

## Rutinbeskrivning för digitala arbetsytor för Mittuniversitetets personal

Denna rutin är en del av Mittuniversitetets ledningsinformationssystem för informationssäkerhet.

### Syfte

Rutinerna ska underlätta för slutanvändaren att välja rätt arbetsyta för sin digitala information, beroende på informationstyp.

### Bevarande och gallring

Ingen information arkiveras/bevaras långsiktigt via redovisade arbetsytor. Handlingar som ska arkiveras hanteras i de verksamhetssystem och processer dit de hör och arkiveras elektroniskt, alternativt överlämnas digitalt eller på papper till universitetets arkivfunktion för arkivering enligt överenskomna rutiner. Detta utgör inget hinder för att hantera kopior av arkiverad information/information som kommer att arkiveras via arbetsytorna då behov finns, rutiner i de fastställda lathundarna gäller även kopior av arkiverad information.

### Användning

Det finns två lathundar, en mer **allmän** (sid 2) och en för **tjänster i Office 365** (sid 3). Dessa visar på olika typer av information och möjligheter till arbetsytor i generaliserad form. De använder "Ja" och "Nej" och i undantagsfall en kombination ("Nja") för att visa vilka arbetsytor som kan användas.

Eventuella frågor skickas till Helpdesk, [helpdesk@miun.se](mailto:helpdesk@miun.se).

### Ansvar och uppdatering för dokumentet

INFRA ansvarar för att uppdatering av dokumentet sker och att aktuell version ligger tillgänglig på sidan för *informationssäkerhet* på Medarbetarportalen.



## Allmän lathund för Mittuniversitetets supporterade digitala arbetsytor

De arbetsytor som Mittuniversitetet supporterar (stödjer) ska vara det primära valet för universitetets medarbetare. I vissa fall kräver samarbeten med externa parter andra ytor för samarbete och lagring av dokument. Det är då viktigt att beakta vilken typ av data som får användas var. För användning av såväl Dropbox och iCloud som Facebook, övriga externa tjänster, moln/annat KAN

enklare samarbeten vara möjliga så länge som det enbart gäller text utan personuppgifter, sekretess eller säkerhetsskydd och/eller information med mer harmlösa personuppgifter. Viktigt att komma ihåg är dock att om arbetsytan inte supporteras av universitetet kan heller ingen hjälp fås vid eventuella problem. Kontakta Helpdesk om du är osäker på hur din information får hanteras.

TYP AV INFORMATION TJÄNST	Text utan personuppgifter, sekretess eller säkerhetsskydd. Även information med mer harmlösa personuppgifter.	Information med särskilda kategorier av personuppgifter (s.k. känsliga personuppgifter) eller i annat fall integritetskänsliga personuppgifter	Information som kan vara sekretessbelagd	Information som omfattas av säkerhetsskydd (spioneri, sekretess enligt rikets säkerhet, terrorism) eller där krav på hög säkerhet ställs i exempelvis avtal.
Miuns arbetsytor (nätverksdiskar) som driftas av INFRA.	JA	JA	JA	Nja, möjligtvis efter dialog med INFRA om nödvändiga säkerhetsåtgärder
Box	JA	JA (Men helst inte)	NEJ	NEJ
Office 365	Se egen lathund	Se egen lathund	Se egen lathund	Se egen lathund
Google Docs/Google Drive	(Anställda vid Miun/Rött, Student vid Miun/Grön)	NEJ	NEJ	NEJ

## Lathund för hantering av information i digitala arbetsytor i Office 365 (O365)

I tabellen nedan har en enkel lathund tagits fram för att som ett stöd och en översiktlig bedömning visa vilken typ av information som kan hanteras i O365 tjänster och vad som måste hanteras på annat sätt. Som komplement till denna lathund finns den andra tabellen i denna rutinbeskrivning som gäller för allmän användning av supporterade digitala arbetsytor. Tabellen nedan är mer detaljerad än den allmänna lathunden.

TYP AV INFORMATION TJÄNST	Text utan personuppgifter, sekretess eller säkerhetsskydd. Även information med mer harmlösa personuppgifter.	Information med särskilda kategorier av personuppgifter (s.k. känsliga personuppgifter) eller i annat fall integritetskänsliga personuppgifter	Information som kan vara sekretessbelagd	Information som omfattas av säkerhetsskydd (spioneri, sekretess enligt rikets säkerhet, terrorism) eller där krav på hög säkerhet ställs i exempelvis avtal.
Microsoftprogram där dokument medvetet sparas ned till Miuns lagringsytor (ex H:\)	JA	JA	JA	Nja, möjligtvis efter dialog med INFRA om nödvändiga säkerhetsåtgärder
Molnbaserade tjänster hos Microsoft, ex. OneDrive	JA	NEJ	NEJ	NEJ
Överföring genom e-post (Outlook, ligger i molnet)	JA	Ja, om krypteringsmöjligheten i Outlook används annars nej.	NEJ	NEJ
Information som hanteras med teknisk säkerhet utöver den grundläggande nivån, exv. kryptering	JA	NEJ	Nja, möjligtvis efter dialog med INFRA om nödvändiga säkerhetsåtgärder	NEJ