



Kunnskap for en bedre verden

Fakultet for informasjonsteknologi og informatikk

INFT2504 Skytjenester som arbeidsflate (2024 HØST)

Oblig02

Høst, 30. oktober 2024

1. Del 1

Vi har bare lisens for 24 brukere, + en som er tildelt egen bruker: (admin@cire319.onmicrosoft.com som er [REDACTED]g)

Bedriftsstruktur (24 ansatte):

1. Ledelse (4 personer):	<ul style="list-style-type: none">○ CEO○ CTO○ CFO○ HR-sjef
2. Utviklingsavdeling (8 personer):	<ul style="list-style-type: none">○ 1 Utviklingsleder○ 3 Seniorutviklere○ 4 Juniorutviklere
3. Salg og Markedsføring (5 personer):	<ul style="list-style-type: none">○ 1 Salgs- og Markedsføringssjef
	<ul style="list-style-type: none">○ 2 Selgere○ 2 Markedsførere
4. Kundesupport (4 personer):	<ul style="list-style-type: none">○ 1 Supportsjef○ 3 Supportmedarbeidere
5. IT-drift (2 personer):	<ul style="list-style-type: none">○ 1 IT-sjef○ 1 IT-spesialist
6. Administrasjon (1 person):	<ul style="list-style-type: none">○ 1 Økonomiansvarlig

1.1 Opprett grupper i Microsoft Entra Admin Center

1. Gå til **Microsoft Entra Admin Center** (entra.microsoft.com).
2. I venstremenyen, velg **Grupper > Alle grupper**.
3. Klikk på **Ny gruppe**.
4. Velg **Gruppetype** som **Sikkerhetsgruppe** eller **Microsoft 365-gruppe**.
 - **Microsoft 365-grupper** gir en delingsinnboks og samarbeidsområde.
5. Gi gruppen et navn, for eksempel:
 - **Nyttech-Management** for CEO, CTO, CFO, HR-sjef
 - **DEP-Utvikling** for utviklingsleder, seniorutviklere, juniorutviklere.
6. Velg **Opprett** for å opprette gruppen. Gjenta dette for de resterende avdelingene.

Jeg brukte PowerShell til å automatisere opprettelsen av grupper. Dette effektiviserer prosessen ytterligere og sikrer konsistens mellom brukere og deres tilhørende grupper.

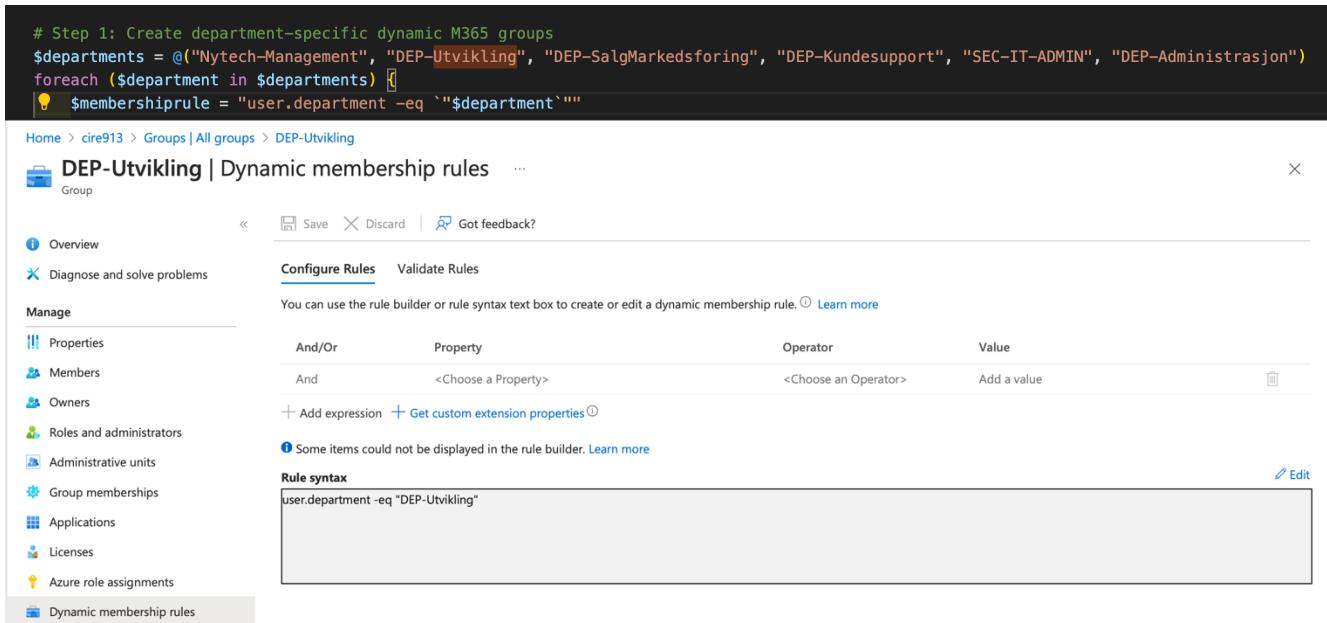
DisplayName	Id	MailNickname	Description	GroupTypes
Nyttech-Management	44a01dbd-36b0-472c-b76c-5b0655249fb5	Nyttech-Management	Gruppe for ansatte i avdelingen Nyttech-Management	{Unified, DynamicMembership}
DEP-Utvikling	751af4d1-8c58-4ddf-a23c-c0e6cea1ae22	DEP-Utvikling	Gruppe for ansatte i avdelingen DEP-Utvikling	{Unified, DynamicMembership}
DEP-SalgMarkedsf...	bdf5938a-096a-41dc-b8f6-f7eb8041f886	DEP-SalgMarkedsf...	Gruppe for ansatte i avdelingen DEP-SalgMarkedsf...	{Unified, DynamicMembership}
DEP-Kundesupport	f7263054-5850-4870-88a2-aa95f93147d0	DEP-Kundesupport	Gruppe for ansatte i avdelingen DEP-Kundesupport	{Unified, DynamicMembership}
SEC-IT-ADMIN	6849cbdf-b3c4-4916-b349-5531edb0e0b8	SEC-IT-ADMIN	Gruppe for ansatte i avdelingen SEC-IT-ADMIN	{Unified, DynamicMembership}
DEP-Administrasj...	396ae797-b2fd-4106-a71e-5a87edf44f45	DEP-Administrasj...	Gruppe for ansatte i avdelingen DEP-Administrasj...	{Unified, DynamicMembership}
0365-TEAM-Prodsa...	b6e009089-d994-4d37-9086-4c69de26f2b1	0365-TEAM-ProdSa...	Gruppe dedikert til samarbeid mellom produktutvilk...	{Unified, DynamicMembership}
0365-TEAM-Suppor...	91688cad-4de3-496a-9d87-c2cf171c3fe7	0365-TEAM-Suppor...	Gruppe for kommunikasjon og tilbakemelding mello...	{Unified, DynamicMembership}
0365-TEAM-SalgSu...	06411825-500a-4cca-aede-a/cb9/e814bd	0365-TEAM-SalgSu...	Gruppe for å styrke samarbeid rundt kundeoppfølg...	{Unified, DynamicMembership}
m365-license	9d3d764e-05e0-4537-860f-0830461703d5	m365-license	Members of this group will get a M365 license	{Unified, DynamicMembership}

<input type="checkbox"/>	 DA	DEP-Administrasjon	396ae797-b2fd-4106-a71e-5a87edf44f45	Microsoft 365	Dynamic	DEP-Administrasjon@cire319.onmicrosoft.com
<input type="checkbox"/>	 OK	DEP-Kundesupport	f7263054-5850-4870-88a2-aa95f93147d0	Microsoft 365	Dynamic	DEP-Kundesupport@cire319.onmicrosoft.com
<input type="checkbox"/>	 DS	DEP-SalgMarkedsforing	bdf5938a-096a-41dc-b8f6-f7eb8041f886	Microsoft 365	Dynamic	DEP-SalgMarkedsforing@cire319.onmicrosoft.co
<input type="checkbox"/>	 DU	DEP-Utvikling	751af4d1-8c58-4ddf-a23c-c0e6cea1ae22	Microsoft 365	Dynamic	DEP-Utvikling@cire319.onmicrosoft.com
<input type="checkbox"/>	 ml	m365-license	9d3d764e-05e0-4537-860f-0830461703d5	Microsoft 365	Dynamic	m365-license@cire319.onmicrosoft.com
<input type="checkbox"/>	 NM	Nytech-Management	44a01dbd-36b0-472c-b76c-5b0655249fb5	Microsoft 365	Dynamic	Nytech-Management@cire319.onmicrosoft.com
<input type="checkbox"/>	 OT	O365-TEAM-ProdSalg	b6e09089-d994-4d37-9086-4c69de26f2b1	Microsoft 365	Dynamic	O365-TEAM-ProdSalg@cire319.onmicrosoft.com
<input type="checkbox"/>	 OT	O365-TEAM-SalgSupport	06411825-500a-4cca-aede-a7cb97e814bd	Microsoft 365	Dynamic	O365-TEAM-SalgSupport@cire319.onmicrosoft.com
<input type="checkbox"/>	 O	O365-TEAM-SupportDev	91688cad-4de3-496a-9d87-c2cf171c3fe7	Microsoft 365	Dynamic	O365-TEAM-SupportDev@cire319.onmicrosoft.com
<input type="checkbox"/>	 SI	SEC-IT-ADMIN	6849cbdf-b3c4-4916-b349-5531edb0e0b8	Microsoft 365	Dynamic	SEC-IT-ADMIN@cire319.onmicrosoft.com

1.2 Konfigurer dynamisk gruppertildeling

1. Gå til Microsoft Entra Admin Center.
2. Velg **Grupper** > **Alle grupper** og åpne **Utviklingsavdeling**-gruppen.
3. Klikk på **Innstillinger** > **Egenskaper** og velg **Dynamisk medlemskap**.
4. Lag en regel som automatisk legger til brukere i utviklingsavdelingen. Klikk på **Legg til dynamisk medlemskapsregel**.
5. Definer medlemskapsregelen basert på et attributt som **Avdeling**:
 - o **Regel:** (user.department -eq "DEP-Utvikling")
6. Klikk på **Lagre** for å aktivere den dynamiske medlemskapsregelen.

Jeg brukte PowerShell til å automatisere opprettelsen av alle gruppene, inkludert et spesifikt eksempel på gruppen DEP-Utvikling som vist nedenfor. Dette eksempelet illustrerer hvordan hver gruppe er konfigurert automatisk, noe som sparar tid og sikrer nøyaktighet i oppsettet.



The screenshot shows the Microsoft Entra Admin Center interface for managing group membership rules. On the left, there's a navigation sidebar with options like Overview, Diagnose and solve problems, Manage (Properties, Members, Owners, Roles and administrators, Administrative units, Group memberships, Applications, Licenses, Azure role assignments), and Dynamic membership rules (which is currently selected).

The main area displays the configuration for the 'DEP-Utvikling' group. It shows a 'Configure Rules' section with a table for defining membership rules. One rule is defined: 'user.department -eq "DEP-Utvikling"'. Below the table, there's a 'Rule syntax' box containing the same expression.

```
# Step 1: Create department-specific dynamic M365 groups
$departments = @("Nytech-Management", "DEP-Utvikling", "DEP-SalgMarkedsforing", "DEP-Kundesupport", "SEC-IT-ADMIN", "DEP-Administrasjon")
foreach ($department in $departments) {
    $membershiprule = "user.department -eq `'$department`'"
}
```

1.3 Sett opp lisensiering via gruppetilhørighet

Jeg har brukt PowerShell fra tidligere (1.1) til å automatisere opprettelsen av alle gruppene, inkludert **m365-license** gruppe.

```
# Step 3: Create an additional group for license assignment
$Params = @{
    DisplayName = "m365-license"
    Description = "Members of this group will get a M365 license"
    MailEnabled = $false
    MailNickname = "m365-license"
    SecurityEnabled = $true
    GroupTypes = @("Unified", "DynamicMembership") # Make it a dynamic group
    MembershipRule = "(user.accountEnabled -eq $true)" # Rule to include all active users
    MembershipRuleProcessingState = "On"
}
New-MgGroup @Params
```

1. Fortsatt i **Microsoft Entra Admin Center**, velg **Lisensiering > Alle produkter**.
2. Velg lisensen du vil tilordne (f.eks., **Microsoft 365 Business Premium**).
3. Klikk på **Tildel > Velg grupper** og velg gruppen du vil tildele lisensen til, for eksempel **m365-license**.
4. Velg hvilke tjenester som skal aktiveres for gruppen.
5. Klikk **Tildel** for å bekrefte. Alle brukere i gruppen vil automatisk motta lisensen.

Home > Licenses > License details

[Back to Licenses](#)

Microsoft 365 Business Premium

You own at least 1 subscription for this product. [Manage subscription details](#)

Licenses

Licenses assigned 1/25


[Users](#) [Groups](#)

Assign and manage group licenses. [Learn how to assign licenses to groups.](#)

[+ Assign licenses](#) [⟳ Refresh](#)

<input type="checkbox"/>	Name ↑	Status
<input type="checkbox"/>	m365-license	:  All licenses assigned

1.4 Opprett brukere i Microsoft 365 Admin Center

1. Gå til **Microsoft 365 Admin Center** (admin.microsoft.com).
2. I navigasjonsmenyen til venstre, velg **Brukere > Aktive brukere**.
3. Klikk på **Legg til en bruker**.
4. Fyll ut informasjon om hver ansatt basert på organisasjonsstrukturen (for eksempel navn, e-post, avdeling).
5. Tildel nødvendige **roller** for brukere, som:
 - o **Administratorroller** (IT-sjef som global administrator eller andre administratorroller for tilgang til adminverktøy).
6. Velg **Opprett** for å legge til brukeren. Gjenta dette for alle 24 ansatte, samt administratorbruken.

For å unngå den tidkrevende prosessen med å manuelt opprette alle brukerkontoer og tilhørende grupper i Microsoft 365 Admin Center, har jeg valgt å bruke PowerShell-verktøyet for å automatisere oppsettet. Jeg opprettet en CSV-fil for å lagre kontoinformasjon, samt to separate PowerShell-skript for å opprette henholdsvis brukere. Dette gjør prosessen raskere og mer effektiv.

Som du så i avsnitt 1.3 ovenfor opprettet jeg en egen gruppe for å sette opp lisensiering via gruppetilhørighet, så her når alle medlemmer av denne gruppen automatisk blir tildelt en lisens gjennom medlemskapet deres (merk at det tar noen minutter å bli aktiv og lisenser må være tilgjengelig).

PS /Users/ericphung/Desktop/m365_oblig2> get-Mguser			
DisplayName	Id	Mail	UserPrincipalName
Nga Van Phung	6d024bf1-0b23-4da8-b584-a5defced89ed	admin@cire319.onmicrosoft.com	admin@cire319.onmicrosoft.com
Astrid Evjen	592618e5-c837-475b-8230-544c038aa0d4	Astrid.Evjen@cire319.onmicrosoft.com	Astrid.Evjen@cire319.onmicrosoft.com
Bente Gundersen	b6801971-eef1-4e9f-afd6-505d9a6ee28e	Bente.Gundersen@cire319.onmicrosoft.com	Bente.Gundersen@cire319.onmicrosoft.com
Dagfinn Warholm	c32da487-5192-45a7-9af0-9b0ca8858710	Dagfinn.Warholm@cire319.onmicrosoft.com	Dagfinn.Warholm@cire319.onmicrosoft.com
Daniel Thorsen	f2bd9873-e482-4937-b6e3-b6ef75294c1f	Daniel.Thorsen@cire319.onmicrosoft.com	Daniel.Thorsen@cire319.onmicrosoft.com
Emilie Lien	4618a8bb-1177-4927-98f8-3b5bc72af392	Emilie.Lien@cire319.onmicrosoft.com	Emilie.Lien@cire319.onmicrosoft.com
Geir Wang	2561aec2-007-4e02-97b5-9f657d1ea64	Geir.Wang@cire319.onmicrosoft.com	Geir.Wang@cire319.onmicrosoft.com
Gjermund Haugen	de2c1738-9c12-4a93-8bee-86319c446b07	Gjermund.Haugen@cire319.onmicrosoft.com	Gjermund.Haugen@cire319.onmicrosoft.com
Ivar Martinsen	fe9b20a7-006c-42e8-8431-0666e45b3c0b	Ivar.Martinsen@cire319.onmicrosoft.com	Ivar.Martinsen@cire319.onmicrosoft.com
Jan Eide	9ac89efc-bcff-4388-8f8f-e05d3ef5a579	Jan.Eide@cire319.onmicrosoft.com	Jan.Eide@cire319.onmicrosoft.com
Johan Karlsen	dd4512ce-1935-40c0-a434-d6d5b46e442b	Johan.Karlsen@cire319.onmicrosoft.com	Johan.Karlsen@cire319.onmicrosoft.com
Jonas Skott	881d93d6-6811-4862-a4ca-8af551c09c6a	Jonas.Skott@cire319.onmicrosoft.com	Jonas.Skott@cire319.onmicrosoft.com
Kari Fretheim	562ecd2b-e73a-4b97-9a9f-114e12b3ac83	Kari.Fretheim@cire319.onmicrosoft.com	Kari.Fretheim@cire319.onmicrosoft.com
Kjetil Riis	d4319992-e463-42d8-9d66-3a7c56432d0b	Kjetil.Riis@cire319.onmicrosoft.com	Kjetil.Riis@cire319.onmicrosoft.com
Kristian Haug	6bc9d893-1d1d-4189-b335-30c75721938b	Kristian.Haug@cire319.onmicrosoft.com	Kristian.Haug@cire319.onmicrosoft.com
Lars Bentzen	bb719c3b-f101-4693-87b6-58229c1e4b69	Lars.Bentzen@cire319.onmicrosoft.com	Lars.Bentzen@cire319.onmicrosoft.com
Maren Moe	0bdc8fc3-2b88-4147-ac56-4882ec1251df	Maren.Moe@cire319.onmicrosoft.com	Maren.Moe@cire319.onmicrosoft.com
Markus Medby	f36b8725-27af-44de-8d28-9083208d7116	Markus.Medby@cire319.onmicrosoft.com	Markus.Medby@cire319.onmicrosoft.com
Mikkel Hansen	a71b9003-767b-4327-ab61-7ec31e74c564	Mikkel.Hansen@cire319.onmicrosoft.com	Mikkel.Hansen@cire319.onmicrosoft.com
Nina Pedersen	3a0d4ae6-5346-4b74-a9f2-01314736a9a6	Nina.Pedersen@cire319.onmicrosoft.com	Nina.Pedersen@cire319.onmicrosoft.com
Petra Alver	93fcfd0f9-c798-4b60-95e7-05295c3b5b31	Petra.Alver@cire319.onmicrosoft.com	Petra.Alver@cire319.onmicrosoft.com
Rikard Berg	9c214e98-8eb6-4709-9787-6853934a5bfd	Rikard.Berg@cire319.onmicrosoft.com	Rikard.Berg@cire319.onmicrosoft.com
Rolf Pedersen	97e1a3e9-c4a2-4f7f-b2b5-b67ce23874a7	Rolf.Pedersen@cire319.onmicrosoft.com	Rolf.Pedersen@cire319.onmicrosoft.com
Siri Moen	f9b76b66-d1f4-4e44-9c1b-312a18e2595e	Siri.Moen@cire319.onmicrosoft.com	Siri.Moen@cire319.onmicrosoft.com
Stian Ytreland	1546c573-bb9c-41cc-a50f-c175ea43d3d4	Stian.Ytreland@cire319.onmicrosoft.com	Stian.Ytreland@cire319.onmicrosoft.com

Active users

Recommended actions (1)			
	Display name ↑	Username	Licenses
<input type="checkbox"/>	Astrid Evjen	Astrid.Evjen@cire319.onmicrosoft.com	Microsoft 365 Business Premium
<input type="checkbox"/>	Bente Gundersen	Bente.Gundersen@cire319.onmicrosoft.com	Microsoft 365 Business Premium
<input type="checkbox"/>	Dagfinn Warholm	Dagfinn.Warholm@cire319.onmicrosoft.com	Microsoft 365 Business Premium
<input type="checkbox"/>	Daniel Thorsen	Daniel.Thorsen@cire319.onmicrosoft.com	Microsoft 365 Business Premium
<input type="checkbox"/>	Emilie Lien	Emilie.Lien@cire319.onmicrosoft.com	Microsoft 365 Business Premium
<input type="checkbox"/>	Geir Wang	Geir.Wang@cire319.onmicrosoft.com	Microsoft 365 Business Premium
<input type="checkbox"/>	Gjermund Haugen	Gjermund.Haugen@cire319.onmicrosoft.com	Microsoft 365 Business Premium
<input type="checkbox"/>	Ivar Martinsen	Ivar.Martinsen@cire319.onmicrosoft.com	Microsoft 365 Business Premium
<input type="checkbox"/>	Jan Eide	Jan.Eide@cire319.onmicrosoft.com	Microsoft 365 Business Premium
<input type="checkbox"/>	Johan Karlsen	Johan.Karlsen@cire319.onmicrosoft.com	Microsoft 365 Business Premium

1.5 Legg til en gjestebruker for samarbeid med eksterne partnere

1. Gå til **Microsoft Entra Admin Center > Brukere > Alle brukere**.
2. Klikk **Ny gjestebruker** og skriv inn e-postadressen til gjesten (f.eks. en e-post fra en samarbeidspartner).
3. Under **Oppgaveinformasjon**, legg til roller og tilordne tillatelser basert på prosjektbehov.
4. Gå til **Microsoft Teams eller SharePoint i Microsoft 365 Admin Center** for å legge gjesten til en spesifikk kanal eller dokumentmappe.
 - o For eksempel kan du gi tilgang til en delt mappe på SharePoint som er relevant for det aktuelle prosjektet.
5. Klikk **Inviter**. Gjestebrukeren vil få en invitasjon på e-post.

Home > cire913 > Groups | All groups > DEP-Utvikling | Dynamic membership rules > Groups | All groups > Nytech-Management > Groups | All groups >

Users						
cire913						
New user Delete Download users Bulk operations Refresh Manage view Per-user MFA Got feedback?						
(i) Azure Active Directory is now Microsoft Entra ID						
Search	Add	26 users found (1 user selected)	User principal name ↑	User type	On-premises sy...	Identities
<input type="checkbox"/>	Astrid Evjen	Astrid.Evjen@cire319.onmicrosoft.com		Member	No	cire319.onmicrosoft.com
<input type="checkbox"/>	Bente Gundersen	Bente.Gundersen@cire319.onmicrosoft.com		Member	No	cire319.onmicrosoft.com
<input type="checkbox"/>	Dagfinn Warholm	Dagfinn.Warholm@cire319.onmicrosoft.com		Member	No	cire319.onmicrosoft.com
<input type="checkbox"/>	Daniel Thorsen	Daniel.Thorsen@cire319.onmicrosoft.com		Member	No	cire319.onmicrosoft.com
<input type="checkbox"/>	Emilie Lien	Emilie.Lien@cire319.onmicrosoft.com		Member	No	cire319.onmicrosoft.com
<input checked="" type="checkbox"/>	External Auditor	vanna1129_gmail.com#EXT#@cire319.onmicrosoft.com		Guest	No	cire319.onmicrosoft.com
<input type="checkbox"/>	Geir Wang	Geir.Wang@cire319.onmicrosoft.com		Member	No	cire319.onmicrosoft.com

Nga Van Phung invited you to access applications within their organization ➤ [Inbox](#)

 Microsoft Invitations on behalf of cire913 <invites@microsoft.com>
to me ▾

7:44 PM (2 minutes ago)    

 Please only act on this email if you trust the individual and organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. If you were not expecting this invitation, proceed with caution.

Sender: Nga Van Phung (admin@cire319.onmicrosoft.com)
Organization: cire913
Domain: cire319.onmicrosoft.com

If you accept this invitation, you'll be sent to <https://myapplications.microsoft.com/?tenantid=177268c0-3a24-40cb-85e7-d0264b394b27>.

[Accept invitation](#)

2. Del 2

2.1 Konfigurer brukerpostbokser for alle ansatte

1. Logg inn på Microsoft 365 Admin Center.
2. Gå til Brukere > Aktive brukere.
3. Velg hver bruker, eller opprett nye brukere som trengs for å sette opp postboksene.
4. **Bruk navnekonvensjon:** Sørg for at hver brukers e-postadresse følger en konsistent navnekonvensjon, som fornavn.etternavn@nytech.com.
5. Microsoft 365 oppretter automatisk en postboks for hver bruker som tildeles en lisens.

Her ble det faktisk opprettet brukerpostbokser for alle ansatte automatisk fra å kjøre skriptet i avsnitt 1.3 og 1.4 ovenfor. Du kan se skriptet jeg brukte til å opprette grupper, tildele lisenser og opprette brukere i avsnitt 4.2 og 4.3 nedenfor.

DisplayName	Mail
Nga Van Phung	admin@cire319.onmicrosoft.com
Astrid Evjen	Astrid.Evjen@cire319.onmicrosoft.com
Bente Gundersen	Bente.Gundersen@cire319.onmicrosoft.com
Dagfinn Warholm	Dagfinn.Warholm@cire319.onmicrosoft.com
Daniel Thorsen	Daniel.Thorsen@cire319.onmicrosoft.com
Emilie Lien	Emilie.Lien@cire319.onmicrosoft.com
Geir Wang	Geir.Wang@cire319.onmicrosoft.com
Gjermund Haugen	Gjermund.Haugen@cire319.onmicrosoft.com
Ivar Martinsen	Ivar.Martinsen@cire319.onmicrosoft.com
Jan Eide	Jan.Eide@cire319.onmicrosoft.com
Johan Karlsen	Johan.Karlsen@cire319.onmicrosoft.com
Jonas Skott	Jonas.Skott@cire319.onmicrosoft.com
Karl Fretheim	Karl.Fretheim@cire319.onmicrosoft.com
Kjetil Ris	Kjetil.Ris@cire319.onmicrosoft.com
Kristian Haug	Kristian.Haug@cire319.onmicrosoft.com
Lars Bentzen	Lars.Bentzen@cire319.onmicrosoft.com
Maren Moe	Maren.Moe@cire319.onmicrosoft.com
Markus Medby	Markus.Medby@cire319.onmicrosoft.com
Mikkel Hansen	Mikkel.Hansen@cire319.onmicrosoft.com
Nina Pedersen	Nina.Pedersen@cire319.onmicrosoft.com
Petra Alver	Petra.Alver@cire319.onmicrosoft.com
Rikard Berg	Rikard.Berg@cire319.onmicrosoft.com
Rolf Pedersen	Rolf.Pedersen@cire319.onmicrosoft.com
Siri Moen	Siri.Moen@cire319.onmicrosoft.com
Stian Ytreland	Stian.Ytreland@cire319.onmicrosoft.com
External Auditor	vannnga129@gmail.com

2.2 Opprett delte postbokser

1. Gå til **Exchange Admin Center (EAC)** via Microsoft 365 Admin Center.
2. Velg **Delte postbokser** i menyen.
3. Klikk på **Legg til delt postboks** og fyll inn navn og e-postadresse, f.eks.:
 - o **support@nytech.com** for kundesupport.
 - o **sales@nytech.com** for salgs- og markedsføringsavdelingen.
4. Når du har opprettet de delte postboksene, gå til **Tillatelser** og gi riktig tilgang til teammedlemmer som trenger tilgang til disse postboksene.
5. Husk å gi medlemmer **Full Access** og eventuelt **Send As** eller **Send on behalf of**-tillatelser, avhengig av behov.

Manage mailboxes

Create and manage settings for shared mailboxes. You can also manage settings for user mailboxes, but to add or delete them you must go to the [Microsoft 365 admin center](#) and do this on the [active users](#) page. [Learn more about mailboxes](#)

Shared mailbox					Search
Display name ↑	Email address	Recipient type	Archive status	Last modified time	Choose columns
Kundesupport	support@cire319.onmicrosoft.com	SharedMailbox	None	10/30/2024, 7:59...	
SalgogMarkedsforing	sales@cire319.onmicrosoft.com	SharedMailbox	None	10/30/2024, 8:01...	

2.3 Konfigurer ressurspostbokser

1. Gå til **Exchange Admin Center (EAC)**.
2. Velg **Ressurser** og deretter **Rom og utstyr**.
3. Klikk på **Legg til rompostboks** og fyll inn detaljer:
 - o For møterommet: Bruk en beskrivende e-postadresse, som meetingrom1@nytech.com.
 - o For dronen: Opprett en ressurspostboks, f.eks. drone@nytech.com.
4. Under **Avansert innstilling** kan du definere regler for ressurser, som tilgjengelighet, automatisk bekreftelse av reservasjoner, og begrensninger.

Resources

Admins can manage two types of resources: room mailboxes and equipment mailboxes. Room mailboxes are assigned to a physical location, such as a conference room or auditorium. After an admin creates room mailboxes, users can reserve rooms by including them in meeting requests. Equipment mailboxes are assigned to resources that aren't location specific, such as a portable computers, projectors or company cars, allowing users to reserve them in meeting requests.

[Learn more about resources](#)

		+ Add a room resource	+ Add an equipment resource	Refresh	Export resources	2 items	Filter	Search	
Display name ↑	Email address	Type							
Bedriftens drone	drone@cire319.onmicrosoft.com	Equipment							
Møteroom	meetingrom1@cire319.onmicrosoft.com	Room							

2.4 Opprett Microsoft 365-grupper for samarbeid mellom avdelingene

Samme som seksjon 1.1 Opprettingsgrupper i Microsoft Entra Admin Center jeg hå gjort men her for tverrfaglig samarbeid kan du opprette grupper som inkluderer medlemmer fra ulike avdelinger:

- Eksempel: Opprett en gruppe som heter Tverrfaglig Prosjektteam som inkluderer medlemmer fra utvikling, salg og kundesupport.

Men her har jeg delt det inn i 3 små grupper som dette:

```
PS /Users/ericphung/Desktop/m365_oblig2> Get-MgGroup | Where-Object { $_.DisplayName -like "0365-TEAM*" } | Select-Object DisplayName, Description
DisplayName          Description
-----              -----
0365-TEAM-SalgSupport Gruppe for å styrke samarbeid rundt kundeoppfølging og salgssupport.
0365-TEAM-SupportDev Gruppe for kommunikasjon og tilbakemelding mellom support og utviklere for å forbedre produkter.
0365-TEAM-ProdSalg   Gruppe dedikert til samarbeid mellom produktutvikling og salg.
```

Dette oppsettet vil nå opprette gruppene med de dynamiske medlemskap reglene, og medlemmer fra de angitte avdelingene vil automatisk bli lagt til gruppene.

```

# Step 2: Create cross-functional collaboration groups with corrected dynamic membership rules
$crossFunctionalGroups = @(
    @{
        DisplayName = "O365-TEAM-ProdSalg"
        Description = "Gruppe dedikert til samarbeid mellom produktutvikling og salg."
        MembershipRule = "(user.department -eq `\"DEP-Utvikling`") -or (user.department -eq `\"DEP-SalgMarkedsforing`\")"
    },
    @{
        DisplayName = "O365-TEAM-SupportDev"
        Description = "Gruppe for kommunikasjon og tilbakemelding mellom support og utviklere for å forbedre produkter."
        MembershipRule = "(user.department -eq `\"DEP-Kundesupport`\") -or (user.department -eq `\"DEP-Utvikling`\")"
    },
    @{
        DisplayName = "O365-TEAM-SalgSupport"
        Description = "Gruppe for å styrke samarbeid rundt kundeoppfølging og salgssupport."
        MembershipRule = "(user.department -eq `\"DEP-SalgMarkedsforing`\") -or (user.department -eq `\"DEP-Kundesupport`\")"
    }
)

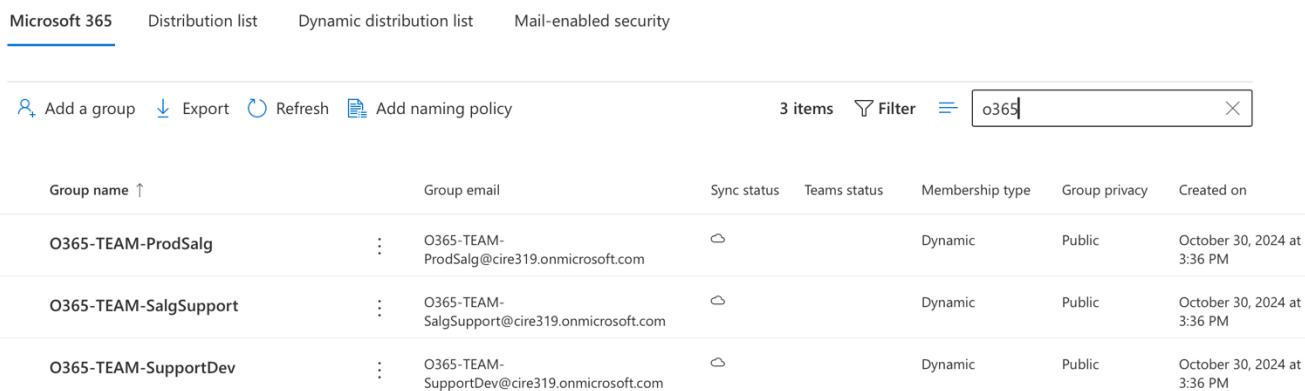
foreach ($group in $crossFunctionalGroups) {
    $Params = @{
        DisplayName = $group.DisplayName
        Description = $group.Description
        MailEnabled = $false
        MailNickname = $group.DisplayName -replace ' ', ''
        SecurityEnabled = $true
        GroupTypes = @("Unified", "DynamicMembership")
        MembershipRule = $group.MembershipRule
        MembershipRuleProcessingState = "On"
    }
    New-MgGroup @Params
}

```

2.5 Konfigurer gruppepostbokser og SharePoint-område for prosjektteamet

- For gruppen **Tverrfaglig Prosjektteam**, sørk for at gruppepostboksen er satt opp slik at alle gruppemedlemmene kan se og bruke den.
- Gå til **SharePoint Admin Center**.
- Finn gruppen **Tverrfaglig Prosjektteam** som ble opprettet i Microsoft 365-grupper. Den har automatisk fått et eget SharePoint-område.
- Tilpass dette SharePoint-området til å inkludere mapper, dokumentbiblioteker og tilganger som støtter samarbeidsbehovene for prosjektteamet.
- Del SharePoint-området og gi nødvendige tillatelser til teammedlemmene.

Groups



The screenshot shows the Microsoft 365 Groups page. At the top, there are navigation links for 'Distribution list', 'Dynamic distribution list', and 'Mail-enabled security'. Below this is a toolbar with buttons for 'Add a group', 'Export', 'Refresh', 'Add naming policy', and a search bar containing 'o365'. The main area displays a table of groups:

Group name ↑	Group email	Sync status	Teams status	Membership type	Group privacy	Created on
O365-TEAM-ProdSalg	O365-TEAM-ProdSalg@cire319.onmicrosoft.com	Cloud	Dynamic	Dynamic	Public	October 30, 2024 at 3:36 PM
O365-TEAM-SalgSupport	O365-TEAM-SalgSupport@cire319.onmicrosoft.com	Cloud	Dynamic	Dynamic	Public	October 30, 2024 at 3:36 PM
O365-TEAM-SupportDev	O365-TEAM-SupportDev@cire319.onmicrosoft.com	Cloud	Dynamic	Dynamic	Public	October 30, 2024 at 3:36 PM

3. Del 3

Risikoprofil:

Avdeling	Risikoprofil	Kritiske sikkerhetsbehov
Ledelse	Tilgang til sensitiv strategisk informasjon; mål for BEC og phishing-angrep.	Anti-phishing, imitation protection, MFA, Conditional Access.
Utviklingsavdeling	Håndterer kildekode og intellektuell eiendom; høy risiko for datainnbrudd og tap av informasjon.	DLP, Safe Attachments, anti-phishing rettet mot utviklere.
Salg og Markedsføring	Kommuniserer med eksterne parter; utsatt for phishing, malware og risiko for datalekkasjer.	Safe Links, ATP, strenge policyer for håndtering av kundedata.
Kundesupport	Tilgang til kundedatabaser; risiko for sosial manipulering og håndtering av eksterne filer.	Safe Attachments, Safe Links, opplæring i sosial manipulering og phishing.
IT-drift	Full tilgang til infrastruktur; risiko for full systemkompromittering ved brudd.	MFA, PIM, Conditional Access.
Administrasjon	Håndterer finansiell informasjon; mål for svindel og økonomisk phishing.	Anti-phishing, DLP, beskyttelse mot BEC-angrep.

Tabell 5: Risikoprofil og kritiske sikkerhetsbehov

Forhåndsdefinerte sikkerhetspolicyer: Jeg har aktivert begge Strenge Preset Security Policies og Standard Preset Security Policies.

Built-in protection



Built-in Microsoft Office 365 security applied to all users in your organization to protect against malicious links and attachments.

- ✓ Additional machine learning models
- ✓ More aggressive detonation evaluation
- ✓ Visual indication in the experience

Note: Built-in protection is enabled only for paid Microsoft Defender for Office 365 tenants.

[Add exclusions \(Not recommended\)](#)

Standard protection



A baseline protection profile that protects against spam, phishing, and malware threats.

- ✓ Balanced actions for malicious content
- ✓ Balanced handling of bulk content
- ✓ Attachment and link protection with Safe Links and Safe Attachments

 Standard protection is on

[Manage protection settings](#)

Strict protection



A more aggressive protection profile for selected users, such as high value targets or priority users.

- ✓ More aggressive actions on malicious mail
- ✓ Tighter controls over bulk senders
- ✓ More aggressive machine learning

 Strict protection is on

[Manage protection settings](#)

Konfigurering:**Policies**

 Anti-phishing	Protect users from phishing attacks, and configure safety tips on suspicious messages.
 Anti-spam	Protect your organization's email from spam, including what actions to take if spam is detected
 Anti-malware	Protect your organization's email from malware, including what actions to take and who to notify if malware is detected
 Safe Attachments	Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams
 Safe Links	Protect your users from opening and sharing malicious links in email messages and Office apps

- Anti-phishing: Konfigurer en streng anti-phishing-policy som beskytter alle brukere, med ekstra beskyttelse for ledelsen.

Anti-phishing

By default, Microsoft 365 includes built-in features that help protect your users from phishing attacks. Set up anti-phishing policies to increase this protection. For example, you can refine the settings to better detect and prevent impersonation and spoofing attacks. The default policy applies to all users within the organization. You can create custom, higher priority policies for specific users, groups or domains. [Learn more about anti-phishing policies](#)

 0 impersonated domain(s) and user(s) over the past 7 days. View impersonations				
Create Export Refresh More actions ▾		1 of 4 selected		
<input type="checkbox"/> Name	Status	Priority	Last modified	 Search
<input type="checkbox"/> Strict Preset Security Policy	● On	--	Oct 31, 2024	 Filter ▾
<input type="checkbox"/> Standard Preset Security Policy	● On	--	Oct 31, 2024	
<input checked="" type="checkbox"/> first-anti-phising-policy	● On	0	Oct 31, 2024	
<input type="checkbox"/> Office365 AntiPhish Default (Default)	● Always on	Lowest	Oct 30, 2024	

- Safe Attachments: for alle brukere.

Safe attachments

Set up an safe attachments policy for specific users or groups to help prevent people from opening or sharing email attachments that contain malicious content. [Learn more about safe attachments for email](#)

<input type="checkbox"/>	Name	Status	Priority
<input type="checkbox"/>	Strict Preset Security Policy	● On	--
<input type="checkbox"/>	Standard Preset Security Policy	● On	--
<input checked="" type="checkbox"/>	First Safe Attachment Policy	● On	0
<input type="checkbox"/>	Built-in protection (Microsoft)	● On	Lowest

- Safe Links: for å beskytte brukere mot farlige URL-er.

Safe links

Safe Links helps prevent your users from following links in email and documents that go to web sites recognized as malicious. Use this page to set up policies that determine how all or specific users in your organization interact with Safe Links. [Learn more about Safe Links](#)

<input type="checkbox"/>	Name	Status	Priority
<input type="checkbox"/>	Strict Preset Security Policy	● On	--
<input type="checkbox"/>	Standard Preset Security Policy	● On	--
<input checked="" type="checkbox"/>	First Safe Link Policy	● On	0
<input type="checkbox"/>	Built-in protection (Microsoft)	● On	Lowest

- I tillegg har jeg også aktivert Anti-spam og Anti-malware policies.

Anti-spam policies

Use this page to configure policies that are included in anti-spam protection. These policies include connection filtering, spam filtering, and outbound spam filtering. [Learn more](#)

<input type="checkbox"/>	Name	Status	Priority	Type
<input type="checkbox"/>	Strict Preset Security Policy	● On	--	Protection templates
<input type="checkbox"/>	Standard Preset Security Policy	● On	--	Protection templates
<input type="checkbox"/>	First inbound anti-spam policy	● On	0	Custom anti-spam policy
<input type="checkbox"/>	First outbound anti-spam policy	● On	0	Custom outbound spam policy
<input type="checkbox"/>	Anti-spam inbound policy (Default)	● Always on	Lowest	
<input type="checkbox"/>	Connection filter policy (Default)	● Always on	Lowest	
<input type="checkbox"/>	Anti-spam outbound policy (Default)	● Always on	Lowest	

Anti-malware

1 of 4 selected			Search	≡	
Name	Status	Priority			
Strict Preset Security Policy	On	--			
Standard Preset Security Policy	On	--			
anti-malware-policy	On	0			
Default (Default)	Always on	Lowest			

Anti-Phishing og Anti-Spam regler for sensitive avdelinger: som inkluderer regler for å blokkere kjente phishing-domenenavn, og legge til imitasjonsbeskyttelse for ledelsen og utviklingsavdelingen.

Policies & rules > Threat policies > Anti-phishing

Anti-phishing

By default, Microsoft 365 includes built-in features that help protect your organization from phishing attacks. For example, you can refine the settings to better detect and protect users within the organization. You can create custom, higher priority policies.

0 impersonated domain(s) and user(s) over the past 7 days. [View impersonations](#)

+ Create Export Refresh More actions

Name	Status	Priority
Strict Preset Security Policy	On	--
Standard Preset Security Policy	On	--
first-anti-phising-policy	On	0
Office365 AntiPhish Default (Default)	Always on	Lowest

first-anti-phising-policy

Policy on | Priority 0 | Thu Oct 31 2024

Turn off Delete policy

Description

cire319 AS demo

Edit description

Users, groups, and domains

Included groups

Nytech-Management@cire319.onmicrosoft.com
DEP-Utvikling@cire319.onmicrosoft.com

Included recipient domains

cire319.onmicrosoft.com

Edit users, groups, and domains

Blokkere spesifikke typer vedlegg: legg til en blokkering for vedleggstyper som .exe, .bat, og andre skadelige filtyper som ofte brukes i phishing-angrep.

Policies & rules > Threat policies > Anti-malware

Anti-malware

+ Create ⏪ Export ⏴ Refresh ⋮ More actions

- Name
- Strict Preset Security Policy
- Standard Preset Security Policy
- anti-malware-policy
- Default (Default)

anti-malware-policy

- Policy on | Priority 0
- Turn off Delete policy

Enable the common attachments filter

- On

Customize file types

.ace, .apk, .app, .appx, .ani, .arj, .bat, .cab, .cmd, .com and 43 other file types

When these file types are found

Reject the message with a non-delivery receipt (NDR)

Enable zero-hour auto purge for malware (Recommended)

- On

Notify an admin about undelivered messages from internal senders

- Send notification to admin admin@cire319.onmicrosoft.com

Notify an admin about undelivered messages from external senders

- Off

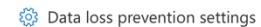
Customize notifications

- Off

Quarantine policy

Data Loss Prevention (DLP) polycer: å overvåke og blokkere sensitiv informasjon (som kildekode og finansielle data) fra å bli delt utenfor organisasjonen.

Policies



Use data loss prevention (DLP) policies to help identify and protect your organization's sensitive info. For example you can set up policies to help make sure information in email and docs isn't shared with the wrong people. [Learn more about DLP](#)

If your role group permissions are restricted to a specific set of users or groups, you'll only be able to manage policies for those users or groups. [Learn more about role group permissions.](#)

[View role groups](#)

+ Create policy ⏪ Export ⏴ Refresh 2 items Search Customize columns

<input type="checkbox"/> Name	Priority	Last modified	Status
<input type="checkbox"/> PCI Data Security Standard (PCI DSS)	0	Oct 31, 2024 7:56 PM	In simulation without notifications
<input type="checkbox"/> GDPR	1	Oct 31, 2024 7:58 PM	In simulation without notifications

Opprett minst to sensitivitetsetiketter: og jeg har også konfigurert en policy for automatisk merking av dokumenter som inneholder sensitive data, som kildekode eller kundeinformasjon:

Name	Priority	Created by	Last modified
<input type="checkbox"/> Strengt konfidensiell for cire319 AS	0 - lowest	Nga Van Phung	Oct 31, 2024 8:38 PM
<input type="checkbox"/> Intern bruk	1 - highest	Nga Van Phung	Oct 31, 2024 8:43 PM

Jeg hoppet over testdelen fordi testen ikke krevde det (selv om jeg testet det selv og det fungerte bra) så jeg skrev ikke om denne delen.

Videre ønsker jeg å implementere auto-merkeordninger for både HR-avdelingen og økonomiteamet. Dette vil sikre at relevante dokumenter automatisk merkes med riktig etikett basert på innhold og type sensitiv informasjon. Denne funksjonen vil bidra til korrekt håndtering av informasjon uten at ansatte må merke dokumentene manuelt.

Imidlertid har jeg mottatt informasjon om at auto-merking foreløpig ikke er tilgjengelig i alle regioner på grunn av en avhengighet til en backend-tjeneste i Azure. Jeg ønsker derfor å undersøke alternative løsninger eller midlertidige tiltak for å oppnå lignende funksjonalitet, inntil auto-merking blir tilgjengelig i vår region.

4. Del 4

For å automatisere opprettelsen av brukere og grupper ved hjelp av informasjon fra en CSV-fil, her er en optimalisert tilnærming som jeg har gjort:

- 1. Opprett en CSV-fil:**

givenName	surName	department	companynname	country	city	jobtitle
Mikkel	Hansen	Nytech-Management	NyTechAS	Norway	Trondheim	CEO
Markus	Medby	Nytech-Management	NyTechAS	Norway	Trondheim	CTO
Kristian	Haug	Nytech-Management	NyTechAS	Norway	Trondheim	CFO
Ivar	Martinsen	Nytech-Management	NyTechAS	Norway	Trondheim	HR-sjef
Maren	Moe	DEP-Utvikling	NyTechAS	Norway	Trondheim	Utviklingsleder
Geir	Wang	DEP-Utvikling	NyTechAS	Norway	Trondheim	Seniorutvikler
Kjetil	Riis	DEP-Utvikling	NyTechAS	Norway	Trondheim	Seniorutvikler
Johan	Karlsen	DEP-Utvikling	NyTechAS	Norway	Trondheim	Seniorutvikler
Dagfinn	Warholm	DEP-Utvikling	NyTechAS	Norway	Trondheim	Juniorutvikler
Gjermund	Haugen	DEP-Utvikling	NyTechAS	Norway	Trondheim	Juniorutvikler
Lars	Bentzen	DEP-Utvikling	NyTechAS	Norway	Trondheim	Juniorutvikler
Rolf	Pedersen	DEP-Utvikling	NyTechAS	Norway	Trondheim	Juniorutvikler
Stian	Ytreland	DEP-SalgMarkedsforing	NyTechAS	Norway	Trondheim	Salgs- og Markedsføringsjef
Petra	Alver	DEP-SalgMarkedsforing	NyTechAS	Norway	Trondheim	Selger
Kari	Fretheim	DEP-SalgMarkedsforing	NyTechAS	Norway	Trondheim	Selger
Nina	Pedersen	DEP-SalgMarkedsforing	NyTechAS	Norway	Trondheim	Markedsfører
Bente	Gundersen	DEP-SalgMarkedsforing	NyTechAS	Norway	Trondheim	Markedsfører
Siri	Moen	DEP-Kundesupport	NyTechAS	Norway	Trondheim	Supportsjef
Jan	Eide	DEP-Kundesupport	NyTechAS	Norway	Trondheim	Supportmedarbeider
Astrid	Evjen	DEP-Kundesupport	NyTechAS	Norway	Trondheim	Supportmedarbeider
Daniel	Thorsen	DEP-Kundesupport	NyTechAS	Norway	Trondheim	Supportmedarbeider
Jonas	Skott	SEC-IT-ADMIN	NyTechAS	Norway	Trondheim	IT-sjef
Rikard	Berg	SEC-IT-ADMIN	NyTechAS	Norway	Trondheim	IT-spesialist
Emilie	Lien	DEP-Administrasjon	NyTechAS	Norway	Trondheim	Økonomiansvarlig

2. **Script 1: for gruppeopprettelse** - Dette skriptet vil forhåndsopprette grupper basert på bedriftsstrukturen, samarbeidsteam og en lisensieringsgruppe. Det vil inkludere dynamiske medlemskapsregler for automatisk å legge til brukere i de riktige gruppene basert på deres avdeling.

```

# If you are already connected to your Tenant from the 01-01-ConnectMgGraph.ps1 script,
# you can skip the connection part in this script.
$TenantID = "177268c0-3a24-40cb-85e7-d0264b394b27"
Connect-MgGraph -TenantId $TenantID -Scopes "User.ReadWrite.All", "Group.ReadWrite.All", "Directory.ReadWrite.All",
                                         "RoleManagement.ReadWrite.Directory"

# Create groups
Get-Help New-MgGroup -Online

# Step 1: Create department-specific dynamic M365 groups
$departments = @("Nytech-Management", "DEP-Utvikling", "DEP-SalgMarkedsforing", "DEP-Kundesupport", "SEC-IT-ADMIN", "DEP-Administrasjon")
foreach ($department in $departments) {
    $membershiprule = "user.department -eq `"$department`""
    $Params = @{
        DisplayName = "$department"
        Description = "Gruppe for ansatte i avdelingen $department"
        MailEnabled = $true
        MailNickname = $department
        SecurityEnabled = $true
        GroupTypes = @("Unified", "DynamicMembership")
        MembershipRule = $membershiprule
        MembershipRuleProcessingState = "On"
    }
    New-MgGroup @Params
}

# Step 2: Create cross-functional collaboration groups with corrected dynamic membership rules
$crossFunctionalGroups = @{
    @{
        DisplayName = "O365-TEAM-ProdSalg"
        Description = "Gruppe dedikert til samarbeid mellom produktutvikling og salg."
        MembershipRule = "(user.department -eq `"DEP-Utvikling`") -or (user.department -eq `"DEP-SalgMarkedsforing`")"
    },
    @{
        DisplayName = "O365-TEAM-SupportDev"
        Description = "Gruppe for kommunikasjon og tilbakemelding mellom support og utviklere for å forbedre produkter."
        MembershipRule = "(user.department -eq `"DEP-Kundesupport`") -or (user.department -eq `"DEP-Utvikling`")"
    },
    @{
        DisplayName = "O365-TEAM-SalgSupport"
        Description = "Gruppe for å styrke samarbeid rundt kundeoppfølging og salgssupport."
        MembershipRule = "(user.department -eq `"DEP-SalgMarkedsforing`") -or (user.department -eq `"DEP-Kundesupport`")"
    }
}
foreach ($group in $crossFunctionalGroups) {
    $Params = @{
        DisplayName = $group.DisplayName
        Description = $group.Description
        MailEnabled = $false
        MailNickname = $group.DisplayName -replace ' ', ''
        SecurityEnabled = $true
        GroupTypes = @("Unified", "DynamicMembership")
        MembershipRule = $group.MembershipRule
        MembershipRuleProcessingState = "On"
    }
    New-MgGroup @Params
}

# Step 3: Create an additional group for license assignment
$Params = @{
    DisplayName = "m365-license"
    Description = "Members of this group will get a M365 license"
    MailEnabled = $false
    MailNickname = "m365-license"
    SecurityEnabled = $true
    GroupTypes = @("Unified", "DynamicMembership") # Make it a dynamic group
    MembershipRule = "(user.accountEnabled -eq $true)" # Rule to include all active users
    MembershipRuleProcessingState = "On"
}
New-MgGroup @Params

```

3. **Script 2: for brukerkontoopprettelse** - Dette skriptet vil opprette brukerkontoer, tilordne dem til riktig avdeling, tildele lisenser og bruke dynamiske medlemskapsregler for å legge dem til relevante grupper.

```
# If you are already connected to your Tenant from the 01-01-ConnectMgGraph.ps1 script,
# you can skip the connection part in this script.
$TenantID = "177268cb-3a24-40cb-85e7-d0264b394b27"
Connect-MgGraph -TenantId $TenantID -Scopes "User.ReadWrite.All", "Group.ReadWrite.All", "Directory.ReadWrite.All", "RoleManagement.ReadWrite.Directory"

# Create users
Get-Help New-MgUser -Online

$users = Import-Csv -Path '03-02-Users.csv' -Delimiter ","
$PasswordProfile = @{
    Password = 'sdfg_sa3SAs3_as3f!'
}

foreach ($user in $users) {
    $Params = @{
        UserPrincipalName = $user.givenName + "." + $user.surName + "@cire319.onmicrosoft.com"
        DisplayName = $user.givenName + " " + $user.surName
        GivenName = $user.givenName
        Surname = $user.surName
        MailNickname = $user.givenName + "." + $user.surName
        AccountEnabled = $true
        PasswordProfile = $PasswordProfile
        Department = $user.Department
        CompanyName = $user.CompanyName
        Country = $user.Country
        City = $user.City
        JobTitle = $user.JobTitle
    }
    $Params
    New-MgUser @Params
}

```

4. **Script 3:** Et fleksibelt script som finner mailboksene til M365 grupper og konfigurerer noen utvalgte brukere til å ha send as / Send on behalf of denne adressen:

```
# In this script we will see how we can manage mailboxes with PowerShell
# Checks if it is connected to Exchange Online
if ($null -eq (Get-Module -ListAvailable -Name ExchangeOnlineManagement)) {
    Write-Host "ExchangeOnlineManagement module not found. Installing..."
    Install-Module -Name ExchangeOnlineManagement -Force -AllowClobber
} else {
    Write-Host "ExchangeOnlineManagement module is already installed."
}

# Import the module
Import-Module ExchangeOnlineManagement

# Connect to Exchange Online
try {
    Connect-ExchangeOnline -ShowProgress $true
    Write-Host "Successfully connected to Exchange Online."
} catch {
    Write-Host "Error connecting to Exchange Online: $_"
}

# Gets all mailboxes
Get-EXOMailbox | Select-Object DisplayName,PrimarySmtpAddress

# Gets all M365 groups with mailboxes
Get-UnifiedGroup | Select-Object DisplayName,PrimarySmtpAddress

# Gets a specific M365 group mailbox
$m365Group = "DEP-Kundesupport"
Get-UnifiedGroup -Identity $m365Group | Select-Object DisplayName,PrimarySmtpAddress

# Puts the mailbox in a variable
$mailbox = Get-UnifiedGroup -Identity $m365Group
```

```

# Gets all members of the mailbox
Get-UnifiedGroupLinks -Identity $mailbox.Identity -LinkType Members |
    Get-Recipient |
        Select-Object DisplayName, PrimarySmtpAddress, RecipientType, Alias, Name |
            Format-Table -AutoSize

# Gets members permissions and send as permissions
Get-RecipientPermission -Identity $mailbox.Identity | Select-Object Trustee,AccessRights

# Adds members permissions and send as or send on behalf of permissions
$trustee = "Jonas.Skott@cire319.onmicrosoft.com"
Add-RecipientPermission -Identity $mailbox.Identity -AccessRights SendAs -Trustee $trustee -Confirm:$false

# Define trustees
[array] $trustees = "Jonas.Skott@cire319.onmicrosoft.com","Rikard.Berg@cire319.onmicrosoft.com"

# Grant send on behalf of permissions
Set-UnifiedGroup -Identity $mailbox.Identity -GrantSendOnBehalfTo $trustees

# Get current permissions of the mailbox
$currentTrustees = (Get-UnifiedGroup -Identity $mailbox.Identity).GrantSendOnBehalfTo
# Loops through the current trustees and gets the primary smtp address and display name
Write-Host "Send on behalf granted to: " -ForegroundColor Yellow
foreach ($currentTrustee in $currentTrustees) {
    $currentTrusteeRecipient = Get-Recipient -Identity $currentTrustee
    Write-Host "Name: $($currentTrusteeRecipient.DisplayName) - SMTP: $($currentTrusteeRecipient.PrimarySmtpAddress) - ID: $($currentTrusteeRecipient.Id)"
}

# Verify the final permissions (Shows only the ID)
Get-UnifiedGroup -Identity $mailbox.Identity | Select-Object GrantSendOnBehalfTo

# Gets all distribution groups
Get-DistributionGroup | Select-Object DisplayName,PrimarySmtpAddress

# Gets all dynamic distribution groups
Get-DynamicDistributionGroup | Select-Object DisplayName,PrimarySmtpAddress

```

Refleksjonsnotat:

Læring og erfaringer: jeg fikk bedre forståelse for Microsoft 365-funksjoner og viktigheten av testing i automatiserte prosesser.

Utfordringer	Løsninger
Dynamiske grupper: Tidkrevende å sette opp riktige regler.	Automatisert med PowerShell-skript for effektivitet og nøyaktighet.
Tilpasning av sikkerhetspolicyer: Krevde justeringer for å møte spesifikke risikoer.	Brukte Microsoft Defender Configuration Analyzer for å identifisere og implementere forbedringer.
PowerShell-skript: Kompleksitet i utvikling og testing.	Grundig testing og detaljerte kommentarer for å sikre korrekt funksjon.

Forbedringer	Beskrivelse
Bedre dokumentasjon	Utvikle en håndbok for NyTechs IT-avdeling for bruk og vedlikehold av PowerShell-skript.
Flere sensitivitetsmerker	Opprette flere sensitivitetsnivåer for bedre kontroll over sensitiv informasjon.
Ekstra automatiseringsløsninger	Utvide PowerShell-skript for rutineoppgaver som rettighetsgjennomgang og lisensstatus.

Referanseliste

Fra fagets pensum:

- Uke 34: 01-ssa-introduksjon.pdf, 02-ssa-abonnement-lisenser.pdf
- Uke 35: 03-ssa-IdentityAccessManagement.pdf, 04-ssa-EnOrganisasjoniSkyen.pdf
- Uke 36: 05-ssa-exchange.pdf
- Uke 37: 05-ssa-exchange security.pdf
- Uke 39: 06-ssa-exchange-rules.pdf, 00-Initiere_Org-Configu-M365-ExchangeOnline.pdf
- Uke 40: 07-ssa-compliance.pdf, 07-ssa-Introduksjon-powershell.pdf
- Uke 42: 08-ssa-m365-powershell.pdf

Filene fra Blackboard of INFT2504 Skytjenester som arbeidsflate (2024 HØST):

- PDF_01-Enable standard security policies EOP.pdf
- PDF_02-Create anti-malware policy EOP.pdf
- PDF_03-Creating Anti-Phishing Policy EOP.pdf
- PDF_04 Create Inbound Anti-Spam Policy EOP.pdf
- PDF_05-Create Outbound Anti-Spam Policy.pdf
- PDF_06-Create Safe Attachments Policy.pdf
- PDF_07-Create Safe Links Policy.pdf
- PDF_08-Configuration Analyzer.pdf

Ytterligere referanser for å opprette grupper og kontoer:

- <https://github.com/torivarm/m365/tree/main>
- <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.groups/new-mggroup?view=graph-powershell-1.0>
- <https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.users/new-mguser?view=graph-powershell-1.0>