



**Høgskolen  
i Lillehammer**  
Lillehammer University College • hiil.no

**Arkivplan  
for  
Høgskolen i Lillehammer  
mai 2011**

## **Innholdsfortegnelse:**

<b>1</b>	<b>Bakgrunn for arkivplanen</b>	<b>side 3</b>
<b>2</b>	<b>Egen organisasjon</b>	<b>side 5</b>
	<b>Arkivorganisering</b>	<b>side 6</b>
	<b>Ansvarsområder – post- og dokumentbehandling</b>	<b>side 8</b>
	<b>Opplæring</b>	<b>side 10</b>
<b>3</b>	<b>Lover og bestemmelser</b>	<b>side 12</b>
<b>4</b>	<b>Sikkerhet</b>	<b>side 13</b>
<b>5</b>	<b>Organisering av arkivmaterialet</b>	<b>side 15</b>
	<b>Periodisering</b>	<b>side 15</b>
	<b>Tilgangskoder</b>	<b>side 18</b>
	<b>Framfinningssystemer</b>	<b>side 20</b>
	<b>Avlevert arkiv</b>	<b>side 22</b>
<b>6</b>	<b>Bestandsoversikt</b>	<b>side 23</b>
<b>7</b>	<b>Vedlegg:</b>	
	<b>1) Policy for informasjonssikkerhet av 2009</b>	<b>side 26</b>
	<b>2) Revidert utfylt skjema for dokumentbasert tilsyn av elektronisk arkivdanning i UH-sektoren</b>	<b>side 44</b>
	<b>3) Sentrale arkivtermer for høgskolens bruk</b>	<b>side 49</b>
	<b>4) Grunnkurs for saksbehandlere i ePhorte</b>	<b>side 61</b>

## 1. Bakgrunn for arkivplanen

Alle offentlige organ er pålagt å ha en arkivplan, jf. § 2-2 i Forskrift om offentlige arkiver av 11. desember 1998:

***”Eit offentlig organ skal til kvar tid ha ein ajourført samleplan, ein arkivplan, som viser kva arkivet omfattar og korleis det er organisert. Arkivplanen skal også vise kva slags instruksar, reglar, planar m.v. som gjeld for arkivarbeidet.”***

Statlig, fylkeskommunal eller kommunal institusjon blir regnet som et offentlig organ, jf. forskriftens § 1-1:

***”Offentlege organ pliktar å halde arkiv i samsvar med føresegnene i forskrifta her. Som offentlig organ blir rekna statleg, fylkeskommunal eller kommunal institusjon eller eining, jf. arkivlova § 2, bokstav g.”***

### Formål med arkivplanen

Arkivplanen gir bindende retningslinjer for all behandling av informasjon og dokumentasjon i høgskolen.

Arkivloven med forskrifter ligger til grunn for rutine/retningslinjene. Arkivplanen skal bidra til at Høgskolen i Lillehammer ivaretar arkivansvaret sitt etter Arkivlovens § 6 der det heter *”Offentlege organ pliktar å ha arkiv, og desse skal vere ordna og innretta slik at dokumenta er tryggja som informasjonsskjelder for samtid og ettertid”*.

Arkivplanen skal

- være et verktøy for å kvalitetssikre behandlingen av høgskolens arkivmateriale
- styre produksjon, lagring og bevaring av dokumentasjon i høgskolen
- holde oversikt over høgskolens dokumenter (def.: ”ei logisk avgrensa informasjonsmengd som er lagra på eit medium for seinare lesing, lyding, framsyning eller overføring,” jfr. Arkivlovens §2 a)
- være intern oppslagsbok ved behov for kunnskap om arkivforhold
- bidra til å etablere en felles arkivpolitikk for hele høgskolen
- fungere som dokumentasjon når eksterne myndigheter ber om opplysninger om arkivforholdene

En mer omfattende forståelse av begrepet er å betrakte arkivplanen som en samling dokumenter som gir oversikt over rutiner, arkivserier, elektroniske systemer, organisasjonsforhold, arkivnøkler og andre gjenfinningsmidler og all annen arkivrelatert kunnskap i høgskolen, knyttet både til dagens situasjon og til fortiden - altså både det som skapes og brukes i dag, og det som har vært skapt og brukt tidligere.

Arkivplanens hovedmål er å styre produksjon, lagring og bevaring av dokumentasjon (arkivdokumenter) i høgskolen. I tillegg til å være intern dokumentasjon, skal den også fungere som dokumentasjon når eksterne myndigheter og overordnede myndigheter ber om opplysninger om arkivforholdene.

HiL har en felles arkivpolitikk for hele høgskolen, slik at tilsatte til enhver tid skal vite hvordan oppgavene knyttet til dokumentbehandlingen skal løses, og hvilke retningslinjer som gjelder. Dette skal sikre en rask og korrekt saksbehandling og en effektiv service.

Arkivplanen skal altså ikke bare fungere som oversikt, den skal også være organets interne oppslagsbok. Her skal ledere, saksbehandlere og ikke minst arkivpersonalet kunne slå opp når de har behov for kunnskap om arkivforhold

### **Denne arkivplanen skal erstatte:**

Arkivplanen for HiL - som gjaldt for perioden 1994 - 2010 – og som tidligere var lagt på høgskolens nettsider. Før planen ble fjernet fra nettsidene, ble det tatt utskrift. Papirutskriftene ligger pr. dato på arkivleders kontor og er arkivert i ePhorte.

### **Oppdatering av arkivplanen**

Iflg. arkivforskriften § 2-2 skal arkivplanen hos et offentlig organ til enhver tid være ajourført. Det er derfor behov for jevnlig oppdatering. Slik oppdatering vil som regel gjelde enkeltopplysninger eller enkeltdokumenter som inngår i planen.

Ansvar: Arkivleder.

**Full gjennomgang** av arkivplanen bør skje minst hvert 4. år og ved endringer som

- omfattende omorganisering av høgskolen
- vesentlige endringer i høgskolens oppgaver og myndighet

Ansvar: Arkivleder.

Arkivleder avgjør om det er behov for oppdatering av arkivplanen når

- det blir tatt i bruk ny versjon av arkivnøkkel
- det blir tatt i bruk nye versjoner av datasystem for lagring av informasjon

**Arkivansvarlig skal ha melding om alle endringer med mulige følger for arkivet i god tid før de blir satt i verk, og har rett til å uttale seg om følgene de kan få for arkivet.**

### **Arkivbegreper**

Riksarkivet har utarbeidet en nettside med **sentrale arkivbegreper og –termer**. Den finnes på:<http://www.arkivverket.no/arkivverket/Offentlig-forvaltning/Regelverk/Arkivbegreper>.

De mest sentrale arkivtermer for høgskolens bruk følger som vedlegg 3.

## **2. Egen organisasjon**

### **Virksomhetens hovedmål**

Sitat fra Strategisk plan 2008-2011:

”Høgskolen i Lillehammer skal utvikles som attraktiv og profilert universitetscampus med et bredt faglig tilbud, kjent for studie- og forskningskvalitet.

”Høgskolen skal være en lærende organisasjon og en attraktiv arbeidsplass som ivaretar likestilling og antidiskriminering.”

Høgskolen har 5 sentrale målområder:

1. Universitetsbygging
2. Utdanning
3. Forskning, faglig og kunstnerisk utviklingsarbeid
4. Samhandling med samfunns- og næringsliv
5. Organisasjonsutvikling.

### **Kort historikk**

Høgskolen i Lillehammer har bestått siden 01.08.1994 da Oppland distriktshøgskole opphørte som regional høgskole. Den ble ikke sammenslått med noen annen høgskole, men fikk annet navn og ble en av 26 statlige høgskoler med navnet Høgskolen i Lillehammer, beliggende på Storhove.

HiL bestod den gang av 3 avdelinger, Senter for livslang læring (SELL) og en fellesadministrasjon, med felles beliggenhet på Storhove i ombygd Radio- og TV-senter fra OL94.

### **Navn på avdelingene/driftsenhetene før 2004:**

- Avdeling for helse- og sosialfag (AHS)
- Avdeling for kultur- medie- og samfunnsfag (AKMS)
- Avdeling for reiseliv og samfunnsutvikling (ARS)
- Den norske filmskolen (grunnenhet under høgskolestyret) (DNF) (opprettet 1997)
- Senter for livslang læring (SELL)

Avdelingene/driftsenhetene har hatt et felles sentralt arkiv i fellesadministrasjonen.

Fra 01.01.04 hadde HiL 4 avdelinger:

- Avdeling for helse- og sosialfag (AHS)
- Avdeling for samfunnsvitenskap (ASV) (ARS og AKMS sammenslått fra 01.01.02.)
- Avdeling for TV-utdanning og filmvitenskap (TVF)
- Den norske filmskolen (DNF)

I 2007 ble Avd. for samfunnsvitenskap delt i to nye avdelinger:

- Avdeling for økonomi- og organisasjonsvitenskap (ØKORG) og
- Avdeling for humaniora- idrett,- og samfunnsvitenskap (HIS)

Avdelingene reorganiseres fra høsten 2011.

Fellesadministrasjonen (FADM) har vært delt i følgende seksjoner:

- Ledelse og stab
- Økonomi og drift
- Personal (fradelte fra øk. og drift fra årsskiftet 2008/09)
- Studieadministrasjonen
- IT-seksjonen
- Biblioteket

Disse seksjonene består også i 2011.

## Arkivorganisering

I forskrift om offentlige arkiv av 1998 §2-1 heter det:

”Arkivarbeidet i eit offentleg organ skal som hovudregel utførast av ei eiga eining, ei arkivteneste, under dagleg leing av ein arkivansvarleg. Arkivtenesta skal vere felles for organet. Dersom ikkje særlege omsyn tilseier noko anna, skal ho vere underlagd den administrasjonseininga som har ansvaret for organets fellessaker.”

### Arkivansvar HiL

Arkivansvaret skal ligge hos institusjonens øverste ledelse, jf. Forskrift om arkiv § 1-1. Ved Høgskolen i Lillehammer har Høgskoledirektøren hovedansvaret for arkivtjenesten.

**Arkivleder** er faglig ansvarlig for sentral arkivfunksjon, som er felles for hele høgskolen. Arkivleder skal sørge for at arkivarbeidet utføres etter gjeldende regelverk gjennom å gi instruks, råd og faglig veiledning i det lokale arkivarbeidet, jf. Forskrift om arkiv § 2-1. Arkivleder er ansatt ved ledelsens stab, og har ansvar for daglig drift av sentral arkivfunksjon for HiL. Arkivleder rapporterer til høgskoledirektøren, og har personalansvar for arkivmedarbeider(e).

**Arkivmedarbeider(ne)** har ansvar for at det praktiske arkivarbeidet utføres i samsvar med gjeldende regelverk, og skal arbeide iht. rutiner nedfelt i arkivplanen.

På hver avdeling/seksjon skal det i utgangspunktet være en eller flere **superbrukere** for høgskolens elektroniske arkiv- og saksbehandlingssystem ePhorte. **Ledere** på fagavdelingene er nærmeste overordnede for superbrukerne på avdelingene, og har ansvar for at forholdene legges til rette slik at avdelingene har en best mulig brukerstøtte på ePhorte. På hver administrativ enhet er det ansvarlig **saksfordeler** som har ansvar for umiddelbart å fordele all elektronisk post som kommer ufordelt til enheten.

**Saksbehandlerne** plikter å følge de retningslinjer som gjelder for høgskolen i all dokumentbehandling, arkivdanning og bruk av arkivet.

Saksbehandlerne har et spesielt ansvar når det gjelder å få framskaffe all arkivverdig dokumentasjon som skal legges i ePhorte.

Saksansvaret for den enkelte **elektroniske personalmappe** er lagt til den leder som har personalansvaret for vedkommende. Personale ved HiL som var tilsatt før innføringen av ePhorte, har både en fysisk og en elektronisk personalmappe. Personale ved HiL som er tilsatt etter januar 2006 har kun elektronisk personalmappe.

Personalseksjonen oppbevarer fysiske personalmapper (for perioden 1994 – 2006) til tilsatte for hele høgskolen.

Mappene for nevnte periode oppbevares av høgskolens personalseksjon fram til de skal avleveres til Statsarkivet på Hamar.

HiL har ikke elektroniske studentmapper i ePhorte.

Ansvar for å framskaffe og tilrettelegge **elektronisk studentdata** er lagt til FS-ansvarlige ved HiL som også har ansvar for å oppbevare og tilrettelegge **elektronisk studentdata for avlevering**.

Ledelsen av det daglige arkivarbeidet som er sentralisert, har en rådgiver som arkivleder, og stillingen utgjør 50% av hel stilling.

I tillegg er det en hel stilling som førstekonsulent som har den daglige journalføring og andre oppgaver knyttet til arkivtjenesten. Fram til 2006 var denne stillingen delt på to personer som i tillegg hadde sentralbordtjenesten ved høgskolen.

### **Arbeidsområde for arkivleder**

Arkivlederen skal administrere arkivarbeidet ved høgskolen slik at oppgavene blir utført så effektivt og økonomisk som mulig.

Arkivlederen har ansvaret for at utføring av arkivarbeidet skjer i overensstemmelse med gitte regler og instruksjoner, jf. Arkivloven med forskrifter.

Arkivleder plikter å holde seg orientert om den arkivfaglige utvikling.

Arkivleder skal:

- Bistå med utvelgelse og introduksjon når det ansettes arkivpersonale
- Sørge for at nyansatte får nødvendig opplæring og instruksjon
- Sørge for effektiv arbeidsfordeling og disponering av arkivpersonalet
- Holde arkivpersonalet orientert om alle forhold som kan være av betydning for arkivarbeidet

## Ansvarsområder i ePhorte – Post- og dokumentbehandling

Ved HiL er følgende roller tildelt i ePhorte: Stillingsbetegnelse/

### funksjon

Høgskoledirektør	LD (Leder / saksfordeler)	
Avdelingsdirektører	LD / saksfordeler	
Rektor	LD	
Prorektor	LD	
Dekaner	LD	
Kontorsjefer	LD / saksfordeler	
Hovedbibliotekar	LD / saksfordeler	
IT-sjef	LD / saksfordeler	
Saksbehandlere	SB (Saksbehandler)	
Utvalgssekretærer	Arkiv/utvalg	
Arkivleder	SY + LD + AR1 + SB	Arkivleder og 1 arkivar har rollen SY (systemansvarlig)
Arkivarer	AR1 + SB	
Superbrukere	AR2 + SB	
	AR1 + SB i kursbasen	

Det er systemansvarlig (som regel arkivleder) som legger inn nye brukere hvor roller tildeles i henhold til skjema over. Registrering av nye brukere og tildeling av roller må være klarert av leder ved enheten.

Arkivleder har ansvar for å administrere og ajourføre brukerrettigheter til systemet. HiL er en oversiktlig virksomhet, og hvor alle brukere av ePhorte er kjente av arkivet som har jevnlig kontakt og oppfølging i bruken av ePhorte.

## Leders ansvar i.f.m. fordeling av dagens post

Leder for enheten har det endelige ansvaret for at dagens post er korrekt fordelt.

Leder bør kontrollere at:

- **dokumentet har blitt fordelt til rett enhet** Er det påført feil administrativ enhet? Leder endrer administrativ enhet til "Ufordelt" samt skriver forklaring vedr. omfordelingen i merknadsfeltet. Dokumentet vil da automatisk bli oversendt arkivet for fordeling til ny enhet.
- **rett saksbehandler har blitt påført** Er det påført feil saksbehandler, men riktig administrativ enhet.
- **kontroll av unntak fra offentlighet er vurdert** Er dette et dokument alle brukere ved HiL av ePhorte kan ha innsyn i? Er det hjemmel for unntak fra offentlighet? Kan også påføres/endres av leder.
- **forslag til tilgangskode og skjerming er riktig** Er påført forslag om kode og eventuelt ytterligere skjerming riktig? Kan også påføres/endres av leder.

Leder kan foreta følgende "ledersøk" i.f.m. fordeling av dagens post:

**Inngående brev - fordel til saksbehandler**

**Mottatte notater - påfør saksbehandler**

**Kopi av utgående brev - påfør saksbehandler** Søkene over viser saksdokumenter som tilhører egen administrativ enhet, og som ikke er fordelt til saksbehandler, d.v.s. står Ufordelt på enheten.

**Mottatt for godkjenning (fellessøk)**

Viser journalposter som er sendt leder for godkjenning.

Leder kan foreta andre aktuelle søk for å få en god oversikt over hva som mottas, produseres og ekspederes på egen enhet:

**Post til min enhet (ledersøk)**

Viser inngående dokumenter, N-notat, X-notat og kopi av utgående brev mottatt på egen administrativ enhet siste 7 dager.

**Post fra min enhet (ledersøk)**

Viser utgående dokumenter, N-notat og X-notat sendt fra egen enhet og innen egen enhet siste 7 dager.

**Min enhets restanser (ledersøk)**

Viser alle restanser knyttet til enhetens saksbehandlere. Bør følges opp av avdelingens ledere.

## **Saksbehandlers ansvar i.f.m. fordeling av dagens post**

Saksbehandler har ansvar for å **kontrollere**:

- **at han/hun er rette saksbehandler/saksansvarlig for saken/dokumentet** Er dokumentet fordelt til feil saksbehandler? Mottaker gir leder/saksfordeler eller arkiv beskjed. Leder/saksfordeler eller arkiv endrer og fordeler på nytt. Saksbehandler kan ikke påføre annen saksbehandler uten å gå om sin leder
- **at dokumentet/JP er registrert i riktig sak** Er dokumentet/JP registrert i feil sak? Kontakt arkivet
- **sakstittel og JP-tittel** Er saks- eller JP-tittel feil eller mangelfull, må arkivet kontaktes dersom status på sak er B og status på JP er J
- **at hele det innskannede dokumentet med eventuelle vedlegg er lesbart** Hvis ikke dokumentet er lesbart, kontakt arkivet. Papirkopien blir bevart i ca. 2 måneder, og kan skannes inn på nytt.

Når ovennevnte kontroller er foretatt:

**Saksbehandler har alltid ansvar for å kontrollere at nødvendige kopimottakere er påført/evt. påføres.**

Under Fellessøk har saksbehandler oversikt over sine restanser, forfallslistene, dokumenter som ikke er ekspedert, dokumenter under arbeid, sendt til godkjenning, dokumenter med status F (f.eks. som er godkjente av leder) m.v.

## **Arkivpersonalet**

Daglig oppfølging og kvalitetssikring medfører bl.a. :

- journalføring og kvalitetssikring av alle innskannede dokumenter og dokumenter mottatt pr. e-post til høgskolens postmottak**
- journalføring og kvalitetssikring av alle saker og JPer opprettet av saksbehandlerne. Dette gjøres dagen etter at saksbehandlerne setter JPene til ferdig. Dokumentene konverteres da automatisk til arkivformat pdf.**
- søke opp og fordele JP'er og saker sendt tilbake til arkiv**
- søke opp, kontrollere og avslutte saker som er ferdige fra saksbehandler**
- kvalitetssikring av offentlig journal**
- oppfølging av restanser**
- oppfølging av dokumenter under arbeid**

I venstremenyen i ePhorte under Arkivsøk er det opprettet egne søk for arkivpersonalet.

## **Saksbehandlere/ledere**

Saksbehandlere skal **daglig** søke fram:

- "Mine restanser" (mottatt JP som skal avskrives).
- "Min forfallsliste" (mottatt JP som er påført frist for å besvare).
- "Mottatt for godkjenning" (mottatt JP som saksbehandler skal godkjenne).
- "Sendt til godkjenning" (JP sendt til godkjenning, men som ennå ikke er behandlet).

I tillegg kan saksbehandlere/ledere bruke ulike søk for oversikt/kontroll på egne saker/JPer. Eksempler:

- "Post til orientering" (JP'er som ikke må besvares - siste 30 dager).
- "Mine JP'er under arbeid" (egenproduserte dokumenter som ikke er ferdigstilt).
- "Mine besvarte JPer" (besvarte JP'er siste 30 dager).
- "Mine JP'er med status F (JP'er som er ferdigstilt eller godkjent, men ikke ekspedert).

I tillegg kan leder bruke følgende søk for oversikt/kontroll på egen enhet.

Eksempler:

- "Post til min enhet" Ledersøk
- "Post fra min enhet" Ledersøk
- "Min enhets restanser" Ledersøk

## **Rutiner for e-post sendte direkte til saksbehandler**

Det har gjennom alle år med e-post vært presisert og gjentatt ved opplæring at det er saksbehandlers ansvar å legge inn mottatte e-poster som er ledd i saksbehandling i ePhorte, på samme måte som utgående e-poster via ePhorte. Dette fungerer tilfredsstillende.

HiL har Lotus Notes mail-system hvor innboksen manuelt må settes opp i ePhorte. Dette følges opp av arkivpersonalet, og e-post-behandling berøres også når opplæring/kurs gis.

## **Opplæring**

### **Arkivmedarbeidere**

#### **Ekstern opplæring**

Faglig kompetanse på arkiv kan oppnås via kurs gjennom Statskonsult eller Norsk Arkivråd. Høyere utdanning i faget kan oppnås ved Universitetet i Oslo, ved Arkivakademiet (som er et samarbeid mellom Norsk Arkivråd og Riksarkivet) eller Høgskolen i Oslo og Høgskolen i Lillehammer.

Den enkelte arkivmedarbeider er selv ansvarlig for å søke om opptak på ovennevnte utdanninger og kurs.

**Nytilsatte arkivmedarbeidere** må gjennomføre grunnleggende kurs i arkivfaget og innføringskurs i bruk av arkivsystemet ePhorte, dersom de ikke har gjennomgått slike kurs tidligere. Videre plikter nytilsatte arkivmedarbeidere å sette seg inn i høgskolens gjeldende arkivplan.

Grunnleggende kurs i arkivfag tilbys både av Statskonsult og av Norsk Arkivråd.

Innføringskurs i bruk av ePhorte holdes internt ved høgskolen.

Jf. vedlegg: Grunnkurs i ePhorte ved HiL.

#### **Intern opplæring**

Det er arkivleders ansvar at arkivaren(e) ved høgskolen er oppdatert til enhver tid.

Den mest effektive måten dette kan praktiseres på er:

- arkivleder innkaller til felles møter ved behov  
arkivfaglig tema tas opp som eget punkt på hvert møte
- arkivplanen skal kunne benyttes som et arbeidsredskap, slik at alle tilsatte til enhver tid vet hvordan oppgavene knyttet til dokumentbehandlingen skal løses og hvilke retningslinjer som gjelder
- arkivleder videreformidler all aktuell informasjon

## **Saksbehandlere**

### **Intern opplæring**

For at saksbehandlingen skal utføres effektivt, er det viktig at saksbehandlerne har god kunnskap til den arkivmessige del av saksgangen. Saksbehandlerne skal også kjenne til og arbeide etter de lover og regler som gjelder for arkivarbeidet ved høgsolen.

**Nytilsatt saksbehandler** skal en av de første arbeidsfagene ha kontakt med arkivet.

Arkivet skal da sørge for:

- nødvendig tilgang til ePhorte
- -nødvendig opplæring i ePhorte, herunder dele ut kursmateriell, informere om rutinebeskrivelser i ePhorte og om Arkivplan for HiL i ePhorte
- Arkivet skal videre sørge for at nytilsatte saksbehandlere får oppfølging etter behov.
- Arkivet skal i tillegg sørge for at samtlige saksbehandlere får nødvendig veiledning, oppfølging og eventuell kursing i.f.m. den arkivmessige delen av saksbehandlingen.
- Arkivet holder halvårlige interne kortkurs i generell saksbehandling, søking, import av e-post samt tilgangskoding/sladding for å skolere høgsolenes saksbehandlere i ePhorte-bruk.

**Ledere** får samme opplæringstilbud som saksbehandlere. I tillegg er det fokus på det spesielle lederansvaret i ePhorte som de har å følge opp, for å sikre korrekt saksbehandling og dokumentasjon i sin avdeling/seksjon.

### 3. Lover og bestemmelser

**Arkivarbeidet er regulert gjennom lover med forskrifter og internt regelverk.**

Følgende lover er de mest sentrale for arkiv:

**Arkivloven** av 1998 med forskrift § 2-2 som pålegger Høgskolen i Lillehammer som offentlig virksomhet, å ha en oppdatert arkivplan.

Høgskolen må også forholde seg til og etterleve **Offentleglova** med forskrifter som trådte i kraft 01.01.2009. Denne gir rettigheter til den som ønsker innsyn, og det er reduserte muligheter til å unnta dokumenter for innsyn i forhold til den offentlighetslov som gjaldt før 2009. Alle organinterne dokumenter kan heller ikke lenger unntas som intern saksforberedelse. Dette gjelder dokument eller del av dokument som inneholder den endelige avgjørelsen til organet i en sak. Likeså gjelder det generelle retningslinjer for saksbehandlingen til organet. Heller ikke dokumenter mellom administrasjon og avdelinger og mellom høgskolens avdelinger kan unntas.

HiL må følge **Forvaltningsloven** av 1967 som regulerer behandlingsmåten i forvaltningssaker. Statlige høgskoler har viktige saker å forvalte innenfor dette regelverket.

**Personopplysningsloven** fra 2000 gir direktiver for behandling av personopplysninger og hjemler ivaretagelse av de rettmessige krav til behandling/skjerming av personers identitetsopplysninger.

**Forskrift om informasjonssikkerhet** av 2001

Annet sentralt regelverk :

**Arkivnøkkel og kassasjonsplan** for statlige høgskoler sist revidert juli 2005.

Vedtak om **bevaring og kassasjon av eksamensbesvarelser** i høgskolesektoren.

**Retningslinjer for generell bevaring og kassasjon i NOARK-baserte løsninger.**

Rundskriv om arkivloven fra regjeringen til statlige organer.

Rundskriv om pdf- A av 22.01.2009.

Yrkesetiske retningslinjer for arkivarer.

Riksarkivarens øvrige rapporter og retningslinjer for arkivarbeidet.

Interne retningslinjer og rutiner ligger i ePhorte og på HiLs intranett-sider samt utdelt på papir til saksbehandlerne ved oppstart og kursing i ePhorte-bruk. Disse retningslinjer og rutiner har til hensikt å sikre at arkivarbeidet /saksbehandlingen i ePhorte blir utført etter gjeldende lover og regelverk. Rutinene gjennomgås årlig i forbindelse med årlig oppdatering av arkivplanen og kan også endres ved organisatoriske og andre større endringer som måtte komme ved høgskolen.

## **4. Sikkerhet**

Rutiner for fysisk sikring, datasikkerhet og dokument sikring

### **Arkivlokaler**

Arkivforskriften §4-1 hjemler definisjonen av arkivlokale – der hvor arkivmaterialet har sitt faste tilholdssted.

HiL har et ferdig ordnet arkiv for perioden 1994 – 2005 som var siste periode med papirarkiv, men med elektronisk journalføring i Modulink. Dette arkivet er oppbevart i fjernarkivet i 2. etasje Nordhove.

Journalen er lagt inn i ePhorte som historisk base og er likeså deponert hos Riksarkivet.

### **Adgang**

Fjernarkivet er kun beregnet på arkivmateriale og lagrede økonomisaker med tilgangskort for døråpning. Det er godkjente arkivreoler hvor papirarkivet står klart for avlevering med avleveringslister i hver kassett. Det som skal kassereres er frasortert.

I fjernarkivet står også høgskolestyresaker i ringpermer fra 1994 da høgskolen fikk sitt første styre.

Fra 2006 da HiL startet med ePhorte, er styresaker og protokoller lagt inn i utvalgsmodule i ePhorte.

Personalmapper i papir over ansatte fra før 2006 oppbevares i brannsikre safe ved personalseksjonen.

For øvrig følges Arkivforskriftens §4.5 1. ledd med tilsyn etc. av arkivlokalene.

### **Data- og Informasjonssikkerhet**

Arkivloven §1 pålegger høgskolen å ta vare på og gjøre tilgjengelig for ettertiden arkivmateriale som har kulturelt eller forskningsmessig verdi eller som inneholder rettslig eller viktig forvaltningsmessig dokumentasjon.

Det skal sørges for dokument sikkerhet, konfidensialitet, integritet og tilgjengelighet.

Tilgjengelighet handler om at informasjon er tilgjengelig innenfor de krav som er satt. Her er arkivbestandighet, krav som settes til medium slik at skrift, lyd bilde eller elektronisk materiale ikke brytes ned eller blir ødelagt over tid, vesentlig. For papirarkiver er bestemmelser om arkivesker og internasjonale standarder for bl.a permanent papir (ISO 9706) viktige. For elektroniske arkiver er også standarder (NOARK), formater og sikkerhetskopiering vesentlig.

HiL har formelt utpekt økonomi- og driftsdirektør som IT-sikkerhetsansvarlig.

Vedkommende styrer på vegne av høgskoledirektør den operative IT-sikkerheten.

Høgskolen har en vedtatt Policy og retningslinjer for informasjonssikkerhet som er klarert av Uninett og godkjent av Høgskolestyret i 2009 (vedlagt). Denne regulerer ansvar og oppgaver for intern data og informasjonssikkerhet ved høgskolen.

Det elektroniske arkivsystemet ePhorte kjøres mot servere ved universitet i Oslo, USIT, og det er UNINETT som koordinerer driften. HiL tar jevnlig back-up av nødvendige data på lokale servere. Uninett sørger for sikkerhetskopiering av HiLs arkivbase og sikkerhet i forhold til tilgang til servere, back-up og lignende.

HiL har også en overordnet beredskapsplan ved kriser og ulykker:[http://www.hil.no/hil/om\\_hoegskolen/sentrale\\_dokumenter](http://www.hil.no/hil/om_hoegskolen/sentrale_dokumenter)

Dersom systemet skulle være ute av drift i lengre perioder, så vil arkivet i samarbeid med beredskapsgruppa ved HiL ha ansvar for å finne løsninger som vil ivareta arkivdanningen på en forsvarlig måte.

Høgskolen har fylt ut skjema for dokumentbasert tilsyn av elektronisk arkivdanning i revidert utgave av mars 2011 (Vedlegg 3).

### **Taushetsplikt**

Taushetsplikt reguleres av flere lover. De mest sentrale for HiL er Lov om universiteter og høgskoler §41 og Forvaltningsloven §13.

Alle ansatte må skrive under en taushetserklæring ved tilsetting som en del av arbeidsavtalen.

Personopplysningsloven §2 nr. 4 definerer ”behandlingsansvarlig” i en virksomhet, sitat:

”Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes.” Høgskoledirektør er ansvarlig ved høgskolen for behandlingen av personopplysninger.

Ansatte som bruker ePhorte på sine PCer, skal enten logge av eller låse sine datamaskiner når de er ute av kontoret slik at uvedkommende ikke får tilgang til dokumenter i ePhorte eller selve programmet.

## 5. Organisering av arkivmaterialet

### Arkivbegrensning / bevaring / kassasjon

#### Arkivbegrensning

Med arkivbegrensning er ment at dokumenter som faller inn under definisjonen av arkiv i § 2 i arkivloven (*Dokumenter som blir til som ledd i en virksomhet*), men som verken er gjenstand for saksbehandling eller har verdi som dokumentasjon, blir holdt utenfor arkivet, for eksempel i bibliotek, rundskrivmapper, egne kurspermer eller lignende, eller slettes eller kastes, jf arkivforskriften § 3-19:

*Arkivavgrensning bør gjennomførast i samband med postbehandling eller arkivlegging.*

*Dersom dette ikkje er skjedd, skal det gjerast ved bortsetjing eller seinast ved avlevering til arkivdepot. Materiale som blir skilt ut ved arkivavgrensning, kan oppbevarast separat utanfor arkivet, slettast eller kastast*

*Trykksaker, rundskriv, anna mangfalda og allment tilgjengeleg materiale og blankettar som ikkje er utfylte. Frå dette er det følgjande unntak:*

*det organet som har utfërda slikt materiale, skal arkivere eitt eksemplar og dei nødvendige forarbeida, dokument som fører til saksbehandling, eller som er nødvendige vedlegg til ei sak, skal arkiverast.*

*Konsept, utkast, kladdar og kladdenotat, ekstra kopiar, interne meldingar o.l. som ikkje har verdi for saksbehandling eller dokumentasjon.*

*Frå dette er det følgjande unntak:*

*konsept som har noteringar og påteikningar som er nødvendige for å forstå saka og den samanhengen ho står i, skal arkiverast,*

*kopi av utgåande dokument skal arkiverast, andre kopiar m.v. som er nødvendige vedlegg til ei sak, skal arkiverast.*

*Tekstbehandlingsfiler o.l., bortsett frå det som eventuelt inngår i elektronisk sakarkiv, jf. § 2-13.*

*Sakspapir som medlemene av offentlege utval mottek, med mindre dokumenta må reknast som saksdokument for det organet medlemen representerer.*

*Anna materiale som verken er gjenstand for saksbehandling eller har verdi som dokumentasjon.*

### Periodisering / deponering / avlevering

#### Periodisering

Ifølge arkivforskriften § 3-12 skal saksarkivet og tilhørende journal deles inn i perioder. Det skal være samsvar mellom periodeinndeling i journal og i saksarkiv, men en periode i elektronisk journal kan omfatte flere perioder i saksarkivet. En arkivperiode bør være på minst 5 år, og følge kalenderåret.

Høgskolen i Lillehammer ble opprettet 1. august 1994, og høgskolens arkivmateriale består av en avsluttet periode 1.8.1994 – 1.1.2006. Denne perioden inneholder elektronisk journal (Modulink) og papirbaserte dokumenter.

Inneværende periode, som startet 01.01.2006, har fullelektronisk arkiv, og benytter systemet ePhorte. Ny periode i saksarkivet bør starte i 2012.

Periodisering kan skje på ulike måter, jf arkivforskriften § 3-13: **Skarpt periodeskille eller overlappingsperiode.**

### **Skarpt periodeskille**

innebærer i prinsippet at saker fra en avsluttet periode settes bort til bortsetningsarkiv ved periodeskillet. Skarpt periodeskille bør brukes i.f.m. overgang til nytt arkivsystem, innføring av ny arkivnøkkel og ved større organisasjonsendringer.

Da høgskolen gikk over til et nytt system i januar 2006, ble det satt et skarpt periodeskille

Dette ble gjennomført på følgende måte:

Alle saker og dokumenter som var registrert i avsluttet periode ble satt bort i sin helhet, også saker som var aktive pr. januar 2006. Dette førte imidlertid til at saker som var aktive ved periodeskillet ble splittet, og dokumentene i saken befant seg i både aktivt og i bortsatt arkiv. Dette krevde at det ble utarbeidet gode henvisninger, ved lenking i journalene og henvisningskort i de fysiske mappene.

Arkivmaterialet fra den avsluttede perioden oppbevares i fjernarkiv, og er ordnet og pakket for klargjøring til avlevering i 2031. Det er viktig å få ordnet arkivet snarest mulig etter periodeskille, slik at materialet ikke skal gå tapt, og mens personalet som arbeidet med dette arkivet, fremdeles er i organisasjonen.

Dersom det etter periodeskillet kommer inn dokumenter som hadde tilknytning til saker i bortsetningsarkivet, ble det startet ny sak, med de nye dokumentene som de første i saken. De eldre dokumentene kan **lånes ut** fra bortsetningsarkivet, og **settes tilbake** etter behandling.

### **Overlappingsperiode**

Dersom journalen er elektronisk, kan ved normal overgang mellom arkivperioder bruke overlappingsperiode i stedet for skarpt skille, slik det er redegjort for i Noark-standarden, jf. arkivforskriften § 13.

Dette innebærer i prinsippet at aktive saker overføres **etter** periodeskillet. I NOARK-standarden anbefales det å bruke to år av den nye perioden for å avklare hvorvidt saker er aktive eller avsluttet. Saker fra avsluttet periode som i løpet av denne overlappingsperioden får tilført nye dokumenter, defineres som aktive saker og overføres til ny arkivperiode.

### **Deponering**

Ifølge kapittel VIII, § 8-2, bokstav b i Forskrift om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver er definisjonen av deponering slik: *Deponering (depositum)*: en fysisk overføring av arkivmateriale uten at råderetten over det overføres.

§ 8-4 sier dette om ansvarsforhold: Når kopi av elektronisk arkivmateriale deponeres i Arkivverket, jf. arkivforskriften § 3-17 og § 5-2, beholder avgiver råderetten og det fulle ansvaret for materialet. Avgiver skal betjene og vedlikeholde materialet inntil avlevering senere har funnet sted. Arkivverket skal bevare den deponerte kopien utilgjengelig for bruk, og bare utføre teknisk vedlikehold.

Med mindre avgiver eller Arkivverket har meldt behov for en ny vurdering, skifter en deponering automatisk status til avlevering når det fastsatte avleveringstidspunktet er nådd.

### **Avlevering**

Ifølge kapittel VIII, § 8-2, bokstav a i Forskrift om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver er definisjonen av *avlevering slik*: En fysisk overføring av arkivmateriale og råderetten over dette materialet

Med avlevering menes altså flytting og overdragelse av ansvaret for arkivsaker fra en arkivskapende institusjon til en arkivdepotinstitusjon.  
Depotinstitusjon for Høgskolen i Lillehammer er Statsarkivet på Hamar.

### **Krav til materiale og framgangsmåte ved avlevering**

Arkivmaterialet skal avleveres når det er ca 25 - 30 år gammelt, jf arkivforskriften § 5-2.

#### **Unntak:**

- Elektronisk arkivmateriale og materiale på andre optiske og magnetiske medium. Riksarkivaren kan fastsette at det skal deponeres kopier i arkivmaterialet på et tidligere tidspunkt. Ved periodisering skal elektronisk journal straks deponeres i arkivdepot, jf arkivforskriften § 3-17.
- Nedlegging av institusjonen, jf arkivforskriften § 5-3.

**Krav til materialet som skal avleveres** er nedfelt i arkivforskriften § 5-4.

**Fremgangsmåte ved avlevering** skal følge Riksarkivarens bestemmelser i Forskrift om utfyllende tekniske og arkivfaglige bestemmelser om behandling av offentlige arkiver:

Kapittel VI: Bestemmelser om avlevering og overføring av ikke-elektronisk arkivmateriale i statsforvaltningen

Kapittel VII: Fellesbestemmelser for innbinding av møtebøker, kopibøker, registre mv. i statlig og kommunal forvaltning

Kapittel VIII: Bestemmelser om elektronisk arkivmateriale som avleveres eller overføres som depositum til Arkivverket  
Oversikt over arkivene for Oppland distriktshøgskole (fra perioden 1971 – 1994) som Høgskolen i Lillehammer har ordnet og avlevert, finnes i arkivplanens punkt 6 Bestandsoversikt.

## **Brukeradministrasjon / tilgangsstyring**

### **Roller**

Oppsett av roller for brukere ved HiL

Tilgangskoder

Registrerte koder

Oppsett av tilgangskoder for brukere ved HiL

Påføring av tilgangskode m.v. på inngående dokumenter

Påføring av tilgangskode m.v. på nye utgående og interne dokumenter

Tilgangsgrupper

Leserettigheter

Skriverettigheter

### **Roller**

I ePhorte har alle brukere minst én rolle, som sammen med en del andre kriterier, styrer hva de får lov til å gjøre.

Standardrollene for HiL er:

Systemansvarlig **SY**

Arkivleder/arkivar **AR1/AR2**

Saksbehandler **SB**

Leder/saksfordeler **LD**

Utvalgssekretær **US**

Andre AN (kun lesetilgang)

Som hovedregel er administrativt ansatte ved HiL brukere av ePhorte, og alle brukere har fått tildelt én eller flere roller.

I denne sammenheng regnes også rektor, prorektor og dekaner som administrativt personale.

### **Tilgangskoder**

Hva en bruker skal få lov til å lese og søke etter internt i ePhorte og hva som vises på offentlig journal, styres ved hjelp av tilgangskoder og aktiv skjerming av opplysninger på saks- og journalpostnivå. Kun de som har tilgang til påført tilgangskode, innenfor aktuell administrativ enhet, kan lese det som er skjernet internt.

Noe av hensikten med innføring av ePhorte, er at alle brukere ved HiL skal kunne dele informasjon. Tilgangskoder bør derfor kun brukes når opplysningene skal skjermes for eksterne parter. Dette gjelder imidlertid ikke personal- eller studentsaker. Her skal dokumenter være skjernet i de fleste tilfeller.

### **Registrerte koder**

Standard koder for HiL er:

**U** Unntatt offentlighet

**MU** Møtedokumenter unntatt offentlighet

**P** Personalmapper/-opplysninger (avsender/mottaker blir avskjernet)

**SP** Strengt fortrolig personalsak - personalet (tittel og avsender/mottaker blir skjernet)

### **Oppsett av tilgangskoder for brukere ved HiL**

Alle brukere har tilgang til U for egne saker, d.v.s. til dokumenter som de har utarbeidet selv, eller hvor de er mottakere eller kopimottakere.

Det er kun Høgskoledirektør og arkivet som har tilgang til alle saker/dokumenter for hele organisasjonen i arkivbasen.

Alle ledere har tilgang til saker/dokumenter som er unntatt offentlighet for sin enhet.

Alle dekaner, kontorsjefer og øverste administrative ledere har tilgang til personalmappene i tillegg til ansatte ved personalseksjonen og arkivet.

Systemansvarlig legger inn og oppdaterer i henhold til vedtatte tilgangsrettigheter. Eventuelle utvidelser av tilgangskoder må være klarert av ledelsen.

### **Påføring av tilgangskode m.v. på inngående dokumenter**

På nye saker og dokumenter som kommer inn, foreslår arkivet tilgangskode med tilhørende hjemmel og skjerming av taushetsbelagte opplysninger.

Saksbehandler/leder har imidlertid ansvar for offentlighetsvurderingen.

Personalmapper påføres alltid tilgangskode P ved oppretting av ny "mappe"/sak. I tillegg skjermes navn.

Dersom koden SP benyttes skjermes automatisk både tittel og avsender/mottaker på JP.

### **Påføring av tilgangskode m.v. på nye utgående og interne dokumenter**

Saksbehandler/leder skal ta stilling til tilgangskode og hjemmel og aktivt skjermes taushetsbelagte opplysninger på nye utgående dokumenter og interne dokumenter.

## **Tilgangsgrupper**

Det kan opprettes tilgangsgrupper på tvers av administrative enheter hvis en eller flere personer ansatt i en annen administrativ enhet enn den hvor en bestemt type saker hører hjemme har behov for lese/skrivetilgang til slike saker.

Det finnes to typer tilgangsgrupper:

**Faste:** Forhåndsdefinerte tilgangsgrupper som kan gjenbrukes på mapper/poster. Faste tilgangsgrupper må opprettes av systemansvarlig (arkivleder). Saksbehandler kan legge til en fast tilgangsgruppe på sak eller JP.

**Ad hoc:** Tilgangsgruppe som saksbehandler kan opprette og tilknytte en enkelt saksmappe eller JP. Kan ikke gjenbrukes.

## **Leserettigheter**

En brukers rettighet til å gjenfinne og lese informasjon styres via:

- tilgangskoder
- tilgangsgrupper
- brukerens autorisering for ulike tilgangskoder

**Uten tilgangskode på sak eller JP kan interne brukere lese alt og taushetsbelagt informasjon vil ligge åpen for offentligheten!**

## **Skriverettigheter**

En brukers rettighet til:

- å opprette saker
- å opprette journalposter og dokumenter
- å endre informasjon
- skrive dokumenter

styres via

- roller
- tilgangskoder/-grupper
- status (saker/JP/dokumenter)

## **Offentlig journal**

Offentlig journal legges ut på hjemmesiden hver uke etter nøye kontroll slik at personsensitive opplysninger alltid skal være skjermet. Likeså settes denne journalen opp slik på HiL-weben at Google og andre søkemotorer ikke indekserer disse sidene. Det betyr at interesserte kan få opp treff på offentlig journal + HiL og finne frem til selve journalen, men vil ikke få treff på innholdet i selv pdf-filene. Offentlig journal fjernes fra hjemmesiden etter seks måneder.

## Framfinningssystemer

**Arkivordningen ved HiL** skiller mellom:

dagligarkiv (aktivt arkiv - siste periode)

bortsetningsarkiv (pr. dato: Arkivmaterialet fra 1.8.1994 – 1.1..2006)

avlevert arkiv.

### Finne saker / dokumenter i dagligarkiv

Dagligarkiv inneholder materiale som har vært saksbehandlet i siste del av inneværende arkivperiode eller som ikke er ferdig saksbehandlet.

Arkivmaterialet skal være ordnet og organisert på en måte som gjør at det er enkelt å finne fram. På den måten kan det fylle sin funksjon som informasjons- og dokumentasjonskilde.

Høgskolen innførte i 2006 fullelektronisk arkivering, d.v.s. originaldokumentene er elektroniske og papirversjonene blir regnet som arbeidskopier. Systemet som benyttes er ePhorte fra ErgoGroup, og den som skal finne saker må ha tilgang til / være opprettet som bruker av dette systemet.

Alle hoveddokumenter i en sak må være elektroniske, og saksdokumenter skal registreres i journalen før de går til saksbehandling. Dette gjelder også for hastesaker, jf. Arkivforskriften § 3-5. Dette medfører at:

alle innkomne, arkivverdige dokumenter mottatt på papir skal arkivet skanne og registrere før de går til saksbehandling.

Alle innkomne, arkivverdige dokumenter mottatt på høgskolens e-postmottak skal arkivet laste ned, lagre og registrere i PDF-format (eventuelt også i produksjonsformat dersom dette er nødvendig) før de går til saksbehandling. E-post har også saksbehandlere tilgang til å registrere, og dette skal gjøres dersom e-posten inngår i saksbehandling.

**Papirversjonen av dokumenter** som er journalført, skannet og elektronisk arkivert oppbevares hos Arkivtjenesten i 2 måneder før de makuleres av arkivet. Dokumenter som inneholder **sensitive personopplysninger oppbevares separat** inntil de har gått ut av administrativ bruk. Dokumentene makuleres under oppsyn av arkivet.

Som hovedregel skannes **vedleggene** inn ett og ett. Hensikten å skille mellom hoveddokument og vedlegg er at vedlegg skal kunne knyttes elektronisk til andre journalposter i systemet.

Vedlegg som er i format som **ikke kan skannes**, ettersendes pr. post/leveres til ansvarlig saksbehandler. I merknadsfeltet i journalpostopplysningene påføres at vedlegget er oversendt/levert til saksbehandler + dato.

Det kan tas kopi av første (og eventuelt siste siden) - hvis mulig - som skannes inn som et vedlegg til hoveddokumentet.

Vedleggene påføres saks- og dokumentnummer, arkivkode og merknad om at de skal returneres til sentralt arkiv for arkivering etter endt saksbehandling. Vedleggsarkivet i sentralt arkiv vil være ordnet etter saksnummer. Høgskolens arkiv for perioden som startet i 2006 er delt opp i arkivdelar som angir logisk arkivering av saker.

Alle sakene i en arkivdel er ordnet etter ett og samme ordningsprinsipp. f.eks. arkivnøkkel, fødselsnummer, , og alle sakene i en arkivdel periodiseres på samme måte/samme tidshorisont.

**Saksarkiv for HiL SAK** Ordningsprinsipp: Primært: Arkivnøkkel Sekundært: Arkivnøkkel

**Personalarkiv for HiL PERS** (saker som gjelder den enkelte tilsatte) Ordningsprinsipp:

Primært: Arkivnøkkel (221) Sekundært: Fødselsnummer

Det opprettes én sak for hver tilsatt i HiL. Saken opprettes ved mottak/oppretting av første arkivverdige dokument etter 1. januar 2006 som gjelder den tilsatte.

Papirbaserte personalmapper ble avsluttet ved utgangen av 2005, og oppbevares som tidligere.

**Styrer, råd og utvalg ved HiL UTVALG** (for utvalg som utarbeider saksframlegg)

Ordningsprinsipp: Primært: Arkivnøkkel Sekundært: Arkivnøkkel

Pr. september 2010 er utvalgsmodulen ikke tatt i bruk på ordinær måte, men utvalgsdokumenter arkiveres der.

### **Finne saker / dokumenter i bortsettingsarkiv**

Høgskolens bortsettingsarkiv inneholder arkivmateriale fra arkivperioden 1994 – 2006. Denne perioden er avsluttet, men ikke avlevert til Statsarkivet. Denne perioden hadde elektronisk journalføring, men dokumentene var på papir.

Det er opprettet en historisk base i dagens arkivsystem: ePhorte.

**Basen har – i hovedsak - kun arkivtilsatte tilgang til, og den ligger under nettadressen:**

<https://higkurs.ephorte.uninett.no> hvor en velger databasen hist hil.

Høgskolens saksarkiv for perioden 1994 – 2006 er ordnet etter en arkivnøkkel, og arkivnøkkelens prinsipp for ordning av arkivmaterialet består av to hovedelementer:

1. Inndelingsprinsipp: Primært: Emneinndeling (dokumentets innhold)

Sekundært: Inndelt etter objekt ( personalmapper)

2. Rekkeordningssystem: Primært: Desimalsystem

Sekundært: Navn (personalmapper)

For perioden august 1994 - juli 2003 er høgskolens saksarkiv ordnet etter Arkivnøkkel for de statlige høgskoler, opprettet juli 1994, revidert oktober 1996.

Gjeldende arkivnøkkel er i ettertid revidert i fm utarbeidelse av kassasjonsplan. Revidert nøkkel med kassasjonsplan ble godkjent i mai 2001, og hadde tilbakevirkende kraft til 1994. Arkivmaterialet settes bort i henhold til Allment arkivskjema, som er mer omfattende enn arkivnøkkelens. Dette for å finne igjen ulike serier i arkivet. Samlet bortsetting skal gjelde en arkivperiode.

**Møtebøker, referatprotokoller, forhandlingsprotokoller er satt bort i kronologisk rekkefølge.** Dokumentene skulle fortrinnsvis bindes inn. Hvert styre, råd eller utvalg skal stå samlet.

**Kopibøker og andre overgripende registre skal bindes inn og settes bort kronologisk.** (Gjelder papirarkiv)

**Saksarkivet er satt bort etter gjeldende arkivnøkkel, og skal stå samlet for perioden.**

**Personalbyggene ble avsluttet ved skarpt periodeskille 01.01.2006, og ble bortsatt alfabetisk, fysisk skilt fra saksarkivet.**

Nye elektroniske personalmapper ble opprettet 2006, og det ble lagt henvisning til tidligere fysisk personalmappe.

**Eksamensoppgaver** skal arkiveres for hvert studieår – legges i saksarkivet i etterkant av eksamen.

**Eksamensbesvarelser** (master og PhD) som skal bevares etter spesielle kassasjonsregler for universitet og høgskoler, legges inn i ePhorte hvert studieår.

**Eksamensprotokoller** skal bevares og bindes inn (arkivkode 454). Uttrekk fra databasen i Mstas /FS skal deponeres i Statsarkivet, ansvar Studiedirektør v/FS ansvarlige.

### **Utlån**

Dersom saker fra bortsatt arkivmateriale skal lånes bort, må det settes ned lånekort. Det må følges opp at sakene blir returnert til bortsettingsarkivet.

Oversikt over materialet i bortsettingsarkivene finnes i Arkivplan HiL Bestandsoversikt.

### **Avleverte arkiv**

Høgskolen har avlevert materiale fra tidligere Oppland distriktshøgskole (1971-1994) til Statsarkivet på Hamar og Riksarkivet. Arkivverket har utarbeidet kataloger.

Med utgangspunkt i nevnte kataloger, kan en be om Innsyn / kopi av dokumenter hos arkivverket på Hamar.

## **6. Bestandsoversikt**

### **ARKIVSERIER FRA OPPLAND DISTRIKTSHØGSKOLE (1971-94)**

#### **Opplysninger i forbindelse med bortsetting/avlevering av Oppland distriktshøgskoles arkiv perioden 1971-94**

Denne avleveringen inneholder arkivstykker fra skolen ble etablert i 1971 til 01.08.1994 da Oppland distriktshøgskole gikk over til å hete Høgskolen i Lillehammer.

#### **Saksarkivet er delt i perioder etter arkivnøkler: 1971 - 1974, 1974 –85 og 1985 - 1994.**

Saksarkivet for ODH ble avlevert til Statsarkivet i Hamar høsten 2001. Det ble gjennomgått og sortert av Bjørg Grindal ved Statsarkivet.

### **ARKIVSERIER FRA DET REGIONALE HØGSKOLESTYRET FOR OPPLAND**

Fellesorgan for høgskolene i Gjøvik og Lillehammer og bestod 1977 – 1994 i Lillehammer.

#### **Opplysninger i forbindelse med bortsetting av Det regionale høgskolestyret for Oppland sine arkiver:**

Denne avleveringen inneholder arkivstykker som dekker hele tidsperioden til Det regionale høgskolestyret for Oppland, det vil si fra 1977 - 1994.

Saksarkivet er ordnet etter nøkkel og dekker hele perioden.

#### **Arkivnøkkelen ligger i saksarkivet på arkivkode 004.1.**

Det har i perioden blitt benyttet flere arkivnøkler, uten at arkivet er blitt avsluttet. Årsaken til det er at det ikke har forekommet store endringer i nøkkelen. Av den grunn ligger det flere arkivnøkler i saksarkivet, noe som skal gjøre det mulig å finne de ønskede saker ut fra gjeldende tidsperiode.

Arkivet ble avlevert til Statsarkivet i Hamar da Det regionale høgskolestyret ble nedlagt i 1994 i forbindelse med opprettingen av de statlige høgskolene med egne styrer.

#### **Avsluttet men ikke avlevert papirarkiv for Høgskolen i Lillehammer for perioden 01.08.1994 – 08.05.2006**

De pålagte uttrekk av arkivbasen for Høgskolen i Lillehammer 1994 – 2006 ble oversendt Arkivverket og godkjent og deponert der da høgskolen gikk over til fullelektronisk arkiv fra 01.01.2006.

Dette arkivmateriale er ordnet og satt i arkivbokser i fjernarkiv med avleveringslister etter at kassasjon var foretatt og klargjort for avlevering.

Det kasserte materialet er også foreløpig å finne i adskilte arkivbokser i fjernarkivet.

Både Offsak-(1992-97)- og Modulink-(1997-2006)basene er konvertert til ePhorte og skal kunne søkes i via den historiske basen som er tilgjengelig (under kursbase-innloggingen).

## **HiLs produksjonsbase for fullelektronisk arkivering fra 2006**

Det daglige HiL-arkiv ligger fra 2006 i felles arkivbase med Høgskolen i Gjøvik på servere ved USIT, Universitetet i Oslo. Denne løsningen ble valgt da de to institusjonene skulle slå sammen i 2006, men som ikke ble noe av den gangen. Nå utredes prosjekt Innlandsuniversitetet hvor også Høgskolen i Hedmark er deltaker.

UNINETT har ansvaret for driften av Ephorte-systemet for de statlige høgskolene som har valgt denne felles løsningen. Databasen EPHROD ble oppgradert pr. 19.05.11 til versjon 11.2.0.2.

**Vedlegg:**

- 1) Policy og retningslinjer for informasjonssikkerhet ved HiL fra 2009
- 2) Revidert utfylt skjema for dokumentbasert tilsyn av elektronisk arkivdanning fra 03/11.
- 3) Sentrale arkivtermer for høgskolens bruk
- 4) Grunnkurs for saksbehandling i ePhorte

# 1 Policy for informasjonssikkerhet

## 1.1 Sikkerhetsmål

Høgskolen i Lillehammer (HiL) er forpliktet til å ivareta Konfidensialitet, Integritet og Tilgjengelighet i alle fysiske og elektroniske informasjonsverdier i konsernet for å sikre etterlevelse av forretningsmessige, kontraktsmessige og regulative krav.

De overordnede mål for informasjonssikkerheten v/Høgskolen er å;

- Sørge for samsvar med gjeldende lover, forskrifter og retningslinjer.
- Ivareta Høgskolens, ansatte, medlemmenes og andre brukeres krav til konfidensialitet, integritet og tilgjengelighet.
- Etablere kontroller for å beskytte Høgskolens informasjon og informasjonssystemer mot tyveri, misbruk og andre former for skade og tap.
- Motivere ledelse og ansatte til å opprettholde ansvar, eierskap, kunnskap og kompetanse om informasjonssikkerhet slik at frekvens og skadenivå av sikkerhetshendelser kan minimaliseres.
- Sikre at HiL er i stand til å fortsette sine tjenester også dersom større sikkerhetshendelser skulle inntreffe.
- Bidra til at personvernet ivaretas.
- Sikre tilgjengelighet og pålitelighet i nettverksinfrastruktur og tjenester levert og driftet av Høgskolen
- Følge metoder fra internasjonale standarder for informasjonssikkerhet (ISO/IEC 27001).

## 1.2 Sikkerhetsstrategi

Høgskolens gjeldende forretningsstrategi og rammeverk for risikostyring er førende for å identifisere, bedømme, evaluere og kontrollere informasjons relaterte risikoer gjennom etablering og vedlikehold av policy for informasjonssikkerhet.

Begrepet informasjonssikkerhet er knyttet til

- **konfidensialitet**; sikkerhet for at kun autoriserte personer har tilgang til informasjonen, og at den ikke avsløres til uvedkommende.
- **integritet**; sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter.
- **tilgjengelighet**; sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig for autoriserte ved behov.

Høgskolen praktiserer et prinsipp om åpenhet, men vil kunne prioritere hensyn i forhold til tilgjengelighet, integritet og konfidensialitet i forhold til aktuelle situasjoner og tjenester.

Alle ansatte og studenter v/Høgskolen og dataleverandører (andre leverandører også?) er forpliktet til å følge denne policy. Overtredelse av denne policy for informasjonssikkerhet og vedtatte sikkerhetskrav vil derfor være et tillitsbrudd mellom brukeren og Høgskolen, og vil kunne medføre konsekvenser for ansettelses- eller avtaleforholdet.

## Versjonskontroll av retningslinjer

Versjon	Dato	Endringsbeskrivelse
0.7	30.01.2009	Initiell versjon fra Uninett
0.8	18.02.2009	Justert etter Workshop
0.9	April/mai 2009	Høring
1.0	16. juni 2009	Pkt 3.7.20, Vilkårene for innsyn er presisert

### Forfatter og distribusjon

Forfatter	Dato	Rolle
Kenneth Høstland, Per Arne Enstad	30.01.2009	HIL Gigacampus
Distribusjonsliste		Rolle
Jostein Skurdal		Høgskoledirektør
Lars Petter Mathisrud		Personal- og organisasjonsdirektør
Jan Aasen		Økonomi- og driftsdirektør
Kai Gjessing		IT Sjef

### Gjennomgang og godkjenning

Dato	Navn	Rolle	Initialer
18. februar 2009	Jostein Skurdal	Høgskoledirektør	JSK
16. juni 2009	Høgskolestyret	Høgskolestyret	JSK



# Innholdsfortegnelse

<b>1</b>	<b>POLICY FOR INFORMASJONSSIKKERHET .....</b>	<b>26</b>
1.1	SIKKERHETSMÅL.....	26
1.2	SIKKERHETSSTRATEGI .....	26
<b>2</b>	<b>STYRENDE DOKUMENTER FOR SIKKERHETSARBEIDET .....</b>	<b>31</b>
2.1	FORMÅL MED STYRENDE DOKUMENTER.....	31
2.2	DOKUMENTSTRUKTUR .....	31
<b>3</b>	<b>RETNINGSLINJER FOR INFORMASJONSSIKKERHET .....</b>	<b>32</b>
3.1	OPPFØLGING AV POLICY FOR INFORMASJONSSIKKERHET .....	32
3.2	RISIKOSTYRING .....	32
3.3	SIKKERHETSORGANISASJON.....	32
3.4	KLASSIFISERING OG KONTROLL .....	33
3.5	INFORMASJONSSIKKERHET KNYTTET TIL PERSONALET .....	34
3.6	INFORMASJONSSIKKERHET KNYTTET TIL FYSISKE FORHOLD.....	35
3.7	KOMMUNIKASJON OG DRIFTSADMINISTRASJON .....	37
3.8	TILGANGSKONTROLL.....	39
3.9	SYSTEMUTVIKLING OG VEDLIKEHOLD .....	40
3.10	HENDESESHÅNDTERING .....	41
3.11	KONTINUITETSPLANLEGGING.....	41
3.12	SAMSVAR.....	41
<b>4</b>	<b>ROLLER OG ANSVARSOMRÅDER.....</b>	<b>42</b>
4.1	ROLLER OG ANSVARSOMRÅDER .....	42

## 2 Styrende dokumenter for sikkerhetsarbeidet

### 2.1 Formål med styrende dokumenter

Styrende dokumenter for Informasjonssikkerhet skal bidra til å oppnå et balansert nivå på tiltak i forhold til den risiko og de rammebetingelser HIL står overfor.

Det skal eksistere dokumenterte krav og retningslinjer knyttet til informasjonssikkerhet basert på oppdaterte risikoanalyser. De øvrige systemer og infrastruktur skal være dekket av gode basiskontroller innen informasjonssikkerhet som til en hver tid skal etterleves.

### 2.2 Dokumentstruktur

2.2.1 HIL har organisert dokumentstrukturen for beskrivelse av sin sikkerhetsarkitektur i 3 nivåer: Sikkerhetspolicy, Overordnede retningslinjer og prinsipper og rutiner og prosedyrer.

<b>Sikkerhetspolicy</b> definerer mål, hensikt, strategi, ansvar og overordnede krav. I tillegg gir denne en oversikt over de etablerte styrende dokumenter knyttet til informasjonssikkerhet.	
<b>Overordnede retningslinjer/Prinsipper</b> for Informasjonssikkerhet. Her defineres <b>hva</b> som må gjøres for å etterleve den etablerte policy.	
<b>Standarder og prosedyrer</b> for Informasjonssikkerhet med detaljerte retningslinjer for <b>hvordan</b> disse standardene skal implementeres. Dette bør etter hvert etableres for alle sentrale plattformer	

## 3 Retningslinjer for informasjonssikkerhet

### 3.1 Oppfølging av Policy for informasjonssikkerhet

- 3.1.1 Høgskolens ledelse (administrerende direktør) skal sørge for at policy for informasjonssikkerhet, retningslinjer, rutiner og standarder blir benyttet og fulgt opp.
- 3.1.2 Høgskolens ledelse skal sørge for at det tilrettelegges for alle brukere slik at de får nødvendig opplæring og materiell, og slik at brukerne er i stand til å beskytte Høgskolens informasjon og informasjonssystemer.
- 3.1.3 Sikkerhetspolicyen skal gjennomgå og oppdateres regelmessig.
- 3.1.4 Alle viktige endringer mht. Høgskolens aktivitet, eller andre eksterne endringer som vil påvirke dagens trusselbilde, skal føre til en revidering av policyen og retningslinjer som angår sikkerhet.

### 3.2 Risikostyring

#### Risikovurdering

- 3.2.1 Høgskolen skal ha en tilnærming til sikkerhet som er basert på risikovurderinger.
- 3.2.2 HIL skal løpende analysere risikoer og vurdere behovet for beskyttelsestiltak. Tiltak skal vurderes med hensyn til effektivitet, kostnad, praktisk gjennomførbarhet.
- 3.2.3 Risikovurderinger skal identifisere, kvantifisere og prioritere risikoer i forhold til kriterier for akseptabel risiko som er relevant for Høgskolen.
- 3.2.4 Det skal gjennomføres regelmessig risikovurdering i forhold til informasjonssystemer eller når det skjer endringer av betydning for informasjonssikkerheten.
- 3.2.5 Risikovurderinger skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.  
Det skal benyttes anerkjente metoder for risikovurdering,

#### Håndtering av risiko

- 3.2.6 Håndtering av risiko skal foretas i forhold til kriterier som ledelsen har akseptert.
- 3.2.7 Risikovurderinger skal godkjennes av Høgskolens ledelse og/ eller systemeiere.
- 3.2.8 Ved identifisering av uakseptabel risiko, skal det iverksettes tiltak for å redusere risiko til et akseptabelt nivå.

### 3.3 Sikkerhetsorganisasjon

#### Sikkerhetsorganisasjon

- 3.3.1 Ansvar for sikkerhetsområdet er fordelt som følger:
  - Det overordnede sikkerhetsansvaret ligger hos høgskoledirektøren.
  - Økonomi- og driftsdirektør er delegert ansvaret for sikkerhet ved Høgskolen – og deriblant informasjonssikkerheten. ØD-direktøren er med dette CSO (Chief Security Officer) v/Høgskolen.
  - Økonomidirektøren har utførende ansvar for informasjonssikkerhet i økonomi- og innkjøpssystemene.

- Økonomi- og driftsdirektør har utførende ansvar for informasjonssikkerhet knyttet til bygningsmessig infrastruktur ("Fysisk sikkerhet").
- Personal- og organisasjonsdirektøren har det utførende ansvar for informasjonssikkerhet knyttet til personaldata i henhold til Personopplysningsloven.
- Personal- og organisasjonsdirektøren har ansvaret for personal data i SAP
- Arkiv leder har det utførende ansvar for arkiver.
- Studiedirektøren har utførende ansvar for studentregisteret og annen studentrelatert informasjon.
- **Norsk samfunnsvitenskapelig datatjeneste** er personvernombud for forskningsrelaterte personopplysninger. Hovedbibliotekar har utførende ansvar.
- IT-sjefen har det utførende ansvaret for informasjonssikkerhet knyttet til IT-systemer og IT-infrastruktur.
- HMS ansvaret ligger til høgskoledirektør, mens det operasjonelle ansvaret er delegert til Personal- og organisasjonsdirektør.

## Sikkerhetsforum

- 1.3.2 Høgskolen har etablert et informasjonssikkerhetsforum som består av: Økonomi- og driftsdirektør, Personal- og organisasjonsdirektøren og IT-sjefen.
- 1.3.3 Sikkerhetsforumet skal fremme operasjonell informasjonssikkerhet i organisasjonen gjennom nødvendig engasjement og tilstrekkelig ressursbruk.
- 1.3.4 Sikkerhetsforumet skal ha følgende oppgaver:
- Gjennomgå og godkjenne retningslinjer for informasjonssikkerhet og generelle ansvarsforhold.
  - Overvåke vesentlige endringer i truslene mot organisasjonens informasjonsaktiva.
  - Gjennomgå og overvåke innrapporterte sikkerhetshendelser.
  - Godkjenne større initiativ for å styrke informasjonssikkerheten.

## 3.4 Klassifisering og kontroll

- 3.4.1 Informasjon og infrastruktur skal klassifiseres med hensyn til nødvendig sikkerhetsnivå og tilgangsbegrensning.
- 3.4.2 Informasjon skal klassifiseres i en av tre følgende kategorier for konfidensialitet:

### Fortrolig informasjon

Informasjon av sensitiv art, og hvor uautorisert tilgang (også internt) kan medføre betydelig skade for enkeltpersoner, Høgskolen eller deres interesser. Fortrolig informasjon er her synonymt med forvaltningslovens "Unntatt Offentlighet" og POL sensitive personopplysninger. Slik informasjon skal sikres i "Røde" områder.

### Intern informasjon

Informasjon som kan skade virksomheten eller være upassende at tredjepart får kjennskap til. Systemeier avgjør lagrings- og delingsmåte.

### Åpen informasjon

Annen informasjon som ikke inneholder intern eller fortrolig informasjon er åpen.

- 3.4.3 HIL skal gjennomføre risikoanalyser for å kunne klassifisere informasjon ut fra hvor kritisk den er for virksomheten. Systemeier er ansvarlig for dette.
- 3.4.4 Det skal være utarbeidet rutiner for gjennomføring av informasjonsklassifisering og risikoanalyser.
- 3.4.5 Brukere som forvalter informasjon på Høgskolens vegne skal behandle denne i henhold til klassifiseringen.
- 3.4.6 Fortrolige dokumenter skal være tydelig merket.

## **3.5 Informasjonssikkerhet knyttet til personalet**

### **Ved tilsetting**

- 3.5.1 Ansvar for tilsetting skal være klart definert i egen rutine med relevant tilgangsskjema.
- 3.5.2 Sikkerhetsansvar og roller for relevant personell, både ansatte og innleide, skal beskrives.
- 3.5.3 Sjekk av bakgrunnen til alle som innstilles til stillinger ved HIL skal foretas iht. relevante lover og regler.
- 3.5.4 Taushetserklæring skal signeres av alle arbeidstakere, og oppdragstakere eller andre som kan få kjennskap til fortrolig og/eller intern informasjon.
- 3.5.5 IT-reglement skal signeres i alle ansettelsesforhold og ved systemtilganger for tredjepart.

### **For ansatte gjelder**

- 3.5.6 IT-reglement refererer til Høgskolens krav til informasjonssikkerhet og den ansattes og eller oppdragstakers ansvar for å oppfylle disse.
- 3.5.7 IT-reglement skal signeres og gjennomgå med ansatte ved alle nyansettelser
- 3.5.8 Alle ansatte og tredjepartsbrukere skal få tilstrekkelig opplæring og oppdatering i Policy for informasjonssikkerhet og relevante retningslinjer og prosedyrer. Det vil være varierende grad av krav til opplæring.
- 3.5.9 Vesentlige brudd på Policy for informasjonssikkerhet og -retningslinjer vil kunne medføre sanksjoner.
- 3.5.10 Høgskolens informasjon, informasjonssystemer og andre verdier (f.eks. telefon), skal kun benyttes til de formål de er bestemt for. Nødvendig privat bruk tillates.
- 3.5.11 Bruk av Høgskolens IT-infrastruktur i egen næringsvirksomhet er ikke tillatt.

### **Avslutning eller endring av ansettelse**

- 3.5.12 Ansvar for avslutning eller endring av ansettelsesforhold skal være klart definert i egen rutine med relevant avgangskjema.
- 3.5.13 Høgskolens eiendeler skal leveres inn ved opphør av ansettelsesforhold.
- 3.5.14 HIL endrer eller stenger tilgangsrettigheter ved opphør av ansettelse eller endring av arbeidsforhold.

### **For studenter gjelder**

- 3.5.15 IT-reglement refererer til Høgskolens krav til informasjonssikkerhet og studentene plikter å oppfylle disse.
- 3.5.16 IT-reglement bekreftes ved aktivering av studentkonto.
- 3.5.17 Ved avslutning av studier deaktiveres tilganger til bygg og systemer og filer og e-post slettes etter definert rutine

## **3.6 Informasjonssikkerhet knyttet til fysiske forhold**

### **Sikkerhetsområder**

- 3.6.1 Sikre fysiske soner benyttes for å beskytte områder som inneholder IT-utstyr og informasjon som krever beskyttelse. Sikre soner skal beskyttes med hensiktsmessige adgangskontroller for å sikre at kun autorisert personell får adgang.

3.6.2 Følgende soneinndeling skal benyttes:

Sikringsnivå	Område	Sikring
Grønn	Alt er i utgangspunktet tilgjengelig. Kantine.	Ingen
Gul	Noen tekniske rom (slik som koblingsrom?), printerrom og rom hvor det f.eks. finnes skjermverdig / intern informasjon. Kontorlokaler, møterom, noen arkiver.	Utskrift beskyttes med "Follow me"-funksjonalitet der det skrives ut fortrolig informasjon.

Områdene skal avmerkes i bygningsplansjer eller eksplisitt beskrives i eget dokument.

- 3.6.3 Systemeier er ansvarlig for godkjenning av medarbeidere som skal ha adgang til sikre områder.
- 3.6.4 Alle Høgskolens lokaler skal sikres med tilstrekkelige sikringsystemer i henhold til klassifisering, ref. tabell ovenfor, inkludert relevant sporbarhet/logging.
- 3.6.5 Sikkerhetsansvarlig (CSO) er ansvarlig for at arbeid utført av tredjepart i sikre områder er relevant overvåket og dokumentert.
- 3.6.6 Røde områder skal være forsvarlig sikret mot miljøskader forårsaket av brann, vann, eksplosjon, vibrasjoner mv.
- 3.6.7 Alle skalledører og -vinduer skal låses og stenges ved arbeidsløst dags slutt. Siste medarbeider som forlater et område er ansvarlig for sikring.
- 3.6.8 Besøk i rød sone skal ledsages. Adgangskort kan gis til håndverkere, teknikere og andre, som trenger adgang til rød sone, mot at det utstedes ID-kort og utfyllt taushetserklæring.

### Sikring av utstyr

- 3.6.9 IT-utstyr klassifisert som "Høy" skal plasseres eller beskyttes slik at det reduserer risikoen for miljømessige trusler (brann, oversvømmelse, temperatursvingninger, fukt etc.). Tiltak skal iverksettes med basis i ROS-vurdering.
- 3.6.10 Informasjon klassifisert som "Fortrolig" skal passordbeskyttes og krypteres hvis det distribueres og oppbevares på andre medier enn den server det er lagret på.
- 3.6.11 Bærbart utstyr skal håndteres som verdifull håndbagasje under reiser.
- 3.6.12 Stasjonært utstyr kan kun tas ut av lokalene etter godkjenning fra overordnede.
- 3.6.13 Områder klassifisert som "Rød" skal sikres med relevant brannslukkingsutstyr med relevant varslings. Det skal jevnlig gjennomføres brannøvelser.

## **3.7 Kommunikasjon og driftsadministrasjon**

### **Operasjonelle prosedyrer og ansvarsområder**

- 3.7.1 Installasjon av IT-utstyr inklusive programvare skal skje etter definerte rutiner.
- 3.7.2 Systemeier skal sikre dokumentasjon av systemer etter Høgskolens standard.
- 3.7.3 Endringer skal gjennomføres kun når det er virksomhets- og sikkerhetsmessig velbegrunnet.
- 3.7.4 Systemeier har ansvaret for at det foreligger en nødprosedyre for å minimalisere effekten av feilslåtte endringer.
- 3.7.5 Dokumentasjon av driftsprosedyrer skal oppdateres etter vesentlig endringer.
- 3.7.6 Før nye systemer settes i produksjon skal det planlegges og risikovurderes for å forhindre at feil oppstår, i tillegg til å ha rutiner for overvåking og håndtering av uforutsette problemer.
- 3.7.7 Oppgaver og ansvar skal separeres på en slik måte at det reduserer muligheter uautorisert eller uforutsett misbruk av Høgskolens verdier.
- 3.7.8 Utvikling, test og vedlikehold skal separeres for å redusere risikoen for uautorisert tilgang eller uautoriserte endringer og for å redusere risikoen for feilsituasjoner.

### **Ekstern serviceleverandør**

- 3.7.9 Alle avtaler som angår utkontrakterte IT-systemer skal inneholde
  - krav til informasjonssikkerhet (Konfidensialitet, Integritet og Tilgjengelighet)
  - beskrivelse av avtalt sikkerhetsnivå,
  - krav til fortløpende rapportering av avvik fra leverandør
  - beskrivelse av hvordan HIL kan etterprøve at driftsleverandørene oppfyller avtalene.
  - rett til revisjon

### **Systemplanlegging og aksept/godkjenning**

- 3.7.10 Det skal tas hensyn til informasjonssikkerhetskrav før nye IT-systemer tas i bruk, designes, testes, implementeres og oppgraderes, samt ved systemendringer. Det skal utarbeides rutiner for endringshåndtering og systemutvikling/vedlikehold.
- 3.7.11 IT-systemene skal dimensjoneres etter forventede kapasitetsbehov. Belastningen skal overvåkes slik at oppgradering og tilpasning kan finne sted fortløpende. Dette gjelder særlig for virksomhetskritiske systemer.

## **Beskyttelse mot skadelig kode**

3.7.12 Datautstyr skal sikres mot virus og annen ondsinnet og/eller skadelig kode. Systemeier er ansvarlig for sikringen.

## **Sikkerhetskopiering**

3.7.13 Systemeier er ansvarlig for regelmessig sikkerhetskopiering og testing av denne, samt oppbevaring av all relevant data på Høgskolens IT-systemer.

3.7.14 Sikkerhetskopier skal oppbevares eksternt eller i egen relevant sikret brannsoner.

## **Nettverksstyring**

3.7.15 Systemansvarlig har det utførende ansvaret for å beskytte Høgskolens nettverk.

3.7.16 Det skal føres oversikt over alt IT-utstyr som kobles opp i Høgskolens eget nettverk (gjelder ikke studentbyene).

## **Håndtering av datamedier**

3.7.17 Håndtering av flyttbare datamedia (som taper, USB- minnepenner og utskrifter) skal sikres i henhold til klassifikasjon. Det påhviler den enkelte bruker at dette gjennomføres.

3.7.18 Media som kan inneholde fortrolig eller privat informasjon skal avhendes på sikker måte.

## **Utteksling av informasjon**

3.7.19 Det skal etableres prosedyrer og kontroller for å beskytte utveksling av informasjon med tredjepart eller forflytting av informasjon. Eksterne serviceleverandører (også betegnet Databehandlere) er underlagt Sikkerhetspolicyen.

3.7.20 Arbeidsgiver har bare rett til å gjennomføre, åpne eller lese e-post i arbeidstakers e-postkasse etter de regler som er fastsatt i personopplysningsforskriftens kapittel 9; -> når det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten, -> ved begrunnet mistanke om at arbeidstakers bruk av e-postkassen medfører grovt brudd på de plikter som følger av arbeidsforholdet eller kan gi grunnlag for oppsigelse eller avskjed. Innsyn skal alltid være saklig begrunnet. Du oppfordres til å samle personlig e-post i en egen mappe, kalt Privat, i ditt e-postarkiv, tilsvarende for ditt personlige lagringsområde. Det gjør et slikt arbeid enklere og det hindrer innsyn i private e-poster og filer. E-post og filer som arbeidsgiver forstår eller burde forstå er av privat karakter, forblir beskyttet etter reglene om personvern.

## **Offentlig tilgjengelig informasjon**

3.7.21 Systemeier har ansvar for at offentlig tilgjengelig informasjon, f eks på Høgskolens webtjenester, er tilstrekkelig beskyttet mot uautorisert endringer.

## Overvåkning av systemtilgang og bruk

- 3.7.22 Tilgang og bruk av systemer skal logges og overvåkes for å kunne identifisere potensielt misbruk.
- 3.7.23 Bruk og beslutninger skal være sporbare til en spesifikk entitet (f eks person eller enkeltsystem).
- 3.7.24 Systemeier (med samarbeidspartner(e)) skal registrere vesentlige forstyrrelser og uregelmessigheter i driften av systemene, samt mulige årsaker til feil.
- 3.7.25 IT-systemer og nettverk skal overvåkes i tilstrekkelig grad i forhold til kapasitet, oppetid og kvalitet for pålitelig drift og tilgjengelighet.
- 3.7.26 Systemeier (med samarbeidspartner(e)) skal logge sikkerhetshendelser i alle vesentlige systemer
- 3.7.27 Systemeier med samarbeidspartner(e)) skal sikre at systemenes klokke jevnlig synkroniseres til korrekt tid.
- 3.7.28 For informasjonssystemer som behandler personopplysninger, skal all autorisert bruk og forsøk på uautorisert bruk logges. Loggene skal lagres i minst 3 måneder.

## 3.8 Tilgangskontroll

### Tilgangs policy

- 3.8.1 Det skal finnes en skriftlig tilgangs- og passordpolicy som er basert på virksomhets- og sikkerhetsmessige krav og behov. Tilgangspolicyen skal revideres regelmessig.
- 3.8.2 Tilgangspolicyen skal inneholde retningslinjer for endringsfrekvens, passordregler (minimumslengde, type karakterer som kan/skal benyttes mv) og hvordan passordet kan lagres.

### Brukeradministrering- og ansvar

- 3.8.3 System og systemaksess autentiseres minimum ved hjelp av personlige brukeridenter og passord.
- 3.8.4 Brukere skal ha unike kombinasjoner av brukeridenter og passord eller tilsvarende.
- 3.8.5 Brukere er ansvarlige for enhver bruk av brukeridenter og passord. Brukere holder brukeridenter og passord konfidensielle, og røper bare disse hvis det er spesifikt autorisert av CSO og dokumentert.

### Tilgangskontroll/Autorisasjon

- 3.8.6 Tilgang til informasjonssystemer skal være autorisert av nærmeste leder, inkludert tilhørende aksessrettigheter (privilegier) som lagres i "aksesslister". Autorisasjoner gis på bakgrunn av "Need to know"-prinsippet, og reguleres av type rolle/stilling.

Aksesslister beskriver roller og ansvar med tilhørende tilgangsrettigheter med basis i følgende klassifisering.

HIL har følgende roller/klasser:

- Intern (flere roller, faste, midlertidige, innleide, timelærere mv.)
- Ekstern (flere roller)
- Studenter (flere roller)
- Hospitanter
- Publikum

## **Kontroll med nettverkstilgang**

- 3.8.7 Systemeier har ansvaret for at brukernes nettverkstilgang skjer i overensstemmelse med retningslinjene for tilgang.
- 3.8.8 Brukere skal kun ha tilgang til de tjenester de er autorisert for.

## **Mobilt utstyr og fjernarbeidsplasser**

- 3.8.9 Arbeid utenfor Høgskolens lokaler på Høgskolens utstyr er tillatt dersom sikkerhetspolicy overholdes og IT-reglement underskrives og overholdes.
- 3.8.10 Mobile enheter sikres med tilstrekkelige sikkerhetsmekanismer.
- 3.8.11 Fjerntilgang til Høgskolens nettverk skal kun skje gjennom sikkerhetsløsninger godkjent av systemeier.
- 3.8.12 Tilgang til privilegerte kontoer og fortrolige områder begrenses.
- 3.8.13 Brukere skal hindres i å tilegne seg informasjon de ikke skal ha tilgang til.

## **3.9 Systemutvikling og vedlikehold**

### **Sikkerhetskrav til informasjonssystemer**

- 3.9.1 Definisjon av virksomhetens krav til nye systemer eller videreutvikling av systemer skal inneholde sikkerhetsmessige krav.

### **Korrekt virkemåte i applikasjoner**

- 3.9.2 Data inn og ut av applikasjoner skal valideres for å sikre korrekthet og relevans.
- 3.9.3 Pålitelighet og integritet i informasjonsflyt skal defineres og relevante tiltak implementeres.

### **Kryptografiske kontroller**

- 3.9.4 Retningslinjer for administrasjon og bruk av kryptografiske kontroller for beskyttelse av informasjon, skal utvikles og implementeres.

### **Sikkerhet i systemfiler**

- 3.9.5 Endringer i produksjonsmiljø skal følge gjeldende rutiner:  
Implementering av endringer skal kontrolleres - gjennom bruk av formelle prosedyrer for endringskontroll - for å minimalisere mulighetene for skade på informasjon eller informasjonssystemer.

### **Sikkerhet i utvikling og vedlikehold**

- 3.9.6 De systemer som utvikles for og eventuelt av Høgskolen, skal ha klare krav til sikkerhet, inkludert validering av data, sikring av koden før produksjonssetting, og eventuell bruk av kryptografi.  
Endringer i produksjonsmiljø skal følge gjeldende rutiner.
- 3.9.7 Programvare testes og aksepteres formelt av eier/brukere og driftsansvarlig før programvaren overføres til produksjonsmiljøet.

## **Risikovurdering**

- 3.9.8 Før ny programvare (klassifisert som Høy), eller større endringer av ditto systemer settes i produksjon, gjennomføres en sårbarhets- og risikovurdering.

### 3.10 Hendelseshåndtering

#### Ansvar for rapportering

- 3.10.1 Leder og medarbeidere er ansvarlig for å rapportere brudd og mulige brudd på sikkerheten på Høgskolen til IT-tjenesten. Ved alvorlige tilfeller skal det rapporteres til CERT.

#### Måling

- 3.10.2 Det skal være mulig å definere kostnader ved sikkerhetshendelser. CSO er ansvarlig for dette.
- 3.10.3 Det skal utarbeides rutiner for avvikshåndtering og rapportering. Rutinen skal inneholde krav til tiltak for å forhindre gjentakelser og skadereduksjon.

#### Bevissikring

- 3.10.4 Alle medarbeidere skal være kjent med enkle rutiner for bevissikring ved mistanke om sikkerhetshendelser.

### 3.11 Kontinuitetsplanlegging

#### Kontinuitetsplan

- 3.11.1 Det skal utarbeides kontinuitetsplan som dekker kritiske/viktige informasjonssystemer og infrastruktur.
- 3.11.2 Kontinuitetsplan(er) skal utarbeides på bakgrunn av risiko- og sårbarhetsanalyser som tar utgangspunkt i forretningsrisiko.
- 3.11.3 Planen(e) skal avstemmes med Høgskolens øvrige beredskap og katastrofeplanverk.
- 3.11.4 Kontinuitetsplanen skal testes periodisk for å sikre at den er dekkende og at ledelse og ansatte forstår gjennomføringen.
- 3.11.5 Produksjonssystemer og andre systemer klassifisert som "Høy", skal ha reserveløsninger. Tabellen settes etter at ROS/BIA er gjennomført.

Kritikalitet	Tilgjengelighet	Beskrivelse
3 - Høy	<8 time	Systemet kan være utilgjengelig opp til 8 timer

### 3.12 Samsvar

#### Samsvar med juridiske krav

- 3.12.1 HIL skal følge gjeldende lovverk, samt andre eksterne retningslinjer
- Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven)

- Forskrift i forhold til om systematisk helse-, miljø-, og sikkerhetsarbeid i virksomheter (internkontrollforskriften)
- Lov om behandling av personopplysninger (personopplysningsloven)
- Lov om årsregnskap mv. (regnskapsloven)
- Lov om rett til innsyn i dokument i offentlig verksemd (offentleglova)
- Lov om elektronisk signatur (esignaturloven)

### Andre eksterne referanser

- Datatilsynets krav
- Datatilsynets «Veileder i informasjonssikkerhet for kommuner og fylker».

### Samsvar med Sikkerhetspolicy

- 3.12.2 Brukerne er pålagt å forholde seg i overensstemmelse med Policy for informasjonssikkerhet og retningslinjer. Oppfølging av ansatte er linjeledelsens ansvar.
- 3.12.3 Brukerne skal være klare over at bevis fra sikkerhetshendelser tas vare på (lagres) og overleveres ved rettslig krav.

### Kontroll og revisjon

- 3.12.4 Revisjonskrav og revisjonshandlinger planlegges og avtales med de involverte for å minimere risikoen for forstyrrelser av Høgskolens aktiviteter.

## 4 Roller og ansvarsområder

### 4.1 Roller og ansvarsområder

Styret har det overordnede ansvaret for at HIL sine verdier forvaltes på en effektiv og betryggende måte i henhold til gjeldende lover, forskrifter og avtaler. Administrerende direktør har det overordnede ansvar for sikkerheten ved Høgskolen.

#### Sikkerhetspolicy - Eier

- 4.1.1 Administrerende direktør eier sikkerhetspolicy og retningslinjer for informasjonssikkerhet (dette dokumentet). Administrerende direktør delegerer sikkerhetspolitisk dokumentasjon og signaturrettigheter til sikkerhetsansvarlig (CSO). Alle endringer i dokumentet skal dokumenteres og signeres av sikkerhetsansvarlig.

#### Sikkerhetsansvarlig

- 4.1.2 Økonomi og driftsdirektør er sikkerhetsansvarlig ved høgskolen (CSO, Chief Security Officer) og er ansvarlig for å koordinere skolens sikkerhetsarbeid.

## **Systemansvarlige**

- 4.1.3 Systemansvarlige er ansvarlig for spesifikke IT systemer som Høgskolen benytter. Systemansvarlige er personer som forvalter Høgskolens informasjonssystemer eller informasjon som er betrodd HIL fra andre parter. Hver enkelt system kan ha en eller flere dedikerte systemansvarlige. Disse er ansvarlige for å beskytte informasjonen, inklusive å implementere aksesskontrollmekanismer for å sikre konfidensialitet, og å foreta backup slik at kritisk informasjon ikke går tapt. De implementerer, drifter og vedlikeholder dessuten sikkerhetsmekanismer i tråd med intensjonen.

## **Systemeier**

- 4.1.4 Systemeier, er premissgiver for et visst system, herunder ansvarlig for krav til anskaffelse, utvikling og vedlikehold av informasjon og relaterte informasjonssystemer. Alle typer informasjon skal ha en definert eier. For hver type informasjon skal eiere definere hvilke brukere (brukergrupper) som skal ha tilgang til denne, og definere hva som er autorisert bruk av informasjonen. Tabell over systemer med tilhørende systemeier e skal utarbeides og løpende vedlikeholdes av IT avdelingen.

## **Konsulenter og kontraktspartnere**

- 4.1.5 Kontraktspartnere og innleide konsulenter skal skrive under taushetserklæring ved innsyn i fortrolige forhold.

## **Brukere**

- 4.1.6 Brukere er ansvarlige for å gjøre seg kjent med og rette seg etter Høgskolens IT-reglement. Spørsmål om håndtering av forskjellig type informasjon skal stilles til eieren av den aktuelle informasjonen, eventuelt systemansvarlig.

ARKIVVERKET

## RIKSARKIVET

**Vedlegg 2: Dokumentbasert tilsyn av elektronisk arkivdanning i universitets- og høgskolesektoren**

**Skjema til utfylling**

**Utsendt 26 .03 .2010 og revidert utfyllt mars 2011**

Opplysninger om universitetet/høgskolen

**Navn Høgskolen i Lillehammer**

Antall geografisk atskilte lokasjoner - en lokasjon

Skjemaet er fylt ut av Stilling Arkivleder Anne Kari Grimstad

Organisasjonsenhet

Ledelsens stab

Dato for utfylling 02.03.2011

### **A. Ansvar for og organisering av arkivarbeidet**

1 Hvem har det over- ordnede ansvaret for arkivtjenesten i følge arkivplanen

Stilling Høgskoledirektør Kari Kjenndalen

Organisasjonsenhet

ledelsen

2 Hvem har ansvaret for den daglige driften av arkivtjenesten

Stilling Rådgiver/arkivleder Anne Kari Grimstad

Organisasjonsenhet

ledelsens stab

3 Er arkivtjenesten samlet i en organisatorisk enhet? **Ja**

4 Hvis nei, hvor mange organisatoriske enheter består den av?

5 Er arkivtjenesten samlet på ett fysisk sted? Ja

6 Hvis nei, hvor mange fysiske enheter består den av?

7 Hvor mange årsverk er det til sammen i arkivtjenesten(e)? 1,5

8 Har noen arkivmedarbeidere andre oppgaver ved siden av arkivarbeidet (eks. resepsjon, sentralbord eller lignende)? Nei

9 Hvor mange årsverk er det til sammen ved høgskolen? **vitenskapelige 200  
administrative 120**

### **B. Instruksjer, regler og planer for arkivarbeidet**

1 Har universitetet/høgskolen en arkivplan? Ja

2 Når ble arkivplanen sist oppdatert? Mai 2011

3 Inneholder arkivplanen oversikt over hvordan arkivet er organisert og eventuell inndeling i arkivdeler? Ja

4 Inneholder arkivplanen en beskrivelse av ansvaret for tildeling og ajourhold av brukerrettigheter til registrerings - og arkiveringsfunksjoner? Ja

5 Inneholder arkivplanen oversikt over hvilke registrerings- og arkiveringsrettigheter som tildeles ledere og saksbehandlere? Ja

6 Inneholder arkivplanen prosedyre for arkivering av e-post? Ja

7 Inneholder arkivplanen rutine - og ansvarsbeskrivelse for kvalitetssikring av den elektroniske arkiveringen? Ja

8 Inneholder arkivplanen rutine - og ansvarsbeskrivelse for Kvalitetssikring ved skanning av papirdokumenter? Ja

9 Inneholder arkivplanen retningslinjer for å verifisere at skannede dokumenter er korrekte og lesbare før papirversjonen kasseres? Ja

10 Inneholder arkivplanen retningslinjer for kassasjon av mottatte Papirdokumenter som er skannet og arkivert elektronisk? Ja

11 Inneholder arkivplanen spesifisering av hvilke(t) arkivformater) som skal brukes? Ja

12 Inneholder arkivplanen prosedyre og ansvar for konvertering av filer til arkivformat? Ja

13 Inneholder arkivplanen en prosedyre for registrering og arkivering når systemet er ute av drift? Ja.

14 Inneholder arkivplanen rutiner som beskriver:

a) Fordeling av dokumenter? Ja

b) Retting av journal- og arkivopplysninger? Ja

c) Avskrivning av dokumenter? Ja

d) Vurdering av spørsmål vedrørende offentlighet? Ja

e) Registrering av unntak fra offentlighet og hjemmel for dette? Ja

f) Etatens policy i fm bruk av sosiale medier? Nei

g) En beskrivelse av hvilke sosiale medier som brukes i saksbehandlingen? Nei

h) En beskrivelse av hva som er eller kan være arkivverdig materiale fra sosiale medier? Nei

i) Hvordan arkivverdig materiale fra sosiale medier skal bevares? Nei  
Kommentarer: Det er bare e-post som er aktuelt pr. mai 2011.

### **C. Sakarkiv**

1 Hvilket sakarkivsystem bruker universitetet/høgskolen?

**Navn, versjon** ePhorte versjon av mai 2011 fra Ergogroup 11.2.02.

2 Når ble det tatt i bruk? 01.01.2006

3 Har universitetet/høgskolen elektronisk arkiv? Ja

4 Inneholder arkivplanen spesifisering av hvilke arkivdeler/sakstyper som lagres elektronisk og hvilke som evt. lagres på papir? Ja

5 Hvor mange arkivdeler består arkivet av? 3 + fysisk på papir

6 liste over arkivdelene:

**Betegnelse Elektronisk Papirbasert Sist periodisert**

- a) Saksarkiv X
- b) Personalarkiv X
- c) Utvalgsarkiv X
- d) Fysisk arkiv X
- e)

7 Avsluttes arkivsakene fortløpende når de er ferdigbehandlet? Ja  
S Hvis nei, finnes leten rutine for nårog hvordan sakene skal Ja  
avsluttes?

9 Inneholder arkivplanen en plan for periodisering og vedlikehold av arkivet inntil det kan avleveres til arkivdepot? Ja

Kommentarer:

**D. Fagsystemer**

1 Benytter universitetet/høgskolen FS (Felles Studentsystem)? Ja

2 Hvis nei på D1, benytter universitetet/høgskolen et annet studentadministrativt system?

3 Hvis ja på D2, hvilket system?

**Navn, versjon**

4 Hvis FS eller et annet studentadministrativt system benyttes:

**Ja**

a) Produseres det arkivdokumenter i systemet som overføres til sakarkivet? Nei

b) Produseres det arkivdokumenter i systemet som lagres både der og i sakarkivet? Ja

c) Produseres det arkivdokumenter i systemet som bare **lagres i** dette systemet? Antakeligvis

d) Hvis ja på D4c), finnes det noen form for journalføringsfunksjon i systemet? Nei

e)

**5 Benytter universitetet/høgskolen en læringsplattform (LearningManagementSystem - LMS)? Ja**

6 Hvis ja på D5, hvilket system?

7 Hvis et LMS benyttes:

**Navn, versjon Klassfronter**

**Ja**

a) Produseres det arkivdokumenter i LMSsom overføres til sakarkivet?

Nei

b) Produseres det arkivdokumenter i LMSsom lagres både **der og** i sakarkivet?

**Nei**

c) Produseres det arkivdokumenter i LMSsom bare **lagres i dette**

systemet? Nei

d) Hvis ja på D7c), finnes det noen form for journalføringsfunksjon i LMS? Nei

8 Hvilke andre fagsystemer benytter universitetet/høgskolen i dag?

**Produserer Arkivdokumenter**

**Navn/betegnelse, versjon**

**arkivdokumenter til sakarkiv**

a) Easycruit Ja

**b) Nexus Nei**

1 Med fagsystem menes spesialiserte systemer for mer eller mindre automatisert saksbehandling og

beslutningsstøtte, hvor det produseres arkivdokumenter eller opplysninger som skal lagres.

Kommentarer:

**E. Easycruit kommuniserer ikke med ePhorte, så dokumenter må overføres manuelt.**

**Dette kan det bli endringer på i nærmeste fremtid .**

Dokumenter og journalposter

1 Hvor mange journalposter registrert pr år de siste 3 årene:

**Inngående Utgående Notater**

**2007** 1510 1402 262

**2008** 1553 1443 880

**2009** 1666 1562 698

2 Interne dokumenter notater):

a) journalføres Alltid

b) arkiveres uten journalføring **Aldri x**

c) arkiveres ikke Alltid 3

Publiseres offentlig journal **på Internett? Ja**

4 Hvis notater journalføres, tas de med i offentlig journal? Ja fra 01.01.11

Kommentarer:

## **F. Bevaring og kassasjon**

1 Finnes det en bevarings- og kassasjonsplan for fagsystemene? Nei

2 Er dere i gang med å lage en bevarings- og kassasjonsplan for fagsystemene? Skal jobbe med en felles for statlige høgskoler

3 Hvis **ja på spørsmål 2**, hvilke fagsystemer?

a) Det arbeides sentralt med retningslinjer for dette. Systemene skal meldes inn til arkivverket.

## **G. Teknisk systemdrift**

1 Utfører universitetet/høgskolen selv den tekniske driften av sakarkivet?

Nei

2 Hvis nei, hvem drifter systemet? Uninett/USIT

3 Foreligger det en tjensteavtale med driftsoperatøren? Antakelig, men ikke pr. dato i arkivet.

4 Hvis ja, er følgende spesifisert i avtalen:

a) Tjenestenivå Ja Nei

b) Sikkerhetsopplegg Ja Nei

c) Sikkerhetskopiering Ja Nei

d) Oppetider for systemet Ja Nei

5 Utfører universitetet/høgskolen selv den tekniske driften av sine fagsystemer?

Nei

6 Hvis nei, hvem drifter systemene?

a) System FS som driftes av UNINETT/USIT

b) System Easycruit Driftes av Stepstone Solutions

c) System NEXUS Driftes av Høgskolen i Lillehammer

d) System Klassfronter driftes av Fronter

#### **H. Eksamensbesvarelser m .m.**

Det vises til Riksarkivarens vedtak om bevaring og kassasjon av eksamensbesvarelser m.m. i universitetssektoren og høgskolene, som ble sendt ut i brev av 13.3.2007, vår ref. 2005/13708 og brev av 03.10.2007, vår ref. 2007/9563.

**1 Følges Riksarkivarens vedtak? Ja**

**2 Hvilken organisasjonsenhet på universitetet/høgskolen har ansvaret for å bevare eksamensbesvarelsene/avhandlingene? Studieadministrasjonen**

**3 Er det etablert elektroniske løsninger for å bevare dette materialet? Ja**

**4 Hvis ja, er systemet/systemene meldt inn til Riksarkivaren? Ja og legges i ePhorte**

## **Vedlegg 3: De mest sentrale arkivtermer for høgskolens bruk:**

### **Arkiv**

1. Dokumenter som blir til som ledd i en virksomhet, dvs dokumenter som mottas eller produseres av en enkelt arkivskaper og samles som resultat av dennes virksomhet (også kalt enkeltarkiv).
2. Oppbevaringssted for aktivt arkiv
3. Organisatorisk enhet som utfører oppgaver knyttet til arkiv, også kalt arkivtjeneste
4. Dss. arkivdepot.

### **Arkivbegrensning**

Å holde utenfor eller fjerne fra arkivet dokumenter som hverken er gjenstand for saksbehandling eller har verdi som dokumentasjon, jf. arkivforskriften § 3-18.

### **Arkivdanning**

Framvekst av enkeltarkiv gjennom arkivskapers virksomhet.

### **Arkivdel**

En vilkårlig definert del av et arkiv (1) hvor alt materiale er inndelt og ordnet etter ett og samme ordningsprinsipp som primærnøkkel. Vil ofte være definert identisk med arkivserie, men behøver ikke være det.

### **Arkivdepot**

Institusjon hvor bevaringsverdig arkivmateriale oppbevares permanent. Arkivdepotet avlaster arkivskaperen for lagring av eldre arkivmateriale og legger forholdene til rette for betjening av brukere som er interessert i materialet.

### **Arkivdokument**

Dokument som mottas eller produseres som ledd i den virksomhet et organ utøver, og som ikke er gjenstand for arkivbegrensning. Se også

Saksdokument.

### **Arkivering**

Arkivskapers håndtering av arkivsaker.

### **Arkivformat**

Åpent dokumentert, standardisert format for elektronisk arkivering (langtidslagring) av dokumenter, godkjent av Riksarkivaren.

### **Arkivkatalog**

Oversikt over innholdet i enkeltarkiv eller samling som er avlevert til depotinstitusjon.

### **Arkivkode**

En enkelt ordningsverdi i en arkivnøkkel. Arkivkoder i en emnebasert arkivnøkkel kalles ofte emnekoder, mens arkivkoder i en objektbasert arkivnøkkel ofte kalles objektkoder. En arkivkode kan være tall, bokstaver, tegn eller en blanding av disse.

### **Arkivlegging**

Plassering av dokumentene i en sak i arkivet etter endt registrering og/eller saksbehandling.

### **Arkivnøkkel**

Klassifikasjonssystem som omfatter alle de saksområder organet steller med, og gir en systematisk fortegnelse over de verdier (arkivkoder) som benyttes ved ordning av saker i et arkiv. Se også Ordningsprinsipp.

### **Arkivorganisering**

1. Organisering av virksomhetens arkiv (1).
2. Organisering av virksomhetens arkivfunksjoner.

### **Arkivperiode**

Tidsperiode for inndeling av arkivet i forbindelse med bl.a. bortsetting.

### **Arkivplan**

Oversikt over produksjon og oppbevaring av arkivmateriale fra en arkivskaper og bestemmelse om hvor og hvordan dette skal finne sted.

### **Arkivserie**

Del av et arkiv (1), inndelt og ordnet etter ett og samme prinsipp.

### **Arkivskaper**

En organisatorisk enhet eller en person som danner arkiv (1) som ledd i sin virksomhet. En arkivskaper kan være et offentlig organ, en bedrift, en organisasjon, en institusjon, en stiftelse etc. eller en del av en slik enhet.

### **Arkivstykke**

Fysisk enhet i et enkeltarkiv, f.eks protokoll, pakke, eske, kassett, rull, magnetbånd o.a.

### **Arkivstyring**

De funksjoner i et arkivsystem som holder oversikt over og styrer tilgangen til alle saksdokumenter med tilknyttede opplysninger.

Tilsvarende engelsk "record-keeping".

### **Arkivsystem**

System som benyttes til å registrere, administrere, oppbevare og gjenfinne dokumentene som inngår i et arkiv, såvel elektronisk som manuelt arkiv. Et arkivsystem inneholder en samling dokumenter, dokumentbeskrivelser og funksjoner for (dokument)vedlikehold, administrasjon, utlån, søking, rapportutskrifter, statistikk m.v.

### **Arkivverdighet**

Den egenskap hos de arkivdokumenter som er kvalifiserte for oppbevaring, at de har eller antas å ha verdi som grunnlag for saksbehandling og dokumentasjon.

### **Avgradering**

Oppheving av gradering fra et bestemt tidspunkt.

### **Avlevering**

Overføring av eldre og avsluttet arkiv til arkivdepot, jf. arkivforskriften § 5-1.

### **Avleveringsformat**

Måten elektronisk tabellinformasjon og dokumenter er strukturert på ved avlevering til depotinstitusjon.

### **Avleveringsliste**

Fortegnelse over arkivsaker som overdras fra en arkivskapende institusjon til depotinstitusjon.

### **Avskrivning**

Registrering av opplysninger i journalen om når og hvordan behandlingen av et inngående dokument har blitt avsluttet.

### **Behandlingsfrist**

Den frist for behandling som mottaker setter på et dokument.

### **Bevaring**

Å ta vare på dokumenter og/eller annen informasjon over tid.

### **Bortsetting**

At arkivmateriale etter en tid (vanligvis etter et bestemt antall år, jf. Arkivperiode) tas ut av aktivt arkiv og settes bort på et dertil egnet sted. Se også Bortsettingsarkiv.

### **Bortsettingsarkiv**

1. Materiale som er satt bort etter de prinsipper som er beskrevet under Bortsetting.

2. Oppbevaringssted for bortsettingsarkiv 1.

### **Bortsettingsliste**

Liste over arkivmateriale som overføres til bortsettingsarkiv.

## **Delarkiv**

Enkeltarkiv skapt av en arkivskaper som er del av en større enhet, for eksempel en eller flere avdelinger i et offentlig organ.

## **Dokument**

Etter arkivloven § 2: ei logisk avgrensa informasjonsmengd som er lagra på eit medium for seinare lesing, lyding, framsyning eller overføring. I Noark-4 er et dokument en logisk avgrenset informasjonsmengde som kan være lagret på papir, elektronisk eller på andre medier. Vanlige eksempler på dokumenter er brev, notater, rundskriv, rapporter, protokoller m.v. Se også Arkivdokument og

## **Saksdokument.**

Dokumentasjon

Funksjon som omfatter lagrings-, gjenfinnings- og distribusjonsmetoder for informasjon fra dokumenter.

## **Dokumentflyt**

Dokumentenes "gang" fra ledd til ledd i en behandlingsprosess.

## **Dokumentformat**

Måten tegn, struktur og layout er kodet og organisert på i et elektronisk dokument.

## **Dokumenthåndtering**

Registrering, lagring, søking, presentasjon, styring og kontroll av dokumenter.

## **Dokumentmal**

Mønster for å sette opp en bestemt type dokument. Malen er utformet som et eget dokument og inneholder de elementer som er felles for alle dokumenter av samme type. Elementene i en dokumentmal kan for

eksempel være tekst og formatering, stiler, makroer, verktøylinjer og menyer. Dokumentmalene skal sørge for at dokumenter av en gitt type får et felles utseende og et standardisert og strukturert innhold.

### **Dokumentnummer**

Nummer som systemet automatisk tildeler den enkelte journalpost når den opprettes. Dokumentnummeret er koblet til saksnummeret som et undernummer, og angir dokumentenes rekkefølge innenfor saken.

### **Dokumentoffentlighet**

Det at et forvaltningsorgans saksdokumenter som hovedregel skal være offentlig tilgjengelige, så fremt det ikke er gjort unntak i lov eller i medhold av lov. Dokumentoffentlighet reguleres av Offentleglova.

### **Elektronisk arkiv**

Arkiv (1) som består av elektroniske dokumenter.

### **Elektronisk dokument**

Et dokument lagret på elektronisk medium og tilrettelagt for gjenfinning, prosessering og kommunikasjon vha. en datamaskin.

### **Elektronisk dokumentlager**

Et lager av dokumenter på elektronisk medium, tilrettelagt for søk og gjenfinning ved hjelp av funksjoner for dokument-håndtering. Elektronisk arkiv er en spesiell variant av elektronisk dokumentlager, undergitt de regler og prinsipper som gjelder for arkiv (1). Elektroniskarkiv kan også inngå som del av et større elektronisk dokumentlager.

### **Elektronisk saksarkiv**

Arkiv (1) som består av elektroniske saksdokumenter.

### **Elektronisk saksbehandling**

Saksbehandling basert på elektronisk dokumentflyt og gjennomgående IT-støtte til organisering og gjennomføring av prosessen fra saken mottas og registreres til den avsluttes.

### **Fast periodeinndeling**

Periodeinndeling som innebærer at alle avsluttede saker i perioden settes bort samtidig.

## **Gradering**

Skjerming av opplysninger mot innsyn etter sikkerhetsinstruksen og beskyttelsesinstruksen.

## **Internt dokument**

Dokument som er utarbeidet for et forvaltningsorgans interne saksforberedelse, enten av organet selv eller av et underliggende organ, av særlige rådgivere eller sakkyndige eller av et departement til bruk i et annet departement.

## **Journal**

System for fortløpende registrering av referanseopplysninger om arkivdokumenter. Denne registreringen knytter enkeltdokumenter til saker, gir grunnlag for saksadministrasjon, arbeidsstyring og praktisering av bestemmelser om partsinnsyn og offentlighet.

## **Journalenhet**

En arkivorganisasjons enhet som fører journal.

## **Journalføring**

Systematisk og fortløpende loggføring av opplysninger om inn- og utgående dokumenter samt interne dokumenter som inngår i saksbehandlingen.

## **Journalperiode**

Tilsvarende Arkivperiode.

## **Kassasjon**

Bestemme hvilket arkivmateriale som skal fjernes fra arkivet, og tilintetgjøre dette.

## **Kassasjonsliste**

Oversikt over hvilket materiale som skal kasseres eller som er kassert.

### **Kassasjonsplan**

Oversikt over hvilke regler som gjelder for kassasjon i en virksomhet; hva slags arkivmateriale som kan kasseres, når dette kan skje og på hvilken måte.

### **Klageadgang**

Den alminnelige rett som part(er) i sak, eller andre med rettslig interesse i saken har til å bringe en sak inn for et høyere organ enn det som har fattet vedtaket. Den generelle klageadgangen er hjemlet i forvaltningsloven.

### **Klassere**

Påføre et saksdokument én eller flere dekkende arkivkoder eller ordningsverdier fra klassifikasjonssystemet (arkivnøkkelen).

### **Kobling**

Sammenknytning av enkeltsaker ved noteringer på dokumentene og i eventuell journal (tilsvarende lenking).

### **Konsept**

Dokumentutkast.

### **Kopibok**

Samling av kopier av utgående korrespondanse.

### **Kopimottaker**

Mottaker som mottar kopi(er) av dokumentet, og dermed ikke er behandlingsansvarlig.

### **Krysshenvisning**

Toveis forbindelse mellom punkter i arkivnøkkelen som delvis kan dekke samme emne, men som likevel må holdes atskilt.

### **Meroffentlighet**

Prinsipp som sier at et forvaltningsorgan skal vurdere om et dokument kan gjøres kjent, helt eller delvis, selv om det etter offentlighetslovens bestemmelser er adgang til å unnta det fra offentlighet.

### **Møteprotokoll**

Referat (protokoll) fra et bestemt møte i et utvalg. Omfatter opplysninger om tid, sted, frammøte o. l. samt saksprotokoller for alle saker som ble behandlet i møtet. Jf. møtebok i kommuneloven.

### **Obs-dato**

En dato for saksoppfølging som saksbehandler eller leder selv setter for å få hele saken overbragt fra arkivet, ev som saksbehandler/leder selv legger inn i og søker fram fra systemet.

### **Obs-liste**

Liste som skal gjøre arkivpersonalet oppmerksom på de saker som skal bringes fram for saksbehandler på et gitt tidspunkt (obs-dato).

### **Offentlig journal**

En kopi av journalen med allmennheten som målgruppe, hvor opplysninger unntatt offentlighet er strøket ut.

### **Offentlig versjon av dokument**

En versjon av et dokument unntatt offentlighet, hvor alle sensitive opplysninger er avskjermet/strøket slik at dokumentet kan offentliggjøres.

### **Ordning**

Inndeling av av arkivdokumenter i grupper, fastsettelse av rekkefølgen av gruppene og rekkefølgen av arkivdokumentene innenfor gruppene.

### **Ordningsprinsipp**

Prinsipp for rekkeordning av arkivmateriale.

### **Organinternt dokument**

Dokument som et forvaltningsorgan har utarbeidet for sin interne saksforberedelse.

### **Overføringsliste**

Oversikt over arkivmateriale som er overført fra et offentlig organ til et annet, jf. pålegg etter arkivforskriften § 3-22. Se også Avleveringsliste.

### **Overlappingsperiode**

Overgangsfase mellom gammel og ny arkivperiode, oftest de to første årene av hver ny arkivperiode.

### **Part**

Person eller virksomhet som berøres av avgjørelsen i en sak.

### **Periodisering**

Sette et kontrollert tidsskille i arkivet med jevne mellomrom. Dette innebærer at alle saker med dokumenter som har vært registrert innefor et fast tidsrom (en arkivperiode) settes bort samtidig, og utgjør en egen enhet i bortsetningsarkivet.

### **Postjournal**

Se Journal.

### **Postliste**

En samlet oversikt over de saksdokumenter som er kommet inn til eller lagt frem for et organ, dvs mottatte saksdokumenter.

### **Presedens**

Prinsipielt viktig avgjørelse som er regeldannende for behandling av likeartede saker.

### **Primærkode**

Den primære arkivkode som som en sak klasseres etter.

### **Proveniensprinsippet**

Grunnregel som tilsier oppbevaring av arkiv i sin opprinnelige ordning.

### **Referatsak**

Dokument som blir lagt fram for et utvalg til orientering.

### **Register**

Fortegnelse over enheter som f.eks navn og emner, innført etter ett prinsipp og i regelen rekkeordnet systematisk.

### **Rensing**

Utsortering og fjerning av arkivverdige materiale fra dokumentene i en sak før arkivlegging.

### **Sak**

1. Abstrakt: Et spørsmål som er til behandling, på grunnlag av en henvendelse utenfra eller på initiativ fra organet selv (jf forvaltningsloven og offentlighetsloven). Begrepet benyttes også om selve behandlingsforløpet.

2. Konkret: En sak omfatter de saksdokumenter, registreringer, påskrifter etc. som oppstår og/eller inngår i behandlingsforløpet.

### **Saksansvarlig**

Saksbehandler som er ansvarlig for behandling av saken som helhet. Se også Saksbehandler.

### **Saksansvarlig enhet**

Den administrative enhet hvor saksansvaret ligger. Se også Saksbehandler enhet.

### **Saksarkiv**

Den delen av arkivet som består av saksdokumenter.

### **Saksbehandler enhet**

Den administrative enhet hvor saksbehandlingsansvaret for ett eller flere av dokumentene i en sak ligger. Se også Saksansvarlig enhet.

### **Saksbehandler**

Den person i organet som er ansvarlig for oppfølging og behandling av ett eller flere dokumenter i en sak. Se også Saksansvarlig.

### **Saksbehandling**

Vurdering av informasjon knyttet til en intern eller ekstern problemstilling med sikte på **at det** skal fattes en beslutning eller et vedtak. I offentlig saksbehandling vil beslutningen eller vedtaket ofte gi rettsvirkning for en eller flere fysiske eller juridiske personer.

### **Saksbehandlingssystem**

IT-system for elektronisk saksbehandling (Ved HiL ePhorte).

### **Saksdel**

Undergrupper av journalposter innenfor en sak.

## **Saksdokument**

Etter offentlighetsloven er forvaltningens saksdokumenter dokumenter som er utferdiget av et forvaltningsorgan, og dokumenter som er kommet inn til eller lagt frem for et slikt organ. I arkivsammenheng brukes begrepet i hovedsak på samme måte. Møteprotokoller samt registre og databaser regnes som arkivdokumenter (se dette), men vanligvis ikke som saksdokumenter, jf. arkivforskriften § 2-4.

## **Saksgang**

Behandlingssekvens for en sak. Omfatter de trinn eller faser som en sak følger fra den oppstår til den er avsluttet.

## **Saksnummer**

Unikt identifikasjonsnummer som systemet automatisk tildeler den enkelte sak når den opprettes, og som følger saken uendret så lenge den eksisterer.

## **Saksopplysninger**

Opplysninger som er felles for alle dokumenter i en sak.

## **Sakstype**

Kategori for å angi hvordan en sak skal behandles. Sakstypen kan knyttes til en eller flere relaterte prosedyrer eller aktiviteter som skal utføres ved behandling av saken.

## **Sekundærkode**

Arkivkode som angir sekundær underoppdeling av primærkoden.

## **Sentralisert arkiv**

Arkiv samlet under én sentral, faglig ledelse.

## **Skarpt periodeskille**

Absolutt periodeskille i arkiv og journal, hvor utskilling og bortsetting foretas straks en periode er avsluttet.

## **Virksomhet**

1. Aktiviteter i et offentlig organ, en organisasjon, bedrift, institusjon etc. eller hos en person.
2. Et offentlig organ, en organisasjon, bedrift, institusjon eller lignende, eller en del av en slik enhet.

## Vedlegg 4 Grunnkurs for saksbehandling i ePhorte

### Innholdsoversikt

#### **1 SENTRALE BEGREP I EPHORTE 2**

- 1.1 Noark - 4.1 4
- 1.2 Sak (saksmapper)
- 1.3 Journalpost
- 1.4 Dokument
- 1.5 Journalføring (registrering)
- 1.6 Arkivdeler
- 1.7 Klassering
- 1.8 Journalenhet
- 1.9 Administrativ inndeling HiL
- 1.10 Roller
- 1.11 Tilgangskoder
- 1.12 Tilgangsgrupper
- 1.13 Restanse
- 1.14 Avskrivning
- 1.15 Dokumenttyper
- 1.16 Saksframlegg / protokoll / referat
- 1.17 Dokumentflyt (skisse)
- 1.18 Prosesstyring
  - 1.18.1 Statuskoder – sak
  - 1.18.2 Statuskoder – journalpost (JP)
  - 1.18.3 Statuskoder – dokument
  - 1.18.4 Lese- og skriverettigheter

#### **2 KOMME I GANG I EPHORTE 6**

- 2.1 Oppstart og pålogging
  - 2.1.1 Produksjonsbasen
  - 2.1.2 Fungereing for en annen person
  - 2.1.3 Kursbasen
- 2.2 Skjermbildet
  - 2.2.1 Venstremenyen
  - 2.2.2 Verktøylinjen
  - 2.2.3 Øvre høyre skjermbilde
  - 2.2.4 Nedre høyre skjermbilde
- 2.3 Ikoner
- 2.4 Status på saker, journalposter (JP) og dokumenter

#### **3 BRUKERVEILEDNING 9**

- 3.1 Sak
  - 3.1.1 Opprette ny sak
    - 3.1.1.1 Klassering
    - 3.1.1.2 Tilgangskode/-gruppe
    - 3.1.1.3 Fast tilgangsgruppe
    - 3.1.1.4 Ad-hoc tilgangsgruppe
  - 3.1.2 Redigere saksopplysningene
  - 3.1.3 Merknad på saksmappe
  - 3.1.4 Melde sak som ferdigbehandlet
  - 3.1.5 Slette saksmappe
- 3.2 Journalpost / dokument
  - 3.2.1 Opprette ny journalpost og dokument
  - 3.2.2 Legge inn adressater som allerede er mottakere/avsendere i saken
  - 3.2.3 Flett på nytt
  - 3.2.4 Sende til godkjenning
  - 3.2.5 Endring i ferdigstilte notater med interne mottakere?

- 3.2.6 Sende ut utgående brev
  - 3.2.7 Redigere journalpostopplysninger
  - 3.2.8 Endre status på journalpost
  - 3.2.9 Redigere et dokument
  - 3.2.10 Legge vedlegg til et hoveddokument
    - 3.2.10.1 Nytt vedlegg
    - 3.2.10.2 Sette inn vedlegg fra annen (eksisterende) post
  - 3.3 Søk etter saker / Journalposter
    - 3.3.1 Venstremenyen
      - 3.3.2 Søk etter sak, journalpost eller dokument
        - 3.3.2.1 Finne en sak
        - 3.3.2.2 Finne en journalpost eller et dokument
  - 3.4 Behandling (avskrivning) av mottatt post som krever svar / behandling (restanser)
  - 3.5 E-post
- Registrere mottatt e-post  
ePhorte versjon 2.1.15.07

## 1 Sentrale begrep i ePhorte

### 1.1 Noark - 4.1

NORsk ARKivsystem - versjon nr. 4.1 er gjeldende standard for journalføring og arkivering i offentlige organ. ePhorte dekker kravene i standarden og en rekke av de anbefalinger som er fremsatt. ePhorte er godkjent og tilrettelagt for elektronisk arkivering.

### 1.2 Sak (saksmapper)

En sak består av en eller flere journalposter med tilhørende dokumenter som logisk hører sammen, og som er lenket sammen under en felles identitet (saksnummer – eks.: 2006/876).

### 1.3 Journalpost

Journalpost (JP) betyr beskrivelse / referanseopplysninger av ett eller flere dokumenter som inngår i en felles forsendelse/ekspedisjon.

### 1.4 Dokument

Et dokument er en avgrenset og sammenhengende informasjonsmengde, framstilt for et bestemt formål.

En journalpost har alltid ett hoveddokument. Det kan også være knyttet ett eller flere vedlegg til journalposten.

Et hoveddokument kan også ha flere versjoner.

Eks.: En journalpost med hoveddokument og ett vedlegg

### Sak – Journalpost – Dokument

### 1.5 Journalføring (registrering)

Journalføring betyr en systematisk og fortløpende loggføring av arkiververdige opplysninger om:

- innkommende dokumenter
- utgående dokumenter
- interne dokumenter

som inngår i saksbehandlingen

**Husk at ved elektronisk arkivering utvides registreringsbehovet i forhold til tidligere tradisjonelle papirarkiv. Alle dokumenter som er nødvendige for å dokumentere saksbehandlingen skal derfor registreres.**

### 1.6 Arkivdeler

En arkivdel i ePhorte er en logisk del av et arkiv hvor saksmappene i arkivdelen er ordnet / klassert med primærkode fra ett og samme ordningsprinsipp. Arkivet ved HiL er delt opp i tre elektroniske arkivdeler som angir logisk arkivering av sakene.

Arkivdel Kode Forklaring

- Saksarkiv for HiL
- Personalarkiv for HiL – saker som gjelder den enkelte tilsatte

- UTVALG – for utvalg som utarbeider saksframlegg

### 1.7 Klassering

Hver arkivdel er ordnet etter ett og samme ordningsprinsipp. Ett ordningsprinsipp kan være arkivnøkkel, og ordningsverdi kan være arkivkoden (her: 041.1). Det er laget en felles arkivnøkkel for statlige høyskoler med tilhørende kassasjonsplan.

Ordningsprinsipp Arkivdel

Arkivnøkkel: Primærkode for SAK

Fødselsnummer: PERS Sekundærkode for P

Det opprettes en sak for hver ansatt – en elektronisk personalmappe

### 1.8 Journalenhet

En journalenhet er en arkivorganisatorisk enhet som har ansvar for journalføring av dokumenter tilhørende en eller flere arkivdeler. Arkivfunksjonen ved HiL er sentralisert, og HiL har kun en journalenhet:

Sentral journalenhet for Høgskolen i Lillehammer

### 1.9 Administrativ inndeling HiL

Administrative enheter reflekterer høgskolens organisasjonsstruktur. Hver bruker er knyttet til en administrativ enhet. Alle saker og journalposter må påføres en administrativ enhet.

ePhorte ved HiL er delt inn i følgende administrative enheter:

- HIL Høgskolen i Lillehammer

Ledelsen ved HiL

Ledelsens stab

ARKIV Sentral arkivfunksjon

Seksjon for studieseksjonen

Seksjon for økonomisaker og drift

Seksjon for personal- og organisasjon

Biblioteket

IT-tjenesten

AHS Avdeling for helse og sosialfag

ØKORG Avdeling for økonomi- og organisasjonsfag

HIS Avdeling for idrett og humaniora

TVF Avdeling for TV-utdanning

DNF Den norske filmskolen

I tillegg kommer en "enhet" som kalles Ufordelt. Den brukes til saker / journalposter som ikke er fordelt til en enhet eller som er fordelt feil og enheten har returnert saken / journalposten til arkivet.

Fellesadministrasjonen (FA) er ingen enhet i ePhorte.

Avdelingene er ikke inndelt i institutter

### 1.10 Roller

I ePhorte har alle brukere minst én rolle, som sammen med tilgangskoder og -grupper styrer hva de får lov til å gjøre.

SB: De fleste ePhorte-brukere har rollen saksbehandler

LD: Lederne for de administrative enhetene er saksfordelere.

AN: For eksempel hovedtillitsvalgte med kun lesetilgang

### 1.11 Tilgangskoder

Alle som har tilgang til ePhorte har innsyn i alle dokumenter som ikke er skjermet for innsyn.

Tilgangskoder angir om en sak, journalpost eller dokument skal skjermes for innsyn. Titler kan også skjermes.

Ved HiL er følgende tilgangskoder i bruk:

Kode Forklaring

U Unntatt offentlighet (skjerner i hovedsak mot eksternt innsyn)

P Personalsaker (påføres personalmapper og dokumenter som inneholder personopplysninger om tilsatte ved HiL.

PX Sensitive personopplysninger - personal (tittel og avsender/mottaker blir automatisk skjermet)

### 1.12 Tilgangsgrupper

Tilgangsgrupper kan opprettes innen en administrativ enhet eller på tvers av administrative enheter.

De benyttes for

- å gi andre lesetilgang til skjermet informasjon
  - å gi andre saksbehandlere anledning til å opprette nye journalposter i saken
  - å gi andre saksbehandlere skriverettigheter til tekstdokumenter som er tilknyttet JP
- Faste tilgangsgrupper opprettes av arkivet, og kan gjenbrukes på saker og journalposter.  
Ad-hoc tilgangsgrupper opprettes av saksbehandler, og gjelder kun for den saken/journalposten hvor den blir opprettet.

#### 1.13 Restanse

Når saksbehandler mottar et dokument – et inngående brev eller et N-notat som krever oppfølging - kalles dette en restanse.

Dette vises med rødt flagg for den som har restansen. For andre enn mottaker er dette flagget blått. En restanse oppheves ved å avskrive dokumentet (se neste punkt).

Rolle Kode

Systemansvarlig SY

Arkivleder AR1

Arkivar AR2

Saksbehandler SB

Leder/saksfordeler LD

Utvalgsekretær US

Andre AN

#### 1.14 Avskriving

Et mottatt dokument (dokumenttype I eller N) kan avskrives ved

- at det blir opprettet et svardokument (utgående brev eller notat) (kode BU eller NN)
- at dokumentet avskrives direkte med kode (TE/TO/TLF)
- at alle poster avskrives og saken avsluttes (SA)

I ePhorte kan følgende avskrivingsmåter/-koder benyttes:

Avskrivning Kode Merknader

Midlertidig svar \*\*\*

Brev Ut BU

Nytt Notat NN

Til Etterretning TE + eventuelle merknader

Til Orientering TO + eventuelle merknader

Besvart pr. telefon TLF + eventuelle merknader

Saken Avsluttet SA (settes til F av saksbehandler)

#### 1.15 Dokumenttyper

I ePhorte er det følgende hovedkategorier av dokumenttyper:

Kode Forklaring

I

Eksternt innkomne brev, e-poster til HiL (mottaker får rødt flagg )

N

Notater som blir en restanse hos mottaker (mottaker får rødt flagg )

X

Notater som ikke blir en restanse hos mottaker. Kun til orientering

U

Utgående brev fra HiL. Bruk IKKE denne dokumenttypen når du skal sende notat til en annen

ePhorte-bruker ved HiL Y

Mappedokument – ikke arkivverdig og mest aktuell som et arbeidsdokument.

.

Dokumenttype velges når JP opprettes.

For andre enn mottaker vises dette som et blått flagg

7 Dersom du bruker dokumenttype U - Utgående brev - når du skal sende interne notater i ePhorte, kommer dette ikke fram til intern mottaker i ePhorte. Dokumenttype U skal undertegnes, printes ut og sendes ut av huset for eksempel pr. post.

#### 1.16 Saksframlegg / protokoll / referat

Utvalgsmodulen i ePhorte brukes i noen grad ved HiL, og følgende dokumenttype og mal brukes i saksframlegg:

1 Opprett ny journalpost og velg Nytt saksframlegg (S)

2. Fyll ut journalpostopplysningene og velg Lagre og nytt dokument.

### 3. Velg ønsket mal:

- Møte – saksframlegg
- Møteinnkalling
- Møtereferat

1.17 Dokumentflyt. HiL har ikke denne modulen.

### 1.18 Prosesstyring

Ved hjelp av statusbegrepet kan behandlingsprosessen styres. Det opereres med tre nivåer:

1. Saksstatus (angir status for arkivering og saksbehandling av en sak)
2. Journalpoststatus (angir hvor langt en JP er kommet i forhold til registrering og arkivering)
3. Dokumentstatus (angir om dokumentet er under behandling eller er ferdig)

#### 1.18.1 Statuskoder – sak

Kode Forklaring

R Saksnummer er reservert. Saksbehandler har opprettet saken (må ikke gjøres før dokumenter er klare for å legges inn!)

B Saken er under behandling. Arkivet har opprettet saken eller har kontrollert en sak med status R

F Saken skal avsluttes. Saksbehandler signaliserer at saken skal avsluttes

A Saken er avsluttet. Kun arkiv kan endre status til A

U Saken utgår Som over

#### 1.18.2 Statuskoder – journalpost (JP)

Kode Forklaring Kan endres av:

R - Reservert

Når saksbehandler oppretter en JP med et utgående dokument eller internt notat, settes status til R.

S - Registrert av saksbehandler

Når saksbehandler oppretter en JP med ett inngående dokument eller laster ned en e-post, settes status til S.

G - Til godkjenning

Når JP sendes til godkjenning får den status G.

Hvis den godkjennes, vil status automatisk settes til F. Hvis den ikke godkjennes, men returneres til saksbehandler, settes status tilbake til R. Det bør da settes på en merknad fra leder.

Saksbehandler

Leder

F - Ferdig Når JP er ferdig, men ikke ekspedert. Saksbehandler kan endre tilbake til R eller til E.

E – Ekspedert via e-post

Når JP er ekspedert (utgående brev er printet ut og sendt i posten) skal saksbehandler sette status til F.

Alle journalposter for utgående brev skal settes til ferdig etter at de er sendt enten det har skjedd i ePhorte, på papir eller vha. send kopi med e-post.

Interne notat journalføres når de er ferdigstilt.

J - Journalført

Når saksbehandler har satt status til F, kontrollerer arkivet og setter status til J. Det kalles journalføring.

JP og tilhørende dokument er låst for endring.

Dokumentet konverteres automatisk til arkivformat (PDF).

U - Utgått Når journalposten ønskes slettet eller fjernet, kan status settes til U.

#### 1.18.3 Statuskoder – dokument

Kode Forklaring Kan endres av:

B Dokumentet er under behandling

Saksbehandler/arkiv

F Dokumentet er ferdig fra saksbehandler  
Saksbehandler/arkiv

#### 1.18.4 Lese- og skriverettigheter

Leserettigheter er en brukers rettighet til å gjenfinne og lese informasjon. Det styres via tilgangskoder, tilgangsgrupper og brukerens autorisering for ulike tilgangskoder

Skriverettigheter er en brukers rettighet til å opprette saker, å opprette journalposter og dokumenter, å endre informasjon og opprette/skrive dokumenter. Det styres via roller, tilgangskoder/-grupper og status (saker/journalposter/dokumenter).

Alle ePhorte-brukere har i utgangspunktet lesetilgang til saksmapper og journalposter som ikke er påført en tilgangskode.

Det betyr at alle brukere har lesetilgang til offentlige saker, journalposter og dokumenter.

## 2 Komme i gang i ePhorte

### 2.1 Oppstart og pålogging

#### 2.1.1 Produksjonsbasen

Gå til: <https://hig/ephorte.uninett.no/>

Alternativ 1: **Start – Administrative programmer – ePhorte prod**

1) Skriv inn **brukernavn og passord**. Klikk på

(Kontrollér at riktig organisasjon er påført – Høgskolen i Lillehammer)

2) Du kan endre rolle ved å trykke på "pilen" (de fleste har kun en rolle), og trykk OK.

Du er nå inne som ePhorte-bruker og kan begynne å arbeide i ePhorte.

#### 2.1.2 Fungering for en annen person

Skal du fungere for en annen person, innebærer dette at du kan logge deg på som den personen du skal fungere for. Arkivet må ha melding om denne fungeringen i god tid før fungeringsperioden skal inntreffe.

Du vil få samme skrive- og leserettigheter som den du fungerer for, men alle endringer du gjør i saksmapper og journalposter vil avspeiles i logg.

1 Skriv inn (eget) **brukernavn og passord**. Klikk på

2 Hent frem rollen: **Fungering for .....**

#### 2.1.3 Kursbasen

Påloggingen som ved pålogging på produksjonsbasen, men velg ePhorte Kurs (ikke ePhorte Prod).

### 2.2 Skjermbildet

Skjermbildet i ePhorte er oppdelt i flere "deler": Venstremenyen, verktøylinjen og øvre og nedre skjermbilde.

#### 2.2.1 Venstremenyen

I menyen lengst til venstre i skjermbildet finner du Venstremenyen. Her ligger bl.a. Fellessøk som er tilgjengelig for alle ePhorte-brukere. Dette er forhåndsdefinerte søk der du som saksbehandler finner det du trenger mest.

(Rekkefølgen på søkene kan endre seg over tid)

Ønsker du spesielle søk tilrettelagt for deg?: Ta kontakt med arkivtjenesten på [postmottak@hil.no](mailto:postmottak@hil.no)

Restanser: Dokumenter du ikke har besvart eller tatt til etterretning/orientering.

Forfallsliste inngående: Viser dine journalposter med svarfrist 14 dager framover, og de som har forfalt.

Forfallsliste utgående: Viser dine utgående brev du ønsker å følge opp (har satt svarfrist)

Post til orientering: Viser journalposter som er sendt deg til orientering - jnr.ført siste 30 dager.

Dokumenter under arbeid: Viser dine journalposter som ikke er ferdigstilt (status R).

Sendt til godkjenning: Viser dokumenter som du har sendt til godkjenning, men som enda ikke er behandlet.

Dokumenter som er godkjent: Viser dine notater som er godkjent og/eller ferdigstilt og utgående brev som er godkjent/ferdigstilt, men som ikke er ekspedert (status F)

Utgående brev – ikke ekspedert: Viser dine utgående brev som er under arbeid (R), ferdige eller godkjent av leder (status F), men som ikke er ekspedert (status E).

Besvarte journalposter: Viser dine besvarte journalposter - datert siste 30 dager.

Sendte journalposter: Viser journalposter du har sendt fra deg - datert siste 30 dager.

Saker – under behandling: Viser saker du er saksansvarlig for og som ikke er avsluttet.

Saker – ferdige/avsluttet: Viser saker du er saksansvarlig for og som er ferdige/avsluttet.

Dokumenter som ikke er sjekket inn: Viser dine dokumenter som ikke er lagt tilbake i ePhorte. Ligger kun på ditt "hjemmeområde". SJEKK INN!  
Utgåtte journalposter: Viser dine journalposter som du har satt til utgått – siste 30 dager  
Siste saker: Viser de 10 siste sakene du har sett på.

### 2.2.2 Verktøylinjen

Verktøylinjen er fast for alle skjermbilder i ePhorte.  
Følgende valg er tilgjengelige:

### 2.2.3 Øvre høyre skjermbilde

Øvre skjermbilde brukes til å angi søkekriterier og se på resultatene av et søk

Logg på. Husk å **logge av** ePhorte når du er ferdig.  
Ny saksmappe - opprette ny sak der det ikke finnes fra før.  
Søkefunksjon - søketype angitt i rullegardinsmenyen vil startes.  
Send lenke til saksmappe eller journalpost via e-post til annen saksbehandler. (Når det for eksempel er "kjekt å vite"). Dette blir ikke logget.  
(Mottaker må være pålogget ePhorte for å kunne gå inn på lenken.)  
Skift vindu – skift mellom å se søkeresultatet eller detaljer om en post i søkeresultatet  
Hjelpfunksjon – åpner hjelpfunksjonen  
ePhorte versjon 2.1.15.07

### 2.2.4 Nedre høyre skjermbilde

Nedre høyre skjermbilde brukes til å vise og redigere detaljer om en registrering.  
Legg også merke til den såkalte brøds-mulestien i skjermbildene: den hjelper deg til å navigere i systemet.

## 2.3 Ikoner

"Pil ned"

Betyr alltid at det ligger en meny en kan få frem ved å klikke på pilen.

Saksmappe

En sak kan bestå av en eller flere journalposter med tilhørende dokumenter. Alle saker har et unikt saksnummer.

Journalpost

Beskrivelse av et dokument med eventuelle vedlegg – tittel, avsender / mottaker, dokumentdato etc. (metadata).

Dokument

En journalpost kan ha et eller flere dokumenter knyttet til seg, i ulike lagringsformater.

Et dokument kan være hoveddokument i en journalpost, og vedlegg i en eller flere andre journalposter.

## 2.4 Status på saker, journalposter (JP) og dokumenter

Ved hjelp av statusbegrepet kan behandlingsprosessen styres. Det opereres med tre nivåer:

4. Saksstatus Angir status for arkivering og saksbehandling av en sak

5. Journalpoststatus Angir hvor langt en JP er kommet i forhold til registrering og arkivering

6. Dokumentstatus Angir om dokumentet er under behandling eller er ferdig

1 Status for saker

En sak har status etter hvor den er i behandlingsprosessen:

R - Reservert

B - Under behandling

F - Ferdig

A - Avsluttet

En sak som er opprettet av saksbehandler (SB) får status R. Så lenge saken står i status R, kan SB endre saksopplysninger. Når en SB regner en sak for ferdig, kan saken settes til status F. Arkivet vil da kvalitetssikre saken og avslutte den.

3 Status for dokumenter

Viser hvor langt saksbehandler har kommet i produksjon av dokumentet.

B – Under behandling

F – Ferdig

2 Status for journalposter

Journalposten har status etter hvor langt en har kommet med den enkelte posten.

R – Reservert

E – Ekspedert

F – Ferdig

G – Til godkjenning  
J - Journalført  
S – Registrert av saksbehandler  
U - utgått  
En journalpost som venter på leders godkjenning har status G inntil lederen har godkjent. Den går da over til å få status F.

## 3 Brukerveiledning

### 3.1 Sak

#### 3.1.1 Opprette ny sak

Rutine for oppretting av saker ligger i ePhorte på sak 2006/1 – ePhorte Rutine 6.

For å opprette ny sak, **klikk på** på verktøylinjen.

Du får opp dialogboks hvor saken skal "beskrives":

Felter som må fylles inn er:

**Tittel:** **Beskrivende** tittel i ePhorte

Felt som kan fylles inn er:

**Arkivdel:** Arkivdelen SAK kommer automatisk opp.

**Prosjekt:** For større sakskompleks kan det være behov for å danne en overbygning i form av en prosjektkode som binder saksmappene sammen.

Arkivet oppretter prosjektkoden etter beskjed fra saksansvarlig

Via fanene i dialogboksen er det mulig å påføre:

##### 3.1.1.1 Klassering (gjøres av arkivet)

Klassering av en sak innebærer at en registrerer en arkivkode som kan brukes for å søke etter saker som omhandler samme emne eller objekt.

Klassering av en sak påføres ved å "hente frem" fanen Klassering.

Prinsippet Arkivnøkkel kommer opp automatisk, og ordningsverdi (arkivkode) kan settes eller hentes inn.

Husk også å huke av for UOFF

På personalmapper påføres **arkivkode 221** (personalmapper) + **fødselsnummer, navn + huke av for UOFF**, jf.

##### 3.1.1.2 Tilgangskode/-gruppe

Dersom du skal skjerme tekst i tittel, må du ha påført en tilgangskode. Husk at du alltid må ha en hjemmel for å kunne unnta fra offentlighet.

Gå til fanen Ansvarlig/tilgang:

**Søk opp ønsket tilgangskode**

v.h.a. "forstørrelsesglasset".

Hjemmel til valgt tilgangskode legger seg automatisk inn

##### 3.1.1.3 Fast tilgangsgruppe

Du kan påføre faste tilgangsgrupper (er opprettet av arkivet) når du oppretter en sak. Må søkes opp.

Dersom medlemmene av en slik gruppe har fått skrive tilgang, kan de opprette nye dokumenter i saken uten å ha vært mottaker eller kopimottaker av dokumenter i saken.

Fast tilgangsgruppe kan også overføres til samtlige dokumenter i saken v.h.a. funksjonen:

Overfør tilgangsgruppe til journalposter. Dette vil da medføre tilgang til samtlige dokumenter som er opprettet og som vil bli opprettet i saken.

Dersom tilgangsgruppe allerede er lagt inn, og du ønsker å legge til flere medlemmer, velger du Funksjoner – Tilgangsgruppe - Rediger tilgangsgruppe.

Dersom du ønsker å påføre en ad-hoc gruppe, se beskrivelse under.

Når du har påført nødvendig saksopplysninger – LAGRE

##### 3.1.1.4 Ad-hoc tilgangsgruppe

Ønsker du å påføre en tilgangskode som gjelder kun for denne saken?

Stå på saksnivå - velg Funksjoner - Tilgangsgruppe - Lag tilgangsgruppe

Husk å huke av for skrive tilgang hvis du ønsker at gruppen skal få anledning til å skrive nye dokumenter i saken.

### 3.1.2 Redigere saksopplysningene

Så lenge saken har status R (Reservert) kan saksbehandler korrigere/endre saksopplysningene.

Stå på saksnivå og velg Rediger

Dersom saken har fått status B (Under behandling), må arkivet kontaktes for redigering av saksopplysningene.

### 3.1.3 Merknad på saksmappe

Merknad på saksnivå erstatter de tradisjonelle påtegningene som ble gjort på saksmappen/-omslaget.

Du kan registrere flere merknader på en mappe.

Gå til fanen Merknader og velg Ny merknad fra hurtigmenyen.

Skriv inn teksten. **Lagre**.

Eventuelt:

Stå på saksnivå og velg Ny merknad.

### 3.1.4 Melde sak som ferdigbehandlet

Saksbehandler kan gi beskjed om at en saksmappe kan lukkes (avsluttes) til arkivet ved å velge

Marker som ferdig fra hurtigmenyen på saksnivå

Husk da at saken avsluttes, og at ingen nye dokumenter kan legges inn i saken.

### 3.1.5 Slette saksmappe

Det er kun arkivet som kan "slette" saksmapper, d.v.s. sette saksstatus til U – Utgått.

Sletting forutsetter at saken ikke inneholder journalposter som er journalført eller arkivert.

## 3.2 Journalpost / dokument

### 3.2.1 Opprette ny journalpost og dokument

Rutine for oppretting av utgående brev og interne notat ligger i ePhorte på sak 2006/1 – ePhorte Rutine 7 + 8.

Stå på saksnivå i nederste skjermbilde

Velg Ny journalpost og velg dokumenttype (I, U, N, X).

I: Inngående brev eller e-post som du laster ned og legger inn elektronisk (arkivet skanner ev.)

U: Utgående brev

N: Notat som gir mottaker restanse

X: Notat som er til orientering eller et saksframlegg, innkalling eller referat

Eller:

Stå på journalpostnivå (fanen Journalposter)

Klikk på den blå pilen ved siden av "konvolutten"

Velg dokumenttype (I, U, N, X)

Du har følgende valg (ved HiL) av dokumenttyper:

- Ny inngående (I)
- Ny utgående (U)
- Nytt notat (N) – internt notat som mottaker skal besvare eller avskrives, d.v.s. notatet gir mottaker en restanse
- Nytt notat (X) – internt notat som ikke skal besvares
- Nytt mappedokument – dokument som du vil ha liggende på saken, men som ikke er et saksdokument (ikke arkivverdig)

Ny utgående e-post kan ikke brukes ved HiT da e-postsystemet ikke er integrert med ePhorte!

Skal du ekspedere med e-post må du ferdigstille dokumentet og bruke Send kopi med e-post.

Når du har valgt et alternativ, får du opp et skjermbilde hvor du skal beskrive journalposten. Eks. under er et utgående brev:

Felter som må fylles inn er:

1. **Innhold:** Beskrivende tittel på dokumentet du skal skrive
2. På utgående brev må **ekstern mottaker** fylles inn (kan også påføre flere mottakere).
3. På interne notat type N må **intern mottaker** fylles inn.

Felter som kan fylles inn er:

- Forfallsdato: Husk at dersom du ønsker å påføre svarfrist, må dette påføres i journalpostopplysningene. Det er ikke tilstrekkelig å nevne dette kun i brevet/notatet.
- Tilgangskode (dersom journalpostopplysningene eller selve dokumentet skal unntas fra offentlighet)
- Tilgangsgruppe (dersom du f.eks. ønsker at flere enn deg skal ha skrive-tilgang til saken. D.v.s. at andre kan skrive i saken selv om de ikke er mottakere eller kopimottakere av dokumenter i saken).
- Kopimottaker(e)

Feltet Godkjennes av skal ikke fylles ut ved oppretting av journalposten.

Dette feltet blir automatisk fylt ut når du har utarbeidet dokumentet, og velger Til godkjenning + Godkjennes av ..... i stedet for Marker dokument som ferdig.

### 3.2.2 Legge inn adressater som allerede er mottakere/avsendere i saken

Du kan benytte navn og adresser som allerede ligger i saken på følgende måte:

:

Når du oppretter JP'en, går du til fanen Mottakere og gjør et oppslag v.h.a. "forstørrelsesglasset".

I dialogboksen som vises, velger du

Velg de du vil benytte

Legg til valgte rader

Lagre

Ønsker du å benytte adresser som ligger i høgskolens adresseregister, velger du istedenfor Adressater i sak.

jf. punktet over.

### 3.2.3 Flett på nytt

Dersom du setter opp nye mottakere eller kopimottakere ved redigeringen av journalposten, må du huske på å benytte funksjonen Flett på nytt for å få navn og evt. adresser på de nye mottakerne lagt inn på selve dokumentet.

Trykk på

Du vil nå få opp noen HiL-maler du kan velge mellom, eventuelt Hent inn Fil fra disk.

Velg riktig mal og utarbeid dokumentet i Word.

Når du er ferdig, lagre dokumentet og gå (Øverst til venstre i bildet)

Du får opp en såkalt innsjekkingsboks. Det er viktig at denne er riktig utfylt slik at dokumentet blir lagret i ePhorte:

Kontroller at dokumentet har blitt sjekket inn!

Skal du jobbe videre med dokumentet senere?

Trykk kun på boksen

Er du ferdig med dokumentet?

Huk av: +

### 3.2.4 Sende til godkjenning

Dersom dokumentet skal godkjennes av leder haker du av i boksen ved Til godkjenning, se punktet over.

I dialogboksen som da blir vist, henter du opp initialene (+ navn) på den leder som skal godkjenne dokumentet ditt.

Når leder har godkjent får JP-en dokumentet status F.

Leder kan varsle deg med e-post når dokumentet er godkjent.

Du vil finne igjen dokumentene i søket

### 3.2.5 Endring i ferdigstilte notater med interne mottakere?

Som hovedregel skal ikke saksbehandler gå inn og endre informasjon i et notat som er ferdigstilt (status F), og som har en intern mottaker (som er ePhorte-bruker). Mottaker får nemlig innsyn i dokumentet straks det er ferdigstilt, og kan lese innholdet.

Dersom det er nødvendig å gjøre endringer i et slikt notat, bør mottakerne informeres om endringen.

### 3.2.6 Sende ut utgående brev

Når et utgående brev er ferdigstilt, skal det printes ut, undertegnes og sendes pr. post. Saksbehandler endrer da status på JP-en til F (ekspedert), slik at arkivet kan kvalitetssikre og journalføre brevet.

### 3.2.7 Redigere journalpostopplysninger

Hvis du skal endre/føye til mottakere, rette opp skrivefeil i tittel, endre dato og lignende, går du inn og redigerer journalpostopplysningene.

Trykk på pil til høyre for "konvolutt"

Velg Rediger

Endrer du noe på journalpostopplysningene, endres dette ikke automatisk i dokumentet, Ønsker du at endringene du har foretatt i journalpostopplysningene skal legges seg inn i selve dokumentet, bruk funksjonen

Flett på nytt.

Stå på dokumentnivå

Klikk på pil til høyre for "brevark"

Merk av for Flett på nytt.

HUSK: Det er viktig å ikke ferdigstille journalposten før du er helt ferdig.

### 3.2.8 Endre status på journalpost

Husk at hvis du skal gjøre endringer/tilføyelser i selve dokumentet, må JP'en ha status R (under behandling).

Hvis ikke må du gå inn og endre status ved å redigere JP (velg Rediger på journalpostnivå).

### 3.2.9 Redigere et dokument

Stå på dokumentnivå

Klikk på pil til høyre for "brevark".

Merk av for Rediger tekstdokument

Det skal ikke gjøres endringer i et internt notat med påført intern mottaker (ePhorte-bruker) som er ferdigstilt. Mottaker har nemlig tilgang til notatet straks det får status F.

Skal det foretas opprettinger bør det opprettes en ny versjon, utarbeides et nytt notat og ta kontakt med mottaker.

## 3.2.10 Legge vedlegg til et hoveddokument

### 3.2.10.1 Nytt vedlegg

Stå på dokumentnivå

Velg pila til høyre for dokumentikonet

Velg Nytt vedlegg

Tittel fra hoveddokumentet legger seg automatisk inn som tittel på vedlegget.

Husk å **endre dette til en beskrivende tittel for vedlegget.**

Vedlegget blir automatisk påført tilgangskode dersom hoveddokumentet er påført tilgangskode, men du kan også påføre vedlegget tilgangskode selv om ikke hoveddokumentet er unntatt fra offentlighet.

### 3.2.10.2 Sette inn vedlegg fra annen (eksisterende) post

Se fremgangsmåte i punktet over: Nytt vedlegg. Velg Knytt til eksisterende dokument

Da får du to valg:

1. Du kan legge ved et dokument som ligger i en annen sak i basen.
2. Du kan legge ved et dokument som er i samme sak

Gjør oppslag på "forstørrelsesglasset"

Dersom du skal sette inn dokument som tilhører en annen sak, henter du fram Dokumenter

Tips: Du får nå flere valg, men siden basen nå inneholder mange dokumenter, er det som regel kun løpenummeret som er unikt.

(Løpenummeret finner du i journalpostopplysningsfeltet for det dokumentet du ønsker vedlagt.)

Velg fra listen dokumenter du ønsker å knytte til som vedlegg til hoveddokumentet.

Dersom du skal sette inn et dokument som tilhører samme sak, henter du fram

Journalposter i sak.

Merk av det dokumentet du ønsker som vedlegg

Huk av (ved løpenummeret)

Legg til valgte rader Lagre

### 3.3 Søk etter saker / Journalposter

#### 3.3.1 Venstremenyen

I venstremenyen ligger ulike søk:

Under Fellessøk ligger det følgende søk for samtlige ePhorte-brukere:

Her finner du bl.a. oversikt over dokumenter du har mottatt til behandling eller til orientering, dokumenter du har under arbeid og dokumenter som er ferdigstilt eller godkjent i løpet av siste måned. Videre hvilke saker du arbeider med, hvilke saker du har avsluttet og ulike oversikter over all post som har kommet inn til høgskolen de siste dagene eller siste måneden.

I enkelte søk vises det du ikke har sett på ved et tall etter søket og med uthevet skrift:

Eksempel (her tatt fra et Arkivsøk)

Dette betyr IKKE at det er 20 utgående brev med status F, men siden forrige gang jeg har sett på dette søket, har det lagt seg inn 20 nye utgående brev med status F.

#### 3.3.2 Søk etter sak, journalpost eller dokument

ePhorte har flere muligheter for søk, avhengig av hvilken informasjon du ønsker å finne.

Standard søk: Enkelt søkebilde der du kan søke med få og begrensede kriterier.

Avansert søk: Gir mulighet til å søke på flere kriterier

Hurtigsøk: Gir mulighet til å søke på saksnummer direkte

En feil mange gjør, er at de ikke skiller på Sak og Journalpost når de skal søke.

##### 3.3.2.1 Finne en sak

Gå til verktøylinjen og velg søkeform (standard eller hurtigsøk) og klikk på

1. Velg fra rullemenyen – husk å velge Saksmapper/Mapper hvis du ønsker å søke etter en sak!

2. Skriv inn kriterier - du kan bl.a. velge mellom

- Saksnummer (men hvis du har dette, er hurtigsøk den enkleste løsningen)
- Tittel: et eller flere ord som kan befinne seg i sakstittel. Bruk for eksempel tegnet \* bak begynnelsen av ordet for å utvide søkemulighetene (for eksempel samarbeid\*)
- Dato: Hvis du vet hvilken dato saken kan være fra, kan du skrive den inn. Ved å klikke på får du opp en kalender der du kan velge en spesifikk dato eller en periode (intervall)
- Saksansvarlig: Saksansvarligs initialer. Kan søkes opp på Bruk fornavn og \*, for eksempel Ole\*

3. Klikk på "Søk nå"

##### 3.3.2.2 Finne en journalpost eller et dokument

1. Gå til verktøylinjen og velg søkeform Velg fra rullemenyen "Journalposter/Dokumentposter"

2. Skriv inn kriterier, du kan bl.a. velge mellom

- Innhold: et eller flere ord som kan befinne seg i journalpost- eller dokumenttittel
- Avsender/mottaker. Skriv inn deler av navnet med tegnet \* før eller etter, eller let opp navn med
- Journaldato: datoen journalpost/dokument har blitt journalført. Ved å klikke på får du opp en kalender

der du kan velge en dato eller en periode (intervall)

- Saksbehandler: Saksbehandlers initialer. Kan søkes opp på

4. Klikk på "søk nå"

Antall treff du maksimalt kan få er innstilt på 100. I feltet kan du skrive inn et tall for å få færre eller flere treff

### 3.4 Behandling (avskrivning) av mottatt post som krever svar / behandling (restanser)

En restanse er et innkommet brev (også e-post) eller et internt N-notat som du skal behandle, det vil si besvare eller ta til etterretning/orientering. Dette kalles å avskrive.

(Dersom det er brukt et X-notat, vil du ikke få noen restanse. Ta alltid forbehold om at avsender kan ha brukt feil dokumenttype, og sjekk derfor også søket: HiL Dokumenter jeg har mottatt til orientering – siste 30 dager om det kan ligge noe der du skal besvare eller ta til etterretning.)

I ePhorte markeres restansene med et rødt flagg ved siden av posten for den brukeren som har restansen.

For øvrige brukere er fargen på flagget blått.

For å behandle restansen, klikk på den blå pilen . Du får opp en liste over forskjellige alternativer, der du velger Besvar/Avskriv.

- Svar med utgående post - dersom det er svar på et inngående brev
- Svar med notat - dersom det er svar på et mottatt notat  
– her kan du også velge mellom X eller N-notat  
(Husk: N-notat gir mottaker restanse)
- Avskriv JP - dersom du ikke ønsker å besvare, men avskrive med en av følgende koder:
  - TE = tatt til etterretning
  - TO = tatt til orientering
  - TLF = besvart per telefon

