikre ved at det står https:// foran adressen. Bruk VPN for å unngå at kommunikasjonen blir avlyttet.

3.9.8 Reiser (privat og tjeneste)

Reiser til enkelte land medfører behov for ytterligere sikkerhetstiltak. Snakk alltid med nærmeste leder og sikkerhetsansvarlig/informasjonsikkerhetsansvarlig i god tid før avreise for å avklare behov for og omfang av tiltak.

3.9.9 Utenforliggende/ulovlige formål

Enhver bruker skal påse at Politihøgskolens IKT-ressurser ikke brukes til virksomhet som er i strid med norsk lov eller alminnelig sømmelighet for Politihøgskolen, i tillegg til at det ikke går utover virksomhetsrelaterte aktiviteter, eller legger unødvendig beslag på IKT-ressurser.

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

3.9.10 Innlevering/kassasjon/avhending av IKT-ressurser

IKT-ressurser skal ved opphør eller permisjon, returneres til Helpdesk IKT for videre bruk eller korrekt avhending, med mindre annet er skriftlig avtalt.

Det er brukeren som er ansvarlig for å informere om det er være sensitivt eller beskyttelsesverdig informasjon på innlevert utstyr.

3.9.11 Avslutning av bruker-kontoer

Det er brukeren og nærmeste leder som har ansvaret med å sørge for at virksomhetsrelatert informasjon er overlevert arkiv/dokumentasjonsenheten/nærmeste leder før siste arbeidsdag.

Brukeren er selv ansvarlig for å ta vare på personlig informasjon.

Bruker-kontoen til ansatt deaktiveres to dager etter at slutt-dato er satt. Etter ytterligere 88 dager slettes e-postboks og personlig filområde.

Bruker-kontoer til studenter deaktiveres når studieavdelingen har definert studiet som fullført. Fra det tidspunkt studiet er definert som fullført går det to dager til konto er deaktivert, og ytterligere 58 dager til e-postboks og personlig filområde slettes. Tilgang til fleksible læringer opphører umiddelbart.

Det er mulig å terminere bruker-konto og tilhørende e-postboks/personlig filområde umiddelbart ved behov.

4 Sikkerhet og personvern

Behandling av personopplysninger skal kun skje for spesifikke, uttrykkelige, angitte og legitime formål, og før behandling begynner skal det være gjort en vurdering av personvernkonsekvenser med informasjonssikkerhetsansvarlig eller personvernombud.

Ta kontakt med personvernombud og/eller informasjonssikkerhetsansvarlig før behandlingen starter, for å avklare eventuelle krav i lov eller andre styrende dokumenter.

4.1 Sikkerhetsprogramvare

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

4.2 Mobiltelefon

Vær bevisst på at mobiltelefoner, eller andre former for IKT-ressurser som har innebygd kamera/mikrofon, kan ta opp lyd/bilde, spesielt når dette tas med inn i rom der det diskuteres sensitiv informasjon.

Det er ikke anledning å ta med utstyr som ikke er godkjent for gradert behandling i møter, dersom det diskuteres gradert informasjon.

Be i tilfelle møtedeltakere om å legge fra seg utstyret før møtet starter, utenfor møterommet.

For behandling av informasjon på mobil, gjelder forøvrig 3.9.1 Dokumentsikkerhet.

4.3 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, om deg selv/andre.

4.4 Informasjon om personer/installasjoner ved Politihøgskolen eller Innsynsbegjæringer

Generelle spørsmål om personer (ansatte og studenter) eller installasjoner ved Politihøgskolen, skal ikke besvares over telefon.

4.5 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, Instagram, LinkedIn, XING, blogger osv. (listen er ikke uttømmende).

4.6 Innsyn i brukers personlige e-postboks/filområde av arbeidsgiver

Enhver bruker skal være med på å motvirke behov for innsyn av arbeidsgiver, ved å etterkomme krav om behandling virksomhetsrelatert informasjon, jfr. 3.9.1 Dokumentsikkerhet.

Politihøgskolen kan åpne personlige e-postkasser/filområder for å sortere ut og lese informasjon dersom det er god grunn til å tro at det behandles virksomhetsrelatert informasjon og at behandlingen av denne av hensyn til virksomhetens drift ikke kan vente.

Politihøgskolen har, ved mistanke om brudd eller ved brudd på instruks, innsynsrett i all informasjon lagret på våre IKT-ressurser – uten hensyn til lagringssted eller merking. Dette gjelder også i saker som fordrer innsyn i ansattes e-post og personlige dataområder.

Før innsyn gjennomføres, vil bruker bli varslet om dette. Ved innsyn vil verneombud eller en annen representant for brukeren være til stede.

I spesielle tilfeller kan innsyn uten forutgående varsel foretas. Verneombud eller annen representant for den ansatte skal da være til stede, og det skal sendes skriftlig underretning så snart behandlingen er gjennomført.

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 fraværssassistent som sier noe om stedfortreder.

5 Unntak fra denne instruks

All informasjon som behandles digitalt, kontrolleres for skadevare. I tillegg vil Helpdesk IKT uregelmessig foreta skanning av IKT-ressurser for å avdekke uautorisert eller ulisensiert programvare, underholdnings-filer (musikk, video osv.), skadevare, ikke virksomhetsrelatert og annet innhold som ikke er i tråd med IKT-instruks eller som er i strid med norsk lov. For å ivareta informasjonssikkerheten kan Politihøgskolen også foreta sletting av slike filer uten varsel, eksempelvis ved funn av skadevare.

5.1.1 Logging

All aktivitet på Politihøgskolens og andres IKT-ressurser kan spores tilbake til den enkelte bruker og enhet som benyttes. Alle Politihøgskolens IKT-ressurser kan overvåkes og all autorisert og (forsøk på) uautorisert bruk kan registreres i logger. Dette for å ivareta Politihøgskolens krav til informasjonssikkerhet (konfidensialitet, integritet og tilgjengelighet) samt avdekke brudd på denne.

5.1.2 Overvåkning av bruk av IKT-ressurser

Hvis bruken av IKT-ressurser, på grunn av driftssikkerhet eller av andre hensyn må overvåkes av driftspersonalet, skal dette opplyses om; hva er formålet, hvilke opplysninger vi logger, hvor lenge oppbevarer vi loggene og hvem har tilgang til loggene.

5.1.3 Taushetsplikt for Helpdesk IKT

Helpdesk IKT og driftspersonalet 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.

6 Brudd på skolens IKT-instruks

Ved brudd på, eller mistanke om brudd på høgskolens IKT-instruks, kan Helpdesk IKT inndra/utestenge brukerrettigheter til IKT-systemer. For øvrig gjelder også lov om statens ansatte, jfr. § 20 nr. 1, bokstav d, og §§ 25 og 26, samt Forskrift om skikkethetsvurdering, utvisning, bortvisning og utestenging av studenter ved Politihøgskolen, jfr. §§ 4 til 7.

Rektor ved Politihøgskolen eller den myndighet som har rekvirert brukerkontoen, kan inndra brukerrettighetene permanent.

6.1 Spesielt for eksterne brukere/innleide

For eksterne brukere (ikke studenter/ansatte), vil brudd på disse reglene kunne medføre at oppdraget faller bort, uten noen form for erstatning, samt at Politihøgskolen forbeholder seg retten til å kreve erstatning for tap/skade.

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 Dødsfall

Ved dødsfall slettes personlig epostkasse og filområde. Før sletting finner sted, kan innsyn foretas jfr. 4.6 Innsyn i brukers personlige e-postboks/filområde av arbeidsgiver. Automatisk videresending av epost til nærmeste leder eller automatisk svar til avsender, aktiveres ikke.

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

7.3 Utlevering av personlig epostkasse/hjemmeområde

Ved skriftlig henvendelse fra Politi eller påtalemyndighet (beslag og utleveringspålegg eller pålegg iht Politilovens § 5) vil Politihøgskolen utlevere innhold av en navngitt brukers personlige e-postboks/filområder.

7.4 Sikre virksomhetsrelatert kommunikasjon

Helpdesk IKT forbeholder seg retten til å slå av (trådløse) nett og annen kommunikasjon, når forholdene krever det, for å sikre at virksomhetsrelaterte aktiviteter kan gjennomføres.

Oslo, 21.08.2019



Nina Skarpenes

rektor