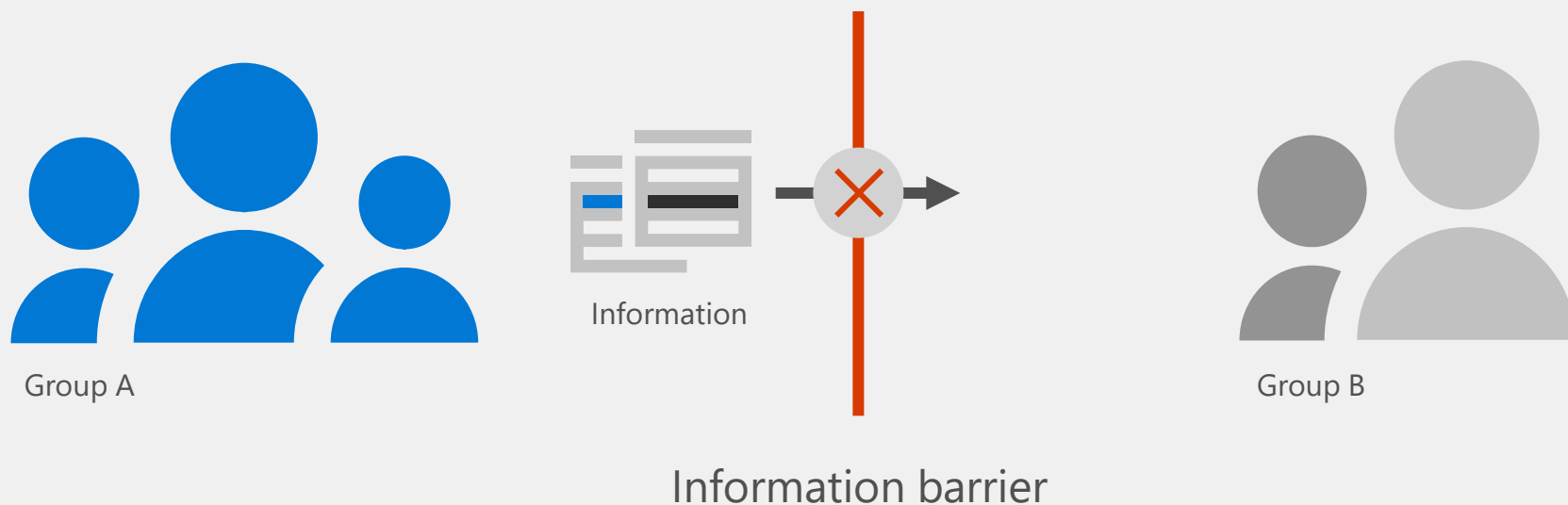# Information barriers

Suppose that you want to restrict communications between two groups to avoid a conflict of interest from occurring in your organization. Or, perhaps you want to restrict communications between certain people inside your organization in order to safeguard internal information. You can use an information barrier to restrict communications among specific groups of users when necessary.

Group A

Information

Group B

Information barrier

Common scenarios

You can define information barrier policies to prevent or allow communications in Microsoft Teams.

With information barrier policies in effect, whenever users who are covered by those policies attempt to communicate with others in Microsoft Teams, checks are done to prevent (or allow) communication (as defined by information barrier policies).
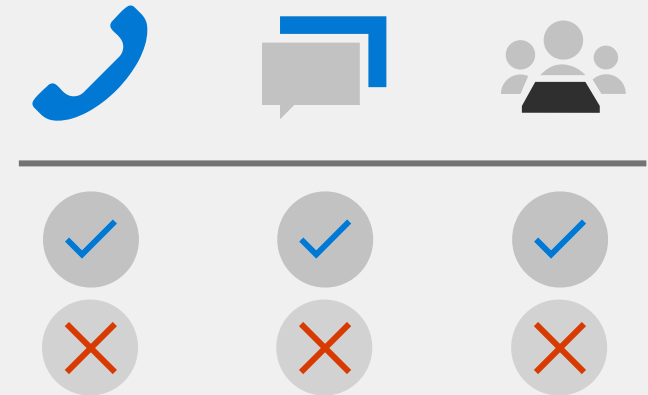
Common scenarios

For example, you could set up policies so that:

1 A day trader cannot call someone on the marketing team.

Marketing group

Day trader

Common scenarios

2 Finance personnel working on confidential company information cannot receive calls from certain groups within their organization

Finance personnel with confidential information

Specific groups

Common scenarios

3 An internal team with trade secret material cannot call or chat online with people in certain groups within their organization
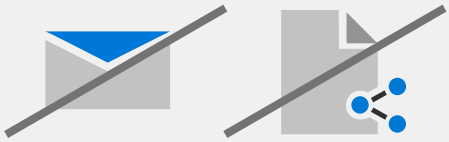
Team with trade secret material

Specific groups

Common scenarios

4 A research team can only call or chat online with a product development team

Product development team

Research team
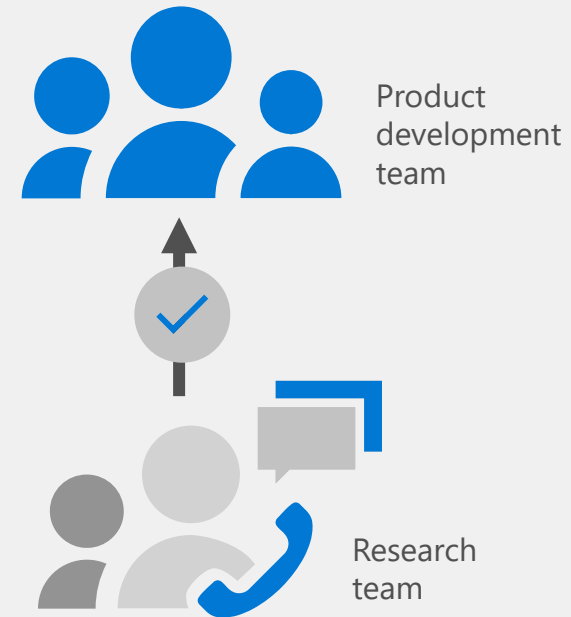
Technical details...

- Currently, information barriers do not apply to email communications or to file sharing through SharePoint Online or OneDrive.

- In addition, information barriers are independent from **compliance boundaries**.

- Before you define and apply information barrier policies, make sure your organization does not have **Exchange address book policies** in effect. (Information barriers are based on address book policies.)

What happens with information barriers

With information barriers, checks are in place to prevent unauthorized communication. This can take the following forms:

Can block activities	Can block all communication with Microsoft Teams	Could be removed from chat sessions	Can't find, select, chat or call users
If the people involved are included in an information barrier policy to prevent the activity, they will not be able to proceed.	In addition, potentially, everyone included in an information barrier policy can be blocked from communicating with others in Microsoft Teams.	When people affected by information barrier policies are part of the same team or group chat, they might be removed from those chat sessions and further communication with the group might not be allowed.	When information barrier policies are in place, people who should not communicate with other specific users won't be able to find, select, chat, or call those users.

Before/after examples

In Microsoft Teams, information barrier policies determine and prevent the following kinds of unauthorized communications:

- Searching for a user
- Adding a member to a team
- Starting a chat session with someone
- Starting a group chat
- Inviting someone to join a meeting
- Sharing a screen
- Placing a call

Initially, information barriers apply to Microsoft Teams chats and channels only.

Licensing and role requirements

Required subscriptions	Required roles	What you need to know
Information barriers are rolling out now, and are included in subscriptions, such as: • Microsoft 365 E5 • Office 365 E5 • Office 365 Advanced Compliance • Microsoft 365 E5 Information Protection and Compliance For more details, see [Compliance Solutions]().	To [define or edit information barrier policies](), you must be assigned one of the following roles: • Microsoft 365 global administrator • Office 365 global administrator • Compliance administrator • IB Compliance Management (this is a new role!) To learn more about roles and permissions, see [Permissions in the Office 365 Security & Compliance Center]().	You must be familiar with PowerShell cmdlets in order to define, validate, or edit information barrier policies. Although we provide several examples of PowerShell cmdlets in the [how-to article](), you'll need to know additional details, such as parameters, for your organization.

Next steps:

- Learn more about information barriers in Microsoft Teams
- See the attributes that can be used for information barrier policies
- Define policies for information barriers
- Edit (or remove) information barrier policies

For more information, visit https://docs.microsoft.com/en-us/microsoft-365/compliance/information-barriers