

Regler för lagring av Högskolan Dalarna information

Ärendet

Regler för lagring av Högskolan Dalarnas information HDa dnr: 1.2-2017/546 har uppdaterats så att de går i linje med de förändrade lagringsmöjligheterna högskolan fått genom avtalet med MS Office 365.

Förändringarna i dokumentet består av hur högskolans information ska hanteras i molntjänster, hur överföring via nätet ska ske, att e-post inte ska betraktas som ett digitalt lagringssystem samt att högskolans information i första hand ska hanteras i verksamhetssystemen.

Föreliggande revidering har förankrats vid bland annat informationsförvaltningsgruppen, MBL-förhandlingar samt hos högskolans jurist.

Rektor föreslås bifalla den nya versionen av ”Regler för lagring av Högskolan Dalarnas information”.

Beslut

Beslutas

- att fastställa bilagda förslag till ” Regler för lagring av Högskolan Dalarnas information”.

Ärendet föredrogs av Anders Forsman, avdelningschef Rektors kansli

Martin Norsell
Rektor

Anders Forsman
Föredragande

Delges

- Ledningsråd
- Förvaltningens chefer
- Akademiernas avdelningschefer
- Forskningsledare



HÖGSKOLAN
DALARNA

Regler för lagring av Högskolan Dalarnas digitala information

Beslut: Rektor 2017-04-10
Reviderad: 2019-11-18
Gäller fr o m: 2019-11-18
HDa dnr: 1.2-2017/546
Ersätter: Tidigare version
Relaterade dokument: -
Ansvarig: Förvaltningschef

Innehåll

Bakgrund	3
Regelverk	3
Lagringsplatser	3
Centralt lagringssystem	3
Lokalt på dator.....	3
Andra bärbara enheter.....	3
Molntjänster.....	3
Informationstyper	4
Information av ringa eller tillfällig betydelse	4
Verksamhetskritisk information	4
Sekretessbelagd information	4
Personuppgifter.....	4
Information som omfattas av bevarandekrav.....	4
Säkerhetsåtgärder	4
Val av lagringplats	5
Nivå 1.....	5
Nivå 2.....	5
Nivå 3.....	5
Checklista att använda vid val av lagringsplats	6
Uppföljning.....	6

Bakgrund

Högskolans information är en viktig resurs och en väl fungerande informationshantering är en förutsättning för en väl fungerande verksamhet. Viss information kan dessutom vara särskilt kritisk för verksamheten eller ha ett stort värde av andra skäl. Utöver detta ställer olika lagar och föreskrifter särskilda krav på högskolans informationshantering. Informationen kan t.ex. omfattas av sekretess, vara särskilt integritetskänslig eller vara av sådant slag att den ska bevaras för framtiden.

Högskolans verksamhet digitaliseras allt mer och därmed finns ett behov av riktlinjer för hantering och lagring av den information som skapas. Information ska i första hand hanteras i de verksamhetssystem som finns för respektive område. Detta förslag till regler för lagring av högskolans information syftar till att ge anställda förutsättningar att välja lämpliga lagringsplatser för den typ av digital information som ska lagras.

Utöver dessa generella regler, finns även specifika styrdokument gällande arkivering (bevarande) av handlingar och förvaltning av IT-baserade verksamhetssystem.

Regelverk

Krav på högskolans informationshantering finns bland annat i tryckfrihetsförordningen, offentlighets- och sekretesslagen, arkivlagen, Riksarkivets föreskrifter, Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter, personuppgiftslagen, dataskyddsförordningen, lagen om offentlig upphandling, förordning om myndigheters bokföring samt förordning om årsredovisning och budgetunderlag. Utöver dessa finns krav på informationshanteringen från t.ex. finansiärer.

Lagringsplatser

Digitala lagringsplatser som erbjuds anställda vid högskolan.

Centralt lagringssystem

Högskolan tillhandahåller kataloger på centralt lagringssystem (server) i form av personliga hemmakataloger (H:) och gemensamma delade lagringsytor (L:). Gemensamma lagringsytor beställs via support. All information som lagras på dessa ytor säkerhetskopieras dagligen och skyddas av IT-driften.

Lokalt på dator

Information kan även lagras lokalt på datorns hårddisk (C:). Information som lagras lokalt på datorn säkerhetskopieras inte automatiskt. Lagras information här måste användaren själv säkerställa att den skyddas.

Andra bärbara enheter

Högskolans tillhandahåller andra bärbara enheter som smarta telefoner, surfplattor, externa hårddiskar, minneskort och USB-minnen etc. Information som lagras på dessa enheter säkerhetskopieras inte automatiskt. Lagras information här måste användaren själv säkerställa att den skyddas.

Molntjänster

En molntjänst är en tjänst där lagringsytan finns hos en leverantör utanför Högskolan Dalarna. Högskolan har avtal med MS Office 365 för lagring i molntjänster. I övrigt finns inga avtal med några andra leverantörer av molntjänster och högskolan ansvarar inte för information som lagras i annan molntjänstleverantör.

Informationstyper

Högskolans verksamhet ger upphov till en mängd olika informationstyper, som i sin tur medför olika krav på lagringsplatsen.

Information av ringa eller tillfällig betydelse

En informationstyp som kan medföra något lägre krav på lagringsplatsen är information av ringa eller tillfällig betydelse. Hit hör t.ex. kopior av information som lagras i original på annat håll eller korrespondens av tillfällig eller rutinmässig karaktär.

Följande fyra informationstyper medför däremot ökade krav på valet av lagringsplats.

Verksamhetskritisk information

Verksamhetskritisk information avser information som skapas i kärn- och stödverksamheterna och är kritisk för enskilda lärare, forskare/forskargrupper, akademi/avdelning eller hela högskolan. Exempel på detta kan vara betygsunderlag, avtal, forskningsdata eller information som samlats in över lång tid och/eller som inte går att återskapa etc.

Sekretessbelagd information

Offentlighets- och sekretesslagen reglerar att viss information i högskolans verksamhet ska sekretessbeläggas. Exempel på handlingar som kan omfattas av sekretess är anbud (under anbudstiden), läkarintyg, rehabiliteringsutredning, skyddad identitet, provfrågor fram tills provet genomförts, uppgift hos studievägledare eller kurator, uppgift rörande stöd till student med funktionsnedsättning, utredning i disciplinärenden, forskningssamverkan med enskild, uppdragsverksamhet för enskilda räkning, patentansökan, insamlade forskningsdata i vissa fall.

Personuppgifter

Dataskyddsförordningen (tidigare personuppgiftslagen) reglerar behandling av personuppgifter, framförallt i digital form. Behandling av känsliga personuppgifter, som etnicitet, politiska åsikter, religiös/filosofisk övertygelse, medlemskap i fackförening, hälsa/sexualliv eller uppgifter om lagöverträdelse betraktas enligt lagen som extra integritetskänsliga, varför särskilt stränga krav ställs vid lagring av dessa. Personnummer är inte en känslig personuppgift enligt lagen, men ska enligt Datainspektionens praxis betraktas som en extra skyddsvärd uppgift.

Information som omfattas av bevarandekrav

Högskolans verksamhet ger upphov till så kallade allmänna handlingar, som i många fall ska arkiveras och bevaras för all framtid. Det ställer krav på en långsiktigt hållbar och säker lagring. Allmänna handlingar kan också gallras, men det får då bara ske i enlighet med Riksarkivets föreskrifter och lokala tillämpningsbeslut. Till de handlingar som normalt inte blir allmänna handlingar och som därmed inte omfattas av bevarandekrav hör arbetsmaterial, kopior och egna minnesanteckningar.

Säkerhetsåtgärder

- Samtliga enheter ska vara lösenordskyddade. Det gäller således inte enbart datorer utan även smarta telefoner och surfplattor. Aktivera enhetens skärmlås.
- Systemägare ansvarar för att det finns rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter.
- E-post är inte att betrakta som ett digitalt lagringssystem och ingen information arkiveras därifrån. Det är varje användares eget ansvar att hantera informationen däri på ett korrekt sätt.

Vidare information om säkerhetsåtgärder finns i styrdokument gällande IT- och informationssäkerhet.

Val av lagringsplats

För att anställda på ett enkelt sätt ska kunna bedöma sin information och välja en lämplig lagringsplats kan följande tre nivåer användas:

Nivå 1

- Informationstyp:
 - Informationen skulle kunna spridas till vem som helst/förloras utan negativa konsekvenser för verksamheten eller enskilda. Innehåller varken sekretess eller personuppgifter.
- Lagringsplats:
 - Informationen bör lagras på centralt lagringssystem (server), lokalt på dator, bärbar media eller avtalad molntjänst.
- Överföring: Inga särskilda hänsyn behöver tas.

Nivå 2

- Informationstyp:
 - Informationen kan inte spridas till vem som helst/förloras utan negativa konsekvenser för verksamheten eller enskilda. Innehåller dock varken sekretess eller känsliga personuppgifter. Kan däremot innehålla andra personuppgifter.
- Lagringsplats:
 - Informationen ska lagras på centralt lagringssystem (server) eller regelbundet överföras dit. Informationen kan även lagras i en molntjänst som högskolan tecknat avtal med. Vid tillfällig lagring lokalt på dator eller bärbar media som smart telefon, surfplatta, extern hårddisk eller USB ska lämpliga skyddsåtgärder vidtas för att säkra informationen under den tiden. Observera att vid bevarandekrav måste informationen senast när ärendet avslutas eller medarbetaren slutar flyttas till annan lagringsplats för arkivering.
- Överföring:
 - Verksamhetssystemen och de säkrade gemensamma lagringssystemen kan användas.
 - Informationstypen avgör vilken lösning som kan vara lämplig. Se tabellen nedan och vid behov kontakta support@du.se för att få hjälp med en bedömning och anpassning.
 - Överföring internt inom högskolan via e-post fungerar men undvik överföring med e-post till extern part.

Nivå 3

- Informationstyp:
 - Informationen innehåller sekretess och/eller känsliga personuppgifter. Den kan inte spridas till vem som helst/förloras utan negativa konsekvenser för verksamheten eller enskilda.
- Lagringsplats:
 - Informationen ska lagras på centralt lagringssystem (server). Informationen ska inte lagras lokalt på datorn eller på bärbar media mer än tillfälligt, och då med skyddsåtgärder. Informationen får inte lagras i molntjänst. Observera att vid

bevarandekrav måste informationen senast när ärendet avslutas eller medarbetaren slutar flyttas till annan lagringsplats för arkivering.

- Överföring:
 - Verksamhetssystemen och de säkrade gemensamma lagringsytorna kan användas. För denna informationstyp är överföring med e-post ej lämplig. I vissa fall kan specifika bedömningar och lämpliga anpassningar behöva göras, i dessa fall kontakta support@du.se

Checklista att använda vid val av lagringsplats

- Gröna rutor visar lämplig lagringsplats.
- Gul kan användas för tillfällig lagring om lämpliga säkerhetsåtgärder vidtas.
- Röd ska inte användas.

Informationstyp Lagringsplats	Ringa eller tillfällig betydelse	Verksamhetskritisk	Sekretess	Känsliga personuppgifter	Personuppgifter	Bevarandekrav ¹
Centralt lagringssystem (H: eller L: etc.)						
Lokalt på dator (C: eller motsvarande)						
Bärbar media: Smarta telefoner, surfplattor, extern hårddisk, usb etc.						
Molntjänst som högskolan tecknat avtal med: MS Office 365 t. ex. Teams och One Drive						
Molntjänst som högskolan saknar avtal med t. ex. Dropbox, iCloud, Google Drive, Evernote.						

Uppföljning

Tillämpningen av dessa regler ska följas upp regelbundet av informationsförvaltningsgruppen. Det ska ske genom kontinuerlig uppföljning av inkomna incidentrapporter och uppföljning av vilka tjänster som används av anställda, bland annat med hjälp av stickprov.

Om behov uppstår som innebär avsteg från dessa regler kan dispens behandlas av IT-chef.

¹ Observera att vid bevarandekrav måste informationen senast när ärendet avslutas eller medarbetaren slutar flyttas till annan lagringsplats för arkivering.