Mittuniversitetet
MID SWEDEN UNIVERSITY

Riktlinjer för användning av Microsoft 365 för medarbetare vid Mittuniversitetet

Publicerad: 2026-08-25

Beslutsfattare: Avdelningschef, Helena Wallskog

Ansvarig funktion: Digitalisering och service

Handläggare: Sonja Balaz

Beslutsdatum: 2026-08-25

Giltighetstid: Tillsvidare

Senaste översyn: 2026-08-25

Sammanfattning: Detta dokument innehåller riktlinjer för hur Microsoft 365 ska användas vid Mittuniversitetet, med fokus på informationshantering, säkerhet, lagring, gallring och användning av olika tjänster.

Tidigare versioner: MIUN 2020/740

Innehållsförteckning

Riktlinjer för användning av Microsoft 365 för medarbetare vid Mittuniversitetet

1 Inledning och syfte

Microsoft 365 (M365) är en molnbaserad tjänst från Microsoft som innehåller bland annat Outlook, Word, Excel, PowerPoint, Forms, OneDrive, SharePoint, Teams och Copilot. Tjänsten används för kommunikation, samarbete, lagring och delning av information i universitetets verksamhet.

Mittuniversitetet ska hantera information i M365 i enlighet med gällande regelverk, däribland tryckfrihetsförordningen (TF), offentlighets- och sekretesslagen (OSL), dataskyddsförordningen (GDPR) samt universitetets egna styrande dokument.

Syftet med denna riktlinje är att tydliggöra hur M365 ska användas på ett sätt som stödjer verksamheten, minskar risker och säkerställer att information hanteras enligt gällande lagar, krav och interna rutiner. Riktlinjen ska också ge stöd i hur medarbetare bedömer vilken typ av information som får hanteras i de olika tjänsterna.

Riktlinjerna gäller för alla medarbetare vid Mittuniversitetet som har tillgång till M365. De ersätter de tidigare reglerna för M365 och tydliggör universitetets gemensamma inriktning för användning, hantering och ansvar. Efter beslut kommer riktlinjerna att införas genom information på medarbetarsidorna, riktade kommunikationsinsatser och användarstöd.

2 Regelverk, sekretess och integritet

Mittuniversitetet hanterar allmänna handlingar och ska samtidigt skydda information som omfattas av sekretess. Det innebär att information som lagras eller delas i M365 alltid behöver bedömas utifrån innehåll, ändamål och skyddsnivå.

GDPR föreskriver att personuppgifter inte ska behandlas i större omfattning eller längre än nödvändigt i förhållande till ändamålet med behandlingen. Personuppgifter i M365 bör raderas när ändamålet med behandlingen är

uppfyllt, under förutsättning att det är förenligt med gällande informationshanteringsplan och gallringsbeslut (se Arkiv och Diarum).

Eftersom M365 är en extern molntjänst ska information som är sekretessbelagd eller särskilt skyddsvärd hanteras med stor försiktighet. Sekretesskyddade uppgifter, känsliga personuppgifter och uppgifter som av annan anledning är extra skyddsvärda ska inte lagras i M365.

Vid e-post som innehåller känsliga personuppgifter, extra skyddsvärda personuppgifter eller sekretessbelagd information ska kryptering användas i enlighet med universitetets anvisningar (se Rutinbeskrivning för digitala arbetsytor för Mittuniversitetet).

3 Känslighetsetiketter

Känslighetsetiketter används för att stödja korrekt hantering av dokument, e-post och annan information i M365. Etiketten visar vilken skyddsnivå som gäller för informationen och hjälper användaren att hantera den på rätt sätt.

Etiketter ska användas konsekvent och väljas utifrån informationens innehåll och skyddsbehov.

Det är varje medarbetares ansvar att använda känslighetsetiketter enligt universitetets riktlinjer och välja rätt etikett utifrån informationens karaktär (se Känslighetsetiketter).

4 Bevarande, gallring och lagring

M365 ska inte användas för långtidsbevarande eller arkivering av handlingar. Handlingar som ska bevaras ska i stället hanteras i verksamhetssystem eller överlämnas till universitetets arkivfunktion enligt fastställda rutiner (se E-post och Teams utifrån arkivkrav och GDPR).

Det är varje medarbetares ansvar att:

- rensa och gallra arbetsytor i M365 enligt informationshanteringsplan och gallringsbeslut
- föra över handlingar som ska bevaras till rätt verksamhetssystem
- undvika att låta tillfälliga arbetsytor bli permanenta lagringsytor

4.1 Retroaktiv gallring

För att följa gällande beslut kan äldre e-postmeddelanden och chattar gallras automatiskt enligt fastställda rutiner (gallringsbeslut 2022–2 och MIUN 2022/2745). Syftet är att rensa information som skulle ha tagits bort tidigare men som fortfarande finns kvar.

5 Generella riktlinjer för användning av M365 och Copilot

- Får inte innehålla sekretessbelagd information, känsliga personuppgifter eller extra skyddsvärda personuppgifter.
- M365 och agenter får inte användas för privata ändamål.
- Får inte användas på ett sätt som bryter mot svensk lag, upphovsrätt eller universitetets ansvarsförbindelse.
- Får inte användas för att kränka, förolämpa, förnedra eller trakassera andra.
- Får installeras på privata datorer, men IT-support ges endast till datorer som Mittuniversitetet äger.
- Varje användare kan använda M365 på totalt fem enheter enligt gällande licensvillkor.

6 Särskilda riktlinjer för Teams och SharePoint

Teams och SharePoint används för samarbete, delning och gemensamt arbete. Den som skapar ett team eller en grupp ansvarar för att innehållet hanteras enligt gällande regelverk:

6.1 Teamägarskap och ansvar

- Alla grupper och team ska ha minst två ägare.
- Den som skapar teamet är kontaktperson gentemot DOS.
- Ägaren ansvarar för medlemskap, åtkomst, namnstruktur och att teamet hålls aktuellt.
- Ägaren ansvarar för att ta bort team som inte längre används.

- Team som inte har använts under 3 månader tas bort efter information till teamets ägare, automatiska påminnelser skickas till teamägarna.

6.2 Namngivning

Team och grupper ska ges tydliga och beskrivande namn som gör det lätt att förstå syftet.

6.3 Chattar

Chattar i Teams ska hanteras utifrån innehåll och sammanhang.

- Chattar mellan medarbetare inom Mittuniversitetet räknas i de flesta fall inte som allmänna handlingar.
- För sådana chattar ska GDPR beaktas, och de ska rensas eller raderas när de inte längre behövs.
- Chattar mellan medarbetare och externa deltagare är i regel allmänna handlingar och ska hanteras enligt informationshanteringsplanen.
- Chattar som behöver bevaras bör dokumenteras i en tjänsteanteckning innan de gallras ur Teams.

6.4 Kanalmeddelanden

- Kanalmeddelanden i interna team räknas i de flesta fall inte som allmänna handlingar.
- För sådana meddelanden ska GDPR beaktas, och de ska rensas eller raderas när de inte längre behövs.
- Kanalmeddelanden i externa team är i regel allmänna handlingar och ska hanteras enligt informationshanteringsplanen.
- Meddelanden som ska bevaras bör dokumenteras i en tjänsteanteckning innan de gallras ur Teams.

6.5 Filer i Teams och SharePoint

Filer som lagras i team och SharePoint kan vara både allmänna handlingar och sådant arbetsmaterial som inte är allmän handling. Innehållet ska därför bedömas och hanteras enligt gällande regelverk.

6.6 Extern delning

Extern delning av filer, mappar och arbetsytor i Teams, SharePoint och OneDrive får endast ske när det är verksamhetsmässigt motiverat och i enlighet med gällande informationssäkerhetsregler.

6.7 Mötesinspelningar, transkribering och sammanfattningar

Mötesinspelningar, transkriberingar och automatiska sammanfattningar ska hanteras med samma omsorg som annan information i M365. Den som ansvarar för mötet ska bedöma om inspelning eller transkribering är nödvändig, samt säkerställa att materialet hanteras enligt gällande regelverk och informationshanteringsplan. Mötesinspelningar ska gallras två år efter mötestillfället. För möten med externa deltagare kan bevarande bli aktuellt om inspelningen bedöms ha värde för forskningen eller har rönt stor uppmärksamhet.

7 Särskilda riktlinjer för Outlook

Outlook används för e-post och kalenderhantering. E-post ska hanteras med samma omsorg som annan information.

- E-post ska inte användas som långtidsarkiv.
- E-postmeddelanden från externa avsändare eller till externa mottagare är i regel allmänna handlingar och ska hanteras enligt informationshanteringsplanen.
- E-post som skickas till eller tas emot från externa parter men som inte utgör allmän handling rensas eller raderas när det inte längre behövs.
- Internt e-postutbyte mellan medarbetare är i många fall inte allmän handling och kan rensas eller raderas när det inte längre behövs.
- För e-post som inte längre behövs ska GDPR-principerna om dataminimering och lagringsminimering beaktas.

8 Särskilda riktlinjer för OneDrive

OneDrive är en personlig lagringsyta för arbetsrelaterade filer.

- OneDrive ska användas för filer som är under arbete eller som inte ska lagras långsiktigt.
- OneDrive ska inte användas som arkiv.
- Handlingar som ska bevaras ska överföras till rätt verksamhetssystem eller lämnas till arkiv enligt fastställda rutiner.

9 Särskilda riktlinjer för Forms

Forms används för enkäter, omröstningar och enklare insamling av uppgifter.

Den som skapar ett formulär eller en enkät ansvarar för att bedöma hur länge formuläret, svaren och eventuella sammanställningar behöver bevaras. När syftet med enkäten är uppnått ska formuläret och tillhörande resultat raderas eller gallras enligt gällande informationshanteringsplan, om inte materialet ska bevaras i annat system eller överföras till arkiv.

9.1 Tillåten användning

Forms får användas för:

- enklare enkäter, utvärderingar och anmälningar
- insamling av uppgifter som inte är sekretessbelagda eller känsliga

Forms ska inte användas för:

- behandling av känsliga personuppgifter eller sekretessbelagd information
- insamling av uppgifter med högt skyddsvärde
- situationer där särskilda krav finns på säker lagring, spårbarhet eller långsiktigt bevarande

9.2 Personuppgifter och information till registrerade

Vid insamling av personuppgifter ska den som ansvarar för formuläret:

- säkerställa att det finns en tydlig information till den registrerade om hur uppgifterna behandlas
- endast samla in de uppgifter som är nödvändiga för ändamålet (uppgiftsminimering)
- undvika fritextfält om det finns risk att känsliga uppgifter lämnas

Om det finns behov av standardiserad informationstext ska denna tillhandahållas som mall eller rekommendation.

9.3 Ansvar och hantering av svar

Den som skapar ett formulär ansvarar för att:

- definiera syftet med insamlingen och säkerställa att uppgifterna används i enlighet med detta
- bedöma hur länge formuläret och svaren behöver sparas
- säkerställa att endast behöriga har tillgång till svaren
- vid behov exportera eller överföra information till rätt verksamhetssystem

9.4 Gallring och bevarande

Forms ska inte användas för långtidslagring eller arkivering.

När syftet med enkäten är uppnått ska:

- enkätfrågor, -svar och sammanställningar hanteras (bevaras eller gallras) enligt gällande informationshanteringsplan
- information som ska bevaras överföras till rätt system eller arkivfunktion

10 Användning av Microsoft Copilot

Mittuniversitetets medarbetare kan använda Microsoft Copilot i de delar av M365 där tjänsten är tillgänglig. Copilot är ett generativt AI-verktyg som kan användas för att söka information, analysera material, skapa utkast och förbättra texter.

När Copilot används via Mittuniversitetets inloggning ska samma krav på informationshantering gälla som i övriga M365-tjänster. Det innebär att användaren måste vara särskilt uppmärksam på vilken information som matas in i promptar.

10.1 Begränsningar vid användning av Copilot

- personuppgifter som tydligt identifierar en person,
- material som användaren inte har rätt att fritt förfoga över
- annat skyddsvärt material som inte bör delas i tjänsten

Medarbetaren ansvarar för att granska information som genereras av Copilot innan den används vidare.

11 Incidenter och avvikelsehantering

Om en medarbetare upptäcker eller misstänker att någon bryter mot dessa riktlinjer ska detta hanteras som en incident enligt Mittuniversitetets incidenthanteringsprocess (MIUN 2026/1729).

Systemägare eller ansvarig funktion får stänga ner eller ta bort grupper och team av driftsäkerhetsskäl eller om det finns befogad misstanke om brott mot universitetets ansvarsförbindelse eller interna regelverk.

Vid överträdelse kan även åtgärder vidtas enligt Mittuniversitetets ansvarsförbindelse.

12 Ansvar

Varje medarbetare ansvarar för att följa denna riktlinje, universitetets ansvarsförbindelse och övriga tillämpbara rutiner. Vid avslut av anställning ansvarar medarbetaren för att hantera information och handlingar enligt gällande informationshanteringsplan samt, vid behov, säkerställa att ägarskap för team eller andra arbetsytor överförs till annan behörig person.

13 Uppföljning

Systemförvaltningen för M365 kommer att löpande följa upp hur dessa riktlinjer efterlevs i de verktyg som ingår i M365.