

# Teams Security Config Solution Pitch Deck and Architecture

# 有關 Microsoft Teams 安全的問題

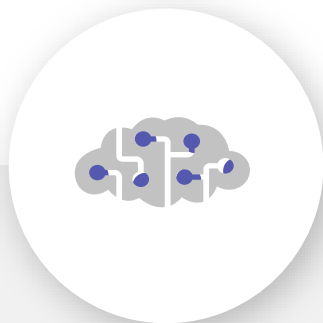
**COVID 19** 改變了人與人之間工作互動的模式，為了避免接觸，**Microsoft Teams**會議與協同作業工具廣為企業採用。然而，開始使用之後如何管理以確保線上會議不受干擾、保護參與者的隱私和個人資訊、禁止不當用語以及各種安全性，是我們該熟悉的作業



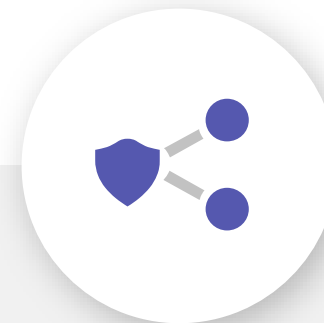
# Microsoft 365 安全原則



跨平臺工作的內建體驗



人工智慧和自動化，以保護  
您的未來



整合人員、設備、應用程式  
和數據

# 身份和存取



## 多因素驗證、條件式存取與簡訊代碼

實施強式認證，防止未經授權或非典型存取風險



## 資訊屏障 (Information Barriers)

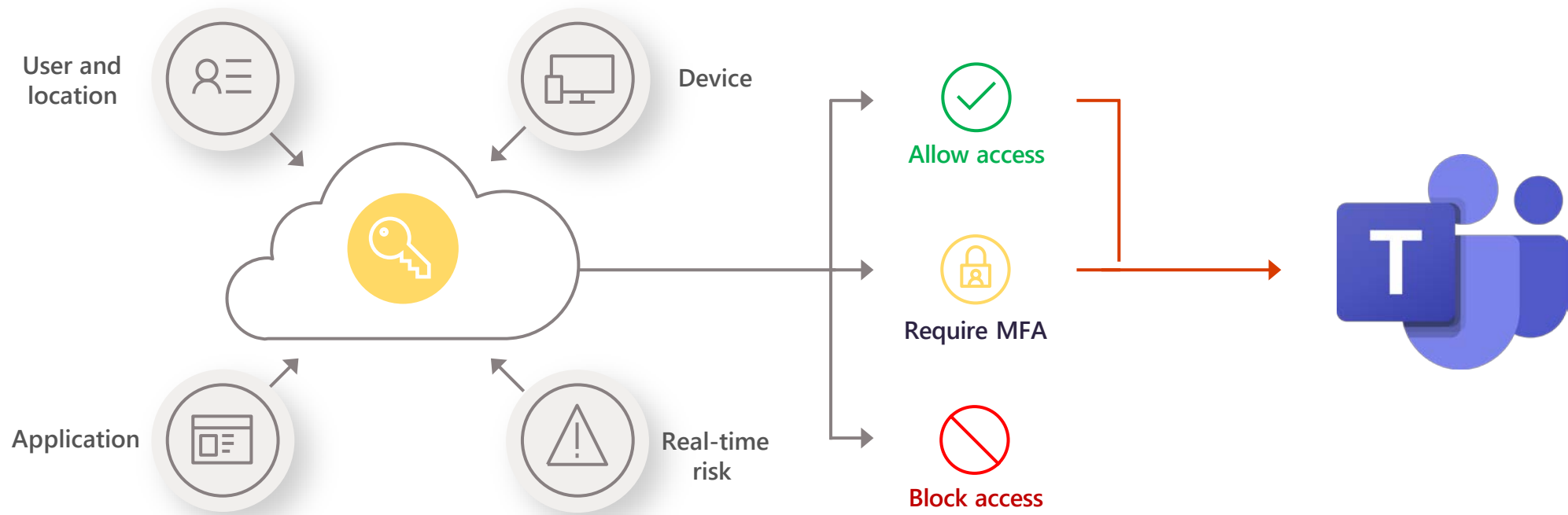
在公司內部和來賓中創建不同的區隔，以阻止被發現和避免溝通



## 來賓和外地跨公司存取

安全地管理外部人員如何存取公司資源並參與聊天和會議

# 條件式存取



# 條件式存取

The screenshot shows the Microsoft Azure portal interface for configuring a Conditional Access policy. The breadcrumb path is: Home > Conditional Access - Policies > Non compliant > Cloud apps or actions. The policy name is 'Non compliant'. Under 'Assignments', 'Users and groups' shows 'Specific users included' and 'Cloud apps or actions' shows '1 app included'. Under 'Conditions', '1 condition selected' is shown. Under 'Access controls', '2 controls selected' is shown. The 'Cloud apps or actions' configuration pane is open, showing 'Select what this policy applies to' with 'Cloud apps' selected. Under 'Include/Exclude', 'None', 'All cloud apps', and 'Select apps' are options. The 'Select' dropdown shows 'Microsoft Teams' is selected.



The screenshot shows a 'Login to Microsoft Teams' window for 'CONTOSO demo'. The user is 'meganb@m365x860223.onmicrosoft.com'. The error message is: 'You cannot access this right now'. The text below reads: 'Your sign-in was successful but does not meet the criteria to access this resource. For example, you might be signing in from a browser, app, or location that is restricted by your admin.' There is a 'More details' link and an 'Insider Ring - details here' link.

防止從非工作地點訪問

The screenshot shows a 'Login to Microsoft Teams' window for 'CONTOSO demo'. The user is 'meganb@m365x860223.onmicrosoft.com'. The error message is: 'You can't get there from here'. The text below reads: 'This application contains sensitive information and can only be accessed from:'. A list includes: 'Devices or client applications that meet Contoso management compliance policy.' Below this, it says: 'If this is a personal device you can choose to let Contoso manage your device by going to Settings > Accounts > Access work or school and clicking in "Connect". When you're done come back and try again.' There is a 'More details' link and an 'Insider Ring - details here' link.

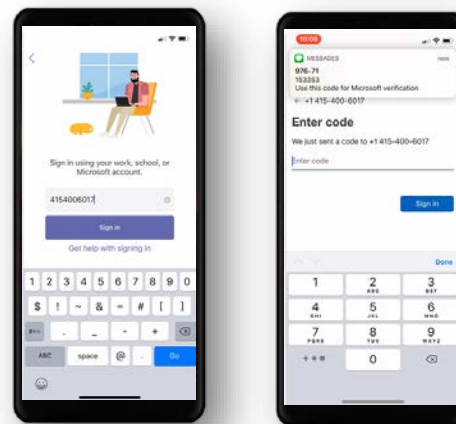
防止經過驗證的使用者  
訪問未經管理的設備

# 第一線員工的安全登入管理

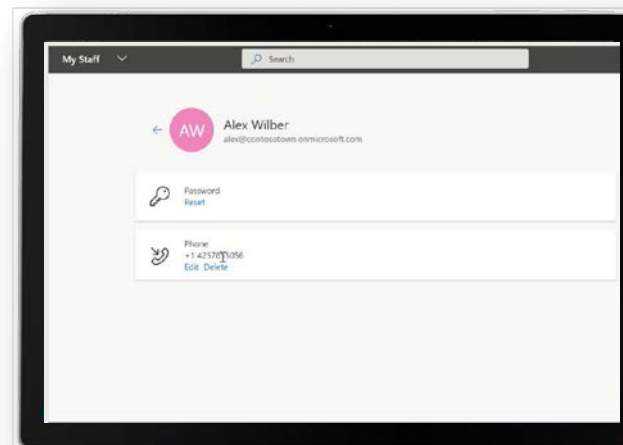
允許第一線員工透過簡訊中的代碼進行身份驗證

避免密碼管理並減少Helpdesk的負擔

直屬主管（不是由IT部門）可以更新電話號碼並重設密碼



簡訊登入



委派管理

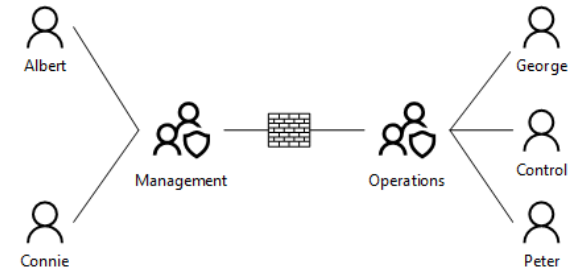
# 資訊屏障 (Information Barriers)

組織需要限制分享、控制資訊流向，並將一群使用者隔離開來

## 資訊屏障可以阻隔：

用戶者主動發現，包括添加到團隊和會議邀請

聊天訊息、螢幕共用、通話和會議也適用於 SharePoint 檔案存取




### Add members to Management

Start typing a name, distribution list, or security group to add to your team. You can also add people outside your organization as guests by typing their email addresses.

Start typing a name or group  Add

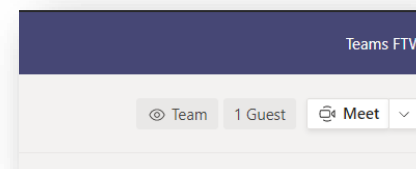
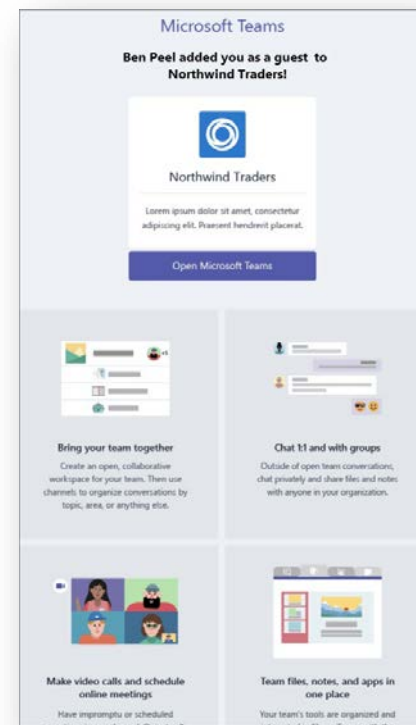
We couldn't add member. [Retry all](#) ↻

 Control CONTROL [Unable to add user due to IT admin settings. Learn more](#) [Retry](#) ↻ ×



# 來賓存取

The screenshot shows the Microsoft Teams System Management Center interface for Contoso Electronics. The left sidebar contains navigation options: 儀表板, 團隊, 裝置, 位置, 使用者, 會議, 訊息原則, Teams App, 語音, 原則套件, 分析與報告, 全組織設定 (highlighted), 外部存取, 來賓存取 (highlighted), Teams 設定, Teams 升級, 假日, and 資源帳戶. The main content area is titled "來賓存取" (Guest Access) and includes a description: "Teams 中的來賓存取可讓您組織外部的人員存取團隊和頻道。當您開啟 [來賓存取] 時，您可以開啟或關閉來賓使用者可以或不能使用的功能。請務必遵循此[檢查清單](#)中的步驟來設定先決條件，以便小組擁有者可以將來賓使用者新增至其小組。深入了解" (Guest access in Teams allows you to allow external people to access teams and channels. When you turn on [Guest Access], you can turn on or off features that guest users can or cannot use. Be sure to follow the steps in this [checklist](#) to set prerequisites so that group owners can add guest users to their groups. Learn more). Below the description, there are several settings sections: "在 Teams 中允許來賓存取" (Allow guest access in Teams) with a dropdown menu set to "服務預設值: 開啟" (Service default: On); "撥號" (Calling) with a toggle for "進行私人通話" (Make private calls) set to "開啟" (On); "會議" (Meetings) with a toggle for "允許 IP 視訊" (Allow IP video) set to "開啟" (On), a dropdown for "螢幕區分享模式" (Screen sharing mode) set to "整個螢幕" (Entire screen), and a toggle for "允許立即開會" (Allow instant meetings) set to "開啟" (On). The "即時訊息" (Instant messages) section is partially visible at the bottom.



# 來賓存取安全性

要求來賓使用多因素驗證並查看特定使用條款

The screenshot shows the 'Grant' configuration page for 'Teams Guest Users'. The left sidebar contains sections for 'Info', 'Assignments', and 'Access controls'. The 'Access controls' section is expanded, showing 'Grant' with '2 controls selected'. The main area is titled 'Select the controls to be enforced.' and has two radio buttons: 'Block access' and 'Grant access', with 'Grant access' selected. Below this are several checkboxes for additional controls: 'Require multi-factor authentication' (checked), 'Require device to be marked as compliant' (unchecked), 'Require Hybrid Azure AD joined device' (unchecked), 'Require approved client app' (unchecked), and 'Data Usage Policy (Terms of Use)' (checked). At the bottom, there are two radio buttons for 'For multiple controls': 'Require all the selected controls' (selected) and 'Require one of the selected controls' (unchecked). A 'Select' button is at the bottom right.

The screenshot shows the 'New terms of use' configuration page. It has a title 'Terms of use' and a subtitle 'Create and upload documents'. There are two required text input fields: 'Name' (with an example 'All users terms of use') and 'Display name' (with an example 'Contoso Terms of Use'). Below these is a 'Terms of use document' section with an 'Upload required PDF' button, a file selection icon, and a 'Select default language' dropdown menu. There is also a '+ Add language' link. A 'Require users to expand the terms of use' toggle is set to 'On'. At the bottom, there is a 'Conditional access' section with a dropdown menu for 'Enforce with conditional access policy templates' set to 'Policy templates'. A 'Create' button is at the bottom left.

# 微調來賓存取安全性

限制來賓可以來自何處，或員工可以作為來賓前往何處


Guest source allow/deny list

### Collaboration restrictions

Allow invitations to be sent to any domain (most inclusive)

Deny invitations to the specified domains

Allow invitations only to the specified domains (most restrictive)

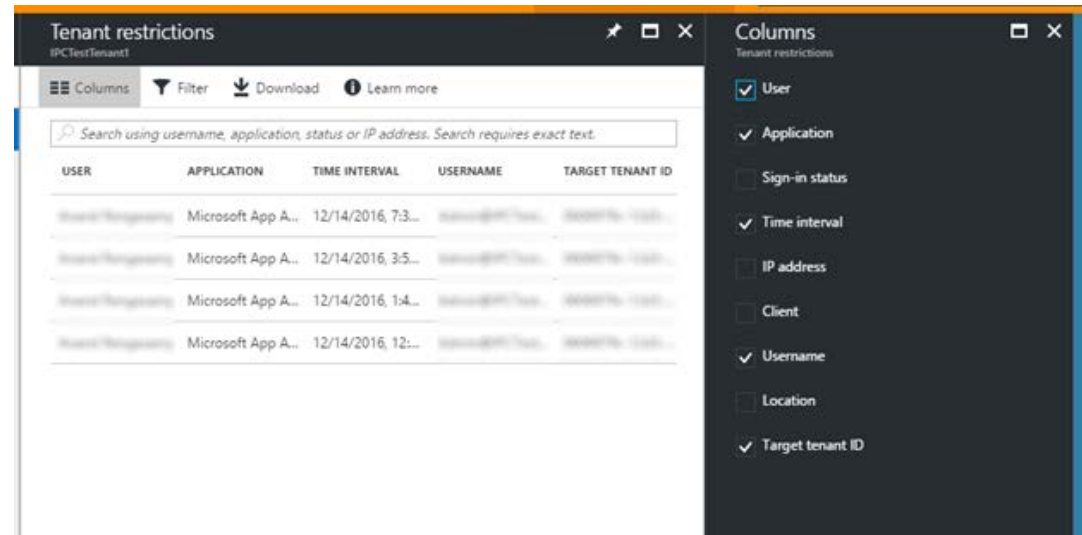
 Delete

TARGET DOMAINS

contoso.com

fabrikam.com

Tenant Restrictions: use proxy to block access to O365 services in all/specific tenants



USER	APPLICATION	TIME INTERVAL	USERNAME	TARGET TENANT ID
Guest/Anonymous	Microsoft App A...	12/14/2016, 7:3...	MicrosoftAppA...	MicrosoftAppA...
Guest/Anonymous	Microsoft App A...	12/14/2016, 3:5...	MicrosoftAppA...	MicrosoftAppA...
Guest/Anonymous	Microsoft App A...	12/14/2016, 1:4...	MicrosoftAppA...	MicrosoftAppA...
Guest/Anonymous	Microsoft App A...	12/14/2016, 12:...	MicrosoftAppA...	MicrosoftAppA...



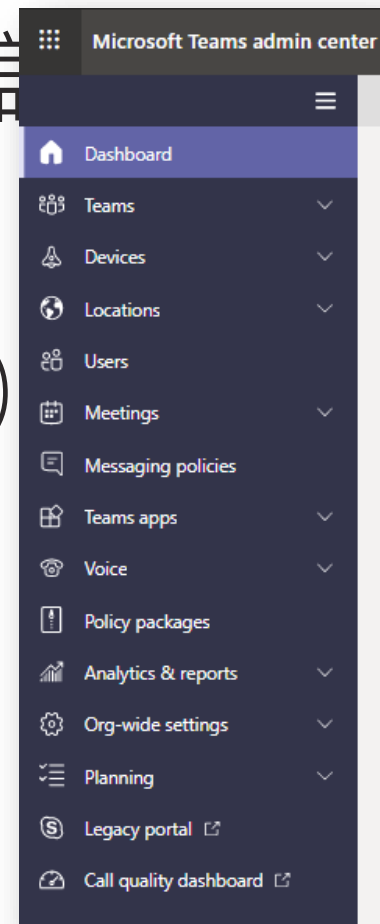
# 設定與原則-概述

**設定**：Settings (例如來賓、同盟、音訊會議)

適用於整個租用戶

**原則**：Policies – (例如訊息原則, 會議原則)

每個使用者 (包括多個) 或租用戶;每個群組



# 設定與原則-詳細說明

**團隊原則**：定義組織中的用戶可以在團隊和頻道中做什麼

**訊息原則**：選擇哪些聊天和頻道訊息的功能可供 Microsoft Teams 中的使用者使用

**會議設定**：使用者在組織中安排的所有 Teams 會議之設定

**會議原則**：控制與出席者會議時可具備的功能，以便參加組織中使用者安排之會議

The screenshot displays the Microsoft Teams System Management Center interface for Contoso Electronics. The left-hand navigation pane includes options like '儀表板', '團隊', '裝置', '位置', '使用者', '會議', '會議權接器', '會議原則', '會議設定', '即時活動原則', '即時活動設定', '訊息原則', 'Teams App', '語音', '原則套件', '分析與報告', '使用方式報告', '全組織設定', '外部存取', '來賓存取', 'Teams 設定', and 'Teams 升級'. The '會議原則' (Meeting Policy) option is highlighted in red. The main content area shows the configuration for the 'RestrictedAnonymousAccess' policy, which is noted as deprecated. Under the '一般' (General) section, four settings are listed and all are turned '開啟' (On): '允許在頻道中立即開會', '允許 Outlook 增益集', '允許頻道會議排程', and '允許排程私人會議'. Under the '音訊與視訊' (Audio and Video) section, '允許禮察' and '允許雲端錄製' are turned '關閉' (Off), while 'IP 音訊的模式' and 'IP 視訊的模式' are set to '已啟用傳出和傳入音訊' and '已啟用傳出和傳入視訊' respectively. Other settings include '允許 IP 視訊' (On), '允許 NDI 串流' (Off), and '媒體位元速率 (KB)' set to 50000.

# 設定與原則-詳細說明

**應用程式使用權限原則** :控制您組織中的 Microsoft Teams 使用者可使用哪些應用程式

**應用程式設定原則** :自訂微軟Teams以突出顯示對使用者最重要的應用程式

The screenshot displays the Microsoft Teams System Management Center interface for 'Contoso Electronics'. The left-hand navigation pane is expanded to show 'Teams App' settings, with '權限原則' (Permissions Policy) selected. The main content area shows the 'Global' application usage policy settings. It includes three sections for selecting which applications users can install: 'Microsoft 應用程式' (Microsoft Applications), '第三方應用程式' (Third-party Applications), and '自訂應用程式' (Custom Applications). Each section has a dropdown menu currently set to '允許所有應用程式' (Allow all applications). At the bottom, there are '儲存' (Save) and '取消' (Cancel) buttons.

# 團隊與頻道的生命週期管理

團隊類型：公共、私人或全組織  
範圍

誰可以創建一個團隊？

命名原則 – 前置字元, 尾碼, 禁用  
詞

過期原則

私有頻道

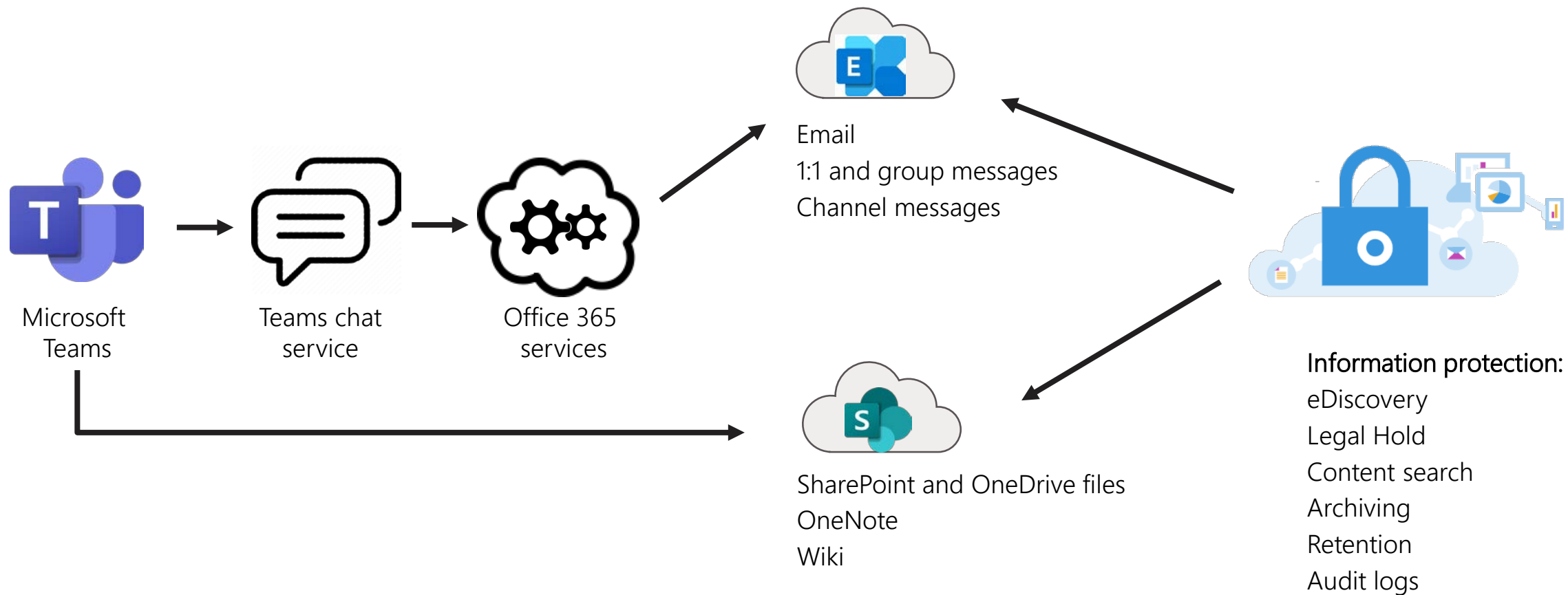


The screenshot shows the settings page for a Microsoft Teams team named 'KSS1S0'. The team icon is a circular logo with 'KSS1S0' and 'KB' inside. The page has a navigation bar with tabs: '成員', '待處理要求', '頻道', '設定' (selected), '分析', '應用程式', and '標籤'. Below the navigation bar is a list of settings items, each with a dropdown arrow and a description:

設定項目	描述
團隊圖片	新增團隊圖片
成員權限	允許建立頻道、新增應用程式等等
來賓權限	啟用頻道建立
@提及	選擇誰可以使用 @團隊和 @頻道形式的提及
團隊代碼	分享此代碼，讓人能直接加入團隊 - 您將不會收到加入要求
有趣小玩意	允許表情圖示、Meme、GIF 或貼圖
標籤	選擇可管理標籤的人員



# Teams 如何支援資訊保護



# 保留原則 Retention Policy

控制訊息資料將保留多長時間—每個使用者、每個團隊

The image displays two overlapping panels from the Microsoft 365 retention policy configuration interface. The background panel, titled 'Editing Locations applied', shows a table of locations with their retention settings. The foreground panel, titled 'Editing Policy settings', shows options for content retention and deletion.

Status	Location	Include	Exclude
<input checked="" type="checkbox"/>	Teams channel messages	All <a href="#">Choose teams</a>	None <a href="#">Exclude teams</a>
<input checked="" type="checkbox"/>	Teams chats	All <a href="#">Choose users</a>	None <a href="#">Exclude users</a>

**Editing Policy settings**

Do you want to retain content?

Yes, I want to retain it

For this long...  days

Do you want us to delete it after this time?

Yes  No

No, just delete content that's older than

years

Retain or delete the content based on

# 敏感度標籤 Sensitivity Label

建立並發布名為「機密」的敏感度標籤，其標籤隱私權選項已配置為「私人」。因此，使用此標籤建立的任何團隊都必須是私人團隊。

您建立並發布名為「一般」的敏感度標籤，其標籤隱私權選項已配置為公用。當使用者建立新團隊時，他們只有在選取此標籤時，才能建立公用或全組織團隊：




### What kind of team will this be?

Sensitivity [Learn more](#)

Confidential

Teams with this sensitivity must be private.

Privacy

-  **Private**  
People need permission to join
-  **Public**  
Anyone in your org can join
-  **Org-wide**  
Everyone in your organization automatically joins




### What kind of team will this be?

Sensitivity [Learn more](#)

General

Teams with this sensitivity must be public.

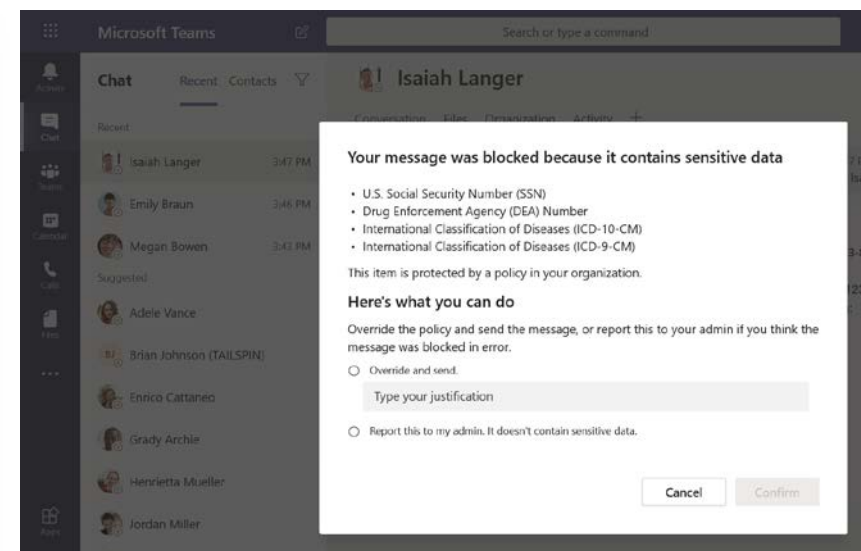
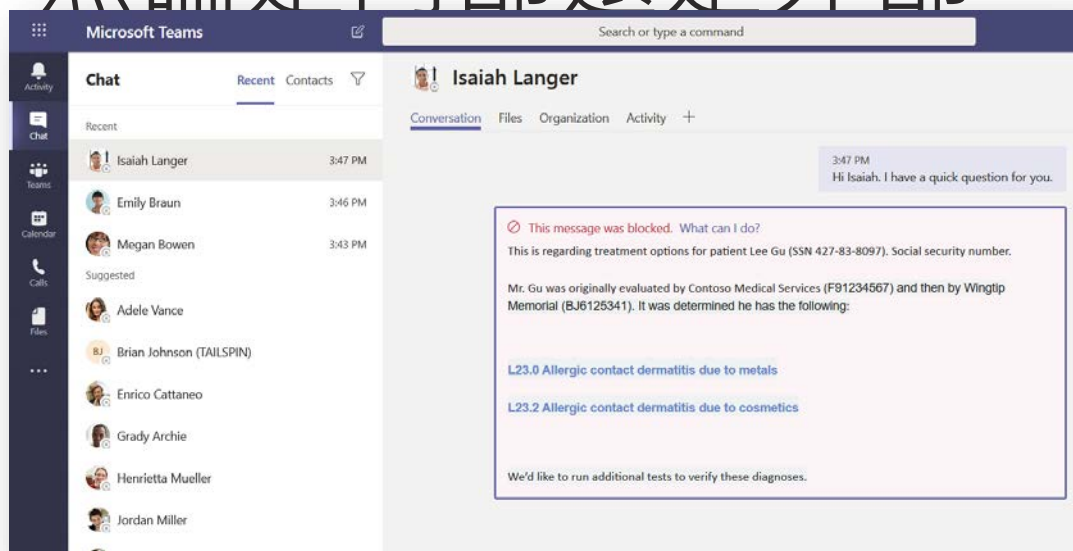
Privacy

-  **Private**  
People need permission to join
-  **Public**  
Anyone in your org can join
-  **Org-wide**  
Everyone in your organization automatically joins

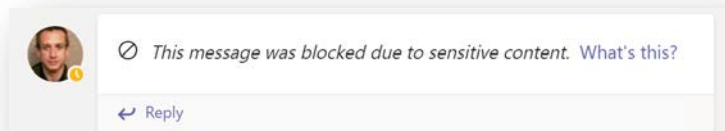
# 資料外洩防護 Data Lost Protection

防止用戶無意間共用有關客戶或機密專案的敏感資訊，無論是內部還是外部

Message sender

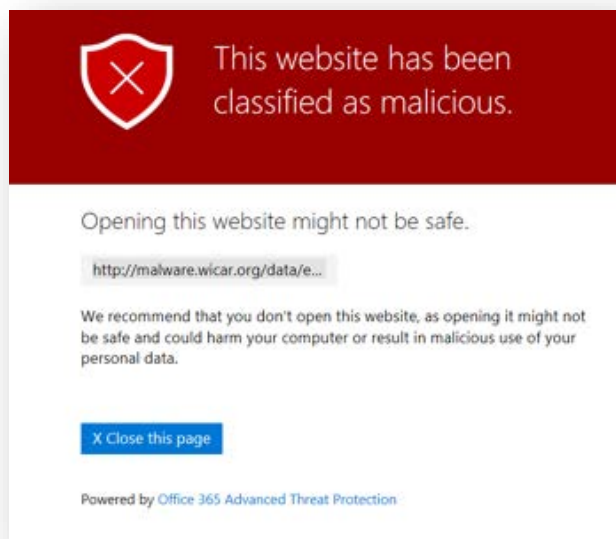
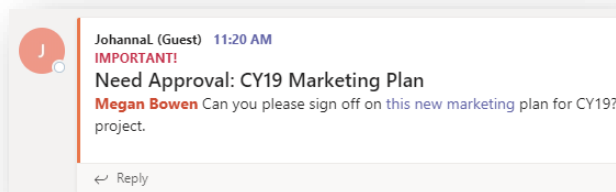


Message viewer

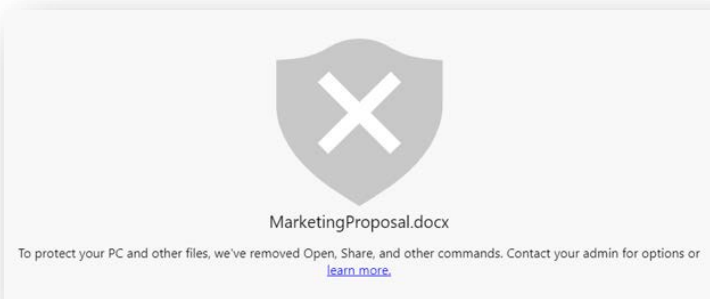
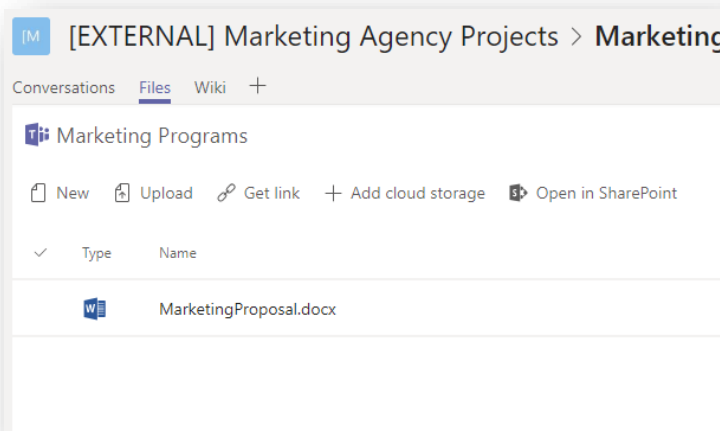


# 針對連結與檔案提供進階威脅防護

Link to malicious site



File with malware



管理員可以查看歷史記錄  
並接收警示

使用 Cloud App Security  
監控團隊中其他雲端空間  
供應商 (如Google) 的安全  
性

Teams還會自動掃描發送  
到頻道的任何內含惡意軟  
體電子郵件

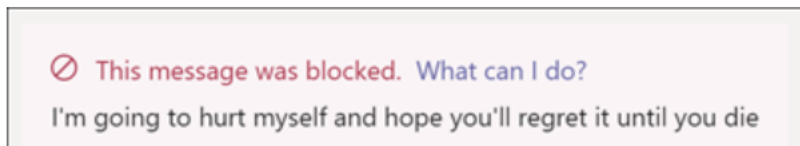
# 通訊合規 **Communication compliance**

## Microsoft 365 中 Insider Risk 解決方案

在團隊頻道或 1 : 1 和群聊中識別以下類型的不當內容：

- 冒犯性、褻瀆和騷擾性語言
- 成人、猥褻和血腥的圖像
- 分享機敏的資訊

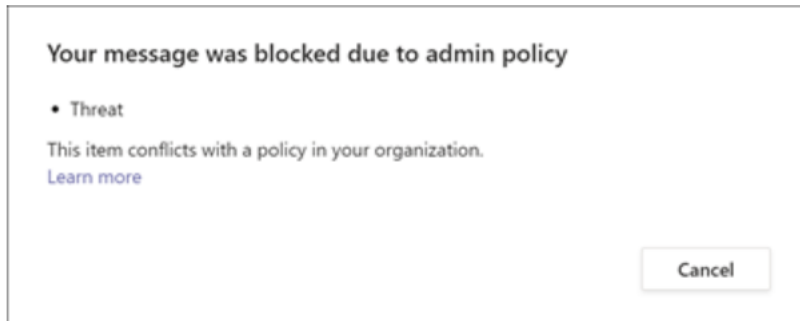
Example of policy tip seen by sender:



Example of policy tip seen by recipient:



Example of policy condition notification seen by the sender:



# 確保線上會議安全

由 IT 和會議召集人控制，以促進安全和包容性的會議

## 會議選項和控制以避免意外中斷

會議前透過選項，來指定大廳體驗、會議角色、聊天和音訊/視訊為個人或所有出席者靜音或禁用視訊以保持會議焦點

## 透過會議大廳限制未經授權的出席者

透過大廳控制誰可以直接參加會議，以限制未經授權的出席者透過不允許會議轉發，確保只有預期的會議參與者才能加入

## 會議中的角色

決定誰可以簡報或分享他們的螢幕與「簡報者」與「出席者」的角色如果需要提升角色，可輕鬆調整會議期間的出席者角色

## 頻道仲裁和控制

仲裁頻道中的對談，控制誰可以，誰不能分享內容確保頻道中的其他人只能查看適當的內容

