HÖGSKOLAN DALARNA

REGEL

Gäller från och med
2022-08-29

Beslutat av
Rektor

Diarienummer
C 2022/936

Regler för lagring av digital information

Rules for the Storage of Digital Information

Bakgrund

Högskolans information är en viktig resurs och en väl fungerande informationsförvaltning 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 informationsförvaltning. Informationen kan till exempel omfattas av sekretess, vara särskilt integritetskänslig eller vara av sådant slag att den ska bevaras för framtiden.

Högskolans verksamhet hanterar en stor mängd digital information och det finns 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 styrdokument syftar till att ge anställda förutsättningar att välja lämpliga lagringsplatser för den typ av digital information som inte ryms i verksamhetssystemen.

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

Regelverk

Krav på högskolans informationsförvaltning 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 informationsförvaltningen från t.ex. finansiärer.

Lagringsplatser

Lagringsplatser som erbjuds anställda vid Högskolan Dalarna.

Verksamhetssystem

Ett verksamhetssystem är ett system som är särskilt utvecklat för att stödja en specifik verksamhet inom ett eller flera verksamhetsområden. Exempel på verksamhetssystem är Learn/Blackboard, LADOK, Agresso, diariet/W3D3, Primula, DiVA. Hur information hanteras i högskolans verksamhetssystem regleras via avtal i samband med upphandling.

Centrala lagringsytor

Högskolan tillhandahåller kataloger på centrala lagringsytor (server) i form av personliga hemmakataloger (H:) och gemensamma delade lagringsytor (till exempel L:), m.m. 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 Microsoft 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.

Lagringsalternativ för forskningsprojekt
Forskningsprojekt kan ibland ställa högre krav, gällande säkerhet och tillgänglighet, än vad som ovan lagringsalternativ kan erbjuda. Högskolan kan då, i dialog med forskningsdatastödet, erbjuda lämpliga anpassade lösningar utifrån de behov som forskningsprojektet kräver. För mer information kontakta Forskningsstödet

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 till exempel 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, institution/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.

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 enskilds räkning, patentansökan, insamlade forskningsdata i vissa fall.

Personuppgifter

Dataskyddsförordningen (tidigare personuppgiftslagen) reglerar behandling av personuppgifter, framför allt i digital form. Behandling av känsliga personuppgifter, som etnicitet, politiska åsikter, religiös/filosofisk övertygelse, medlemskap i fackförening, hälsa/sexualliv eller uppgifter om lagöverträdelser 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. Vid bevarandekrav måste informationen, senast när ärendet avslutas eller medarbetaren slutar, flyttas till annan lagringsplats för arkivering. Frågor gällande bevarande av information kontakta arkivfunktionen arkiv@du.se.

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 kan spridas till vem som helst/förloras utan negativa konsekvenser för verksamheten eller enskilda. Innehåller varken sekretess eller personuppgifter.
- Lagringsplats:
  - Informationen kan 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 lagringsytorna 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 verksamhetskritisk, sekretess och/eller känsliga personuppgifter. Den kan intespridas 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 får överföring via e-post endast ske med hjälp av kryptering. 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

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

Informationstyp Lagringplats	Ringa eller tillfällig betydelse	Verksam-hetskritisk	Sekretess	Känsliga person-uppgifter	Person-uppgifter
Verksamhetssystem (t.ex. Learn, Black board, LADOK, Primula, Agresso Diariet, DIVA)					
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: Microsoft 365 t.ex. Teams och One Drive					
Molntjänst som högskolan saknar avtal med t. ex. Dropbox, iCloud, Google, Drive, Evernote.					

Rules for the Storage of Digital Information

Background

The University's information is an important resource, and well-functioning information management is necessary for a well-functioning organisation. In addition to this, certain information may be particularly critical for the University or may be of value for other reasons. Certain laws and regulations place special demands on information management at the University. Some information may be subject to confidentiality, may be particularly sensitive, or may be of such a kind that it must be retained for the future.

The University processes a large amount of digital information, and guidelines are required about how to process and store the information that is generated. For the most part, information must be processed in the systems that are in place for each area of the organisation. This policy document aims to enable employees to choose the appropriate storage location for the type of digital information that cannot be accommodated in those systems.

As well as these general rules, there are also specific policy documents on the archiving (retention) of documents, information security, and management of IT-based systems.

Regulations

Information management requirements of universities can be found in the Freedom of the Press Act *(Tryckfrihetsförordningen)*, Public Access to Information and Secrecy Act *(Offentlighets- och sekretesslagen)*, Archives Act *(Arkivlagen)*, Swedish Civil Contingencies Agency directives *(Myndigheten för samhällsskydd och beredskaps)*, Personal Data Act *(Personuppgiftslagen)*, General Data Protection Regulation *(datskyddsförordningen)*, Swedish Public Procurement Act *(Lagen om offentlig upphandling)*, Bookkeeping Ordinance *(Förordning om myndigheters bokföring)*, and *Förordning om årsredovisning och budgetunderlag*. In addition to these, funding bodies, for example, also set requirements for information management.

Storage Locations

These are the storage locations available for use by Dalarna University employees:

University Systems

The University has systems that have been specially developed to support specific activities within one or more parts of the organisation. Examples of such systems are Learn/Blackboard, LADOK, Agresso, diariet/W3D3, Primula, DiVA. How information is processed in these is regulated by the agreements at the time of their procurement.

Central Storage Locations
The University provides directories in central storage locations (servers) such as home directories (H:) and shared storage locations (for example, L:). Shared storage locations can be ordered via support. All information stored on these are backed up on a daily basis and protected by IT.

Local Storage on Computers
Information can also be stored locally on a computer's hard drive (C:). Information stored locally on a computer is not backed up automatically. If information is stored on the computer, it is up to the user to ensure it is protected.

Other Portable Devices
Available through the University are other portable devices such as smart phones, tablets, external hard drives, memory cards, and USB sticks. Information stored on these devices is not automatically backed up. If information is stored on the computer, it is up to the user to ensure it is protected.

Cloud Services
A cloud service is when the storage location is with a supplier external to Dalarna University. The University has an agreement with Microsoft 365 for storage in cloud services. The University has no such agreement with any other supplier of cloud services and is not responsible for information stored in other cloud service providers.

Storage Options for Research Projects
Research projects can sometimes demand higher levels of security and availability than the above storage options can offer. In dialogue with research data support services, the University can offer suitable adapted solutions based on the needs of the research project. For more information, contact Research Support.

Information Types
University activities give rise to many types of information, which in turn places different demands on storage location.

Information of Minor or Short-Term Importance
One type of information that may set somewhat lower requirements on storage location is information of minor or short-term importance. This includes, for example, copies of information stored in its original form elsewhere or occasional, everyday correspondence.

The following four types of information, on the other hand, place high demands on the choice of storage location.

Information That Is Critical for University Operations
This type of information refers to information that is created in core and support areas of the University that is critical for individual teachers, researchers/researcher groups, university school/department, or the entire university. Examples are documentation for grades, agreements, research data, or information that has been collected over a long period and/or that cannot be reproduced.

Confidential Information
The Public Access to Information and Secrecy Act regulates the classification of certain information in university operations as being confidential. Examples of documents that may be covered by confidentiality are tenders (during the tender period), medical certificates, rehabilitation investigations,

protected identity, test questions until after the test, information from a study guidance counsellor, information about support for a student with a disability, investigation into disciplinary matters, research collaboration with an individual, the activities of an individual, patent application, and, in some cases, collected research data.

Personal Data

The General Data Protection Regulation (GDPR) (formerly the Personal Data Act) regulates the processing of personal data, principally in digital form. Data about, for example, ethnicity, political opinions, religious/philosophical beliefs, trade-union membership, health, sex life/sexual orientation, and violations of the law is considered extra sensitive according to the law, which is why there are particularly strict requirements about how to store it. A personal identity number *(personnummer)* is not sensitive personal data according to the law, but according to Data Protection Authority practice, it is considered to be data that is worth extra protection.

Information Subject to Retention Requirements

University activities result in the creation of official documents, which in many cases must be archived and preserved for all time. This requires long-term sustainable and safe storage. Retention (also known as preservation) requirements mean that information must be moved to another storage location for archiving at the latest when the matter is closed or when the employee leaves their position of employment. Questions on the preservation of information should be directed to university archives: arkiv@du.se.

Public documents can also be deleted, but this may only be done in accordance with Riksarkivet (the national archives) regulations and local decisions on application. The documents that do not normally become official and that are therefore not covered by retention requirements include work material, copies of documents, and personal notes.

Security Measures

- All devices must be password protected. This, therefore, applies not only to computers but also to smart phones and tablets. Activate the screen lock function on the device.
- System owners are responsible for ensuring that there are procedures in place for assigning, changing, removing, and regularly monitoring authorisation.
- E-mail is not to be considered a digital storage system and no information is archived from it. It is the responsibility of each user to correctly process the information in emails.

Further information on security measures can be found in the policy document on IT and information security.

Choice of Storage Location

For employees to be able to easily assess their information and select a suitable storage location, these three levels can be used:

Level 1

- Information Type:
    - The information can be shared with anyone/can be lost without negative consequences for the University or individuals. It contains neither confidential nor personal data.
- Storage Location:

    - The information can be stored on a central storage system (server), locally on a computer, on portable media, or in a contracted cloud service.
- Transfer:
    - No special considerations.

Level 2

- Information Type:
    - The information cannot be shared to everyone/cannot be lost without negative consequences for the University or individuals. It does not, however, contain any confidential or sensitive personal data. However, it may contain other personal data.
- Storage Location:
    - The information must be stored on a central storage system (server) or be regularly transferred there. The information can also be stored in a cloud service that the University has a signed agreement with. When data is stored temporarily on a computer or portable media, such as a smart phone, tablet, external hard drive, or USB, appropriate safeguards must be taken to protect and secure information during that time. Please note that when it comes to retention requirements, information must be moved to another storage location for archiving at the latest when the matter is closed or the employee leaves their position of employment.
- Transfer:
    - The university systems and the secured shared storage areas can be used.
    - The type of information determines which solution is appropriate. See the table below and, if necessary, contact support@du.se for help with an assessment and adaptation.
    - Transfer within the University by e-mail is possible, but the transfer of information by email to an external party is to be avoided.

Level 3

- Information Type:
    - The information contains data that is critical for the University, data that is confidential, and/or sensitive personal data. It cannot be shared with anyone or be lost without negative consequences for the University or individuals.
- Storage Location:
    - The information must be stored in a central storage system (server). The information should not be stored locally on a computer or on portable media unless this is short-term and so long as it is secure. The information must not be stored in a cloud service. Please note that when it comes to retention requirements, information must be moved to another storage location for archiving at the latest when the matter is closed or the employee leaves their position of employment.
- Transfer:
    - The university systems and the secured shared storage areas can be used. For this type of information, transmission via e-mail is only permitted using encryption. In some cases, specific assessments and appropriate adaptations may be required: when this is the case, contact support@du.se.

Checklist - Selection of Storage Location

- Green shows a suitable storage location.
- Yellow can be used for temporary storage if there are adequate security measures.
- Red must not be used.

Information Type Storage Location	Minor or short-term significance	Critical for the University	Confidential	Sensitive personal data	Personal data
University systems (for example, Learn, Blackboard, LADOK, Primula, Agresso Diariet, DIVA)					
Central storage system (H: or L:, etc.)					
Local on computer (C: or equivalent)					
Portable media: smart phones, tablets, external hard drive, USB, etc.					
Cloud service that the University has a signed agreement with: Microsoft 365 – for example, Teams and One Drive					
Cloud service that the University does not have an agreement with, for example, Dropbox, iCloud, Google, Drive, Evernote					