Lathund för nyttjande av digitala samarbetsverktyg och lagringsytor inom ramen för Umeå universitets verksamhet

Denna lathund är en del av ledningssystemet för informationssäkerhet vid Umeå universitet.

Syfte

Lathunden ska underlätta för användaren att välja rätt samarbetsverktyg eller lagringsyta för sin digitala information, beroende på informationstyp. När det gäller lagring av *personuppgifter* finns begreppet definierat på sidan FAQ Vad är personuppgifter? Vad menas med att det finns olika typer av personuppgifter? Avseende *sekretessbelagd information* finns på sidan offentlighet och sekretess mer information om hur Umeå universitet som myndighet tillämpar reglerna om sekretess. När det gäller *hur e-post vid Umeå universitet ska användas* hänvisas till FAQ om Personuppgifter och e-post.

Bevarande och gallring

Ingen information ska arkiveras eller bevaras långsiktigt på redovisade ytor. Handlingar som ska arkiveras hanteras i de verksamhetssystem och processer dit den hör och arkiveras enligt gällande dokumenthanteringsplaner.

Användning

Lathunden visar på vilka generella möjligheter till lagring som finns för olika typer av information. På sidan om programvaror och licenser framgår vilka samarbetsverktyg och digitala lagringsytor som universitetet har legal rätt (licens för) att använda för universitetets verksamhet. Det är inte tillåtet att använda andra digitala samarbetsverktyg och lagringsytor i universitetets verksamhet utan att såväl licens-, säkerhets- och andra relevanta faktorer säkerställts.

I universitetets verksamhet får man bara använda de tjänster som universitetet rekommenderat. Det här innebär att egna aktiverade tjänster **inte** får användas som exempelvis: Dropbox, Googles molntjänster (t.ex. Drive, Apps) och iCloud.

Eventuella frågor skickas till: servicedesk@umu.se

Vid val av samarbetsverktyg eller lagringsyta kan nedanstående lathund vara till hjälp för att välja rätt samarbetsverktyg eller lagringsyta för aktuell information.

Typ av information / Tjänst	Text utan personuppgifter, sekretess eller säkerhetsskydd. Även information med vanliga personuppgifter	Information med integritetskänsliga personuppgifter	Information med känsliga personuppgifter	Information som kan vara sekretessbelagd	Information som omfattas av säkerhetsskyddslagen	Annan särskilt skyddsvärd information
Min dator	**JA**	**Arbetsmaterial, mindre mängder ****	**Arbetsmaterial, mindre mängder ****	**Arbetsmaterial, mindre mängder ****	**NEJ**	**Arbetsmaterial, mindre mängder ****
Skyddade Dokument (tidigare Trygg Filyta)	**JA**	**JA**	**JA**	**JA**	**NEJ**	**JA**
DIP (Data Insamlings Plattform)	**JA**	**JA**	**JA**	**JA**	**NEJ**	**JA**
RedCap (eCRF-system)	**JA**	**JA**	**JA**	**JA**	**NEJ**	**NEJ**
Lärplattformar (ej alternativ för lagring, LMS (Learning Management System) bör endast användas inom utbildningsrelaterad verksamhet)	**JA**	**NEJ**	**NEJ**	**NEJ**	**NEJ**	**NEJ**
Onedrive, Teams i universitetets O365	**JA**	**Ytterligare skyddsåtgärder krävs*****	**NEJ**	**NEJ**	**NEJ**	**NEJ**
UmU-play (är en videotjänst)	**JA**	**NEJ**	**NEJ**	**NEJ**	**NEJ**	**NEJ**
Klassningsvärde	**1**	**2/3**	**3**	**2/3**	**3**	**3**

Klassningsvärdena i tabellen ovan visar hur Umeå universitet bedömer skyddsnivån för de olika informationstyperna. Kontakta Dan.Harnesk@umu.se för ytterligare information om informationsklassning. I tabellen finns exempel på hanteringsregler för information i de olika klassningsnivåerna.

Hanteringsreglerna fokuserar i detta dokument endast på lagring och delning av information. I tabellen finns även grundläggande it-säkerhetsåtgärder och organisatoriska säkerhetsåtgärder kopplade till respektive klassningsnivå.

** Med mindre mängd avses rekommendationen att bara lagra det som du absolut behöver i ditt dagliga arbete.

*** Primärt rekommenderas 2-faktor autentisering. Om detta ej uppfylls måste filkryptering ske, per fil eller filmapp – se även säkerhetsåtgärder nedan.

Säkerhetsåtgärder kopplade till samarbete och lagringsytor			
Hanteringsregler	**Exempel på data och konsekvens vid förlust/röjande/obehörig åtkomst av data**	**Allmänt för alla klassningsnivåer: Grundläggande säkerhetsåtgärder är att begränsa åtkomst till it-resurser och minimera risk för röjande och förvanskning av information.**	
		it-säkerhetsåtgärd	**Organisatorisk säkerhetsåtgärd**
Klass 1 – skyddsvärd information Informationen får lagras och överföras på och med alla grönmarkerade tjänster som gäller för klassningsvärde 1. Informationen får göras tillgänglig för åtkomst med identifiering av användare.	Information för UmU:s fortlöpande verksamhet som innehåller vanliga personuppgifter, och information som inte faller under sekretess **Måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Enstaka missnöjda samarbetspartners, uttryck i sociala medier. Lindrig förtroendeskada	**Grundläggande skydd säkerställs genom inloggning till it-resurser med UmU-ID eller motsvarande**	**Användare ska endast ges tillgång till it-resurser och it-tjänster som de specifikt beviljats tillstånd för.** **Institutioner och enheter har rutin för att regelbundet identifiera, ta bort eller inaktivera överflödiga behörigheter**
Klass 2 – Information med betydande skyddsvärde Informationen får lagras och överföras på och med alla grönmarkerade tjänster som gäller för klassningsvärde 2. Därtill får informationen, under vissa förutsättningar lagras i Microsofts molntjänst. För bedömning om det är lämpligt kontakta ITS/infosäk för vägledning. Informationen får göras tillgänglig för åtkomst med identifiering av användare	Integritetskänsliga personuppgifter Information som är kritisk för t.ex. en enskild forskare, forskargrupp, forskningsprojekt **Betydande** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Begränsat missnöje, uttryckt i riks- och lokalmedia. Betydande förtroendeskada	**Utökat skydd säkerställs genom 2-faktorsautenticering. ***** **Utökat skydd säkerställs med VPN för åtkomst utanför Umu till interna it-resurser.** **Utökat skydd genom klienthantering med aktiverad lokal kryptering (Bitlocker, FileVault).** **Utökat skydd genom individuell filkryptering med minimum lösenordslängd 12 tecken *****	*Användare ska endast ges tillgång till it-resurser och it-tjänster som de specifikt beviljats tillstånd för.* *Institutioner och enheter har rutin för att regelbundet identifiera, ta bort eller inaktivera överflödiga behörigheter* **Säkerställ att regler för användning av mobila enheter och vid distansarbete efterlevs.**
Klass 3 – Information med högt skyddsvärde Informationen får lagras och överföras på och med alla grönmarkerade tjänster som gäller för klassningsvärde 3. Därtill får informationen, under vissa förutsättningar lagras i Microsofts molntjänst. För bedömning om det är lämpligt kontakta ITS/infosäk för vägledning. Vid samarbete och lagring av viss typ av klass 3 information kan det krävas starkare skydd än universitetets standardlösningar. Till exempel vid hantering av information som faller under säkerhetsskyddslagen Informationen får göras tillgänglig för åtkomst med identifiering av användare	Känsliga personuppgifter Information kopplad till person med skyddad identitet, Särskilt skyddsvärd information i forskningsverksamhet **Allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Flertalet missnöjda samarbetspartners, drev i riksmedier eller sociala grupper. Allvarlig förtroendeskada.	**Högt skydd säkerställs genom 2-faktorsautenticering och kryptering vid överföring och lagring.** **Högt skydd säkerställs med VPN för åtkomst utanför Umu till interna it-resurser.** **Utökat skydd genom klienthantering med aktiverad lokal kryptering (Bitlocker, FileVault** **Utökat skydd genom individuell filkryptering med minimum lösenordslängd 12 tecken**	*Användare ska endast ges tillgång till it-resurser och it-tjänster som de specifikt beviljats tillstånd för.* *Institutioner och enheter har rutin för att regelbundet identifiera, ta bort eller inaktivera överflödiga behörigheter* *Säkerställ att regler för användning av mobila enheter och vid distansarbete efterlevs.* **Dokumenterade rutiner för skydd av information vid användning av mobil it-utrustning.**