Teams Governance General Practices

- Teams Administration Role and Functions
- Teams User Policies
- Teams Tenant level Settings
- Recommended Practices Settings for Site and Channels
- Recommended Practices - Security Settings for Teams Applications
- Recommended Practices - Conditional Access Policies

Teams Administration Roles and Functions

Support Level 1	• Responsible for onboarding new users and assigning Teams policies using the Teams admin portal based on the request • For existing users, update the Teams policies when requested • Responsible for offboarding users and removing Teams policies using Teams admin portal
Help desk	• For Teams Incidents, Performs the troubleshooting basic troubleshooting steps • Escalate incidents that cannot be resolved by help desk to Support level 2
Support level 2	• For Teams Incidents, Performs additional troubleshooting steps to resolve open incidents for Teams. • Escalate incidents that cannot be resolved to SME
SME	• Address and resolve escalated tickets from Support level 1&2 • Mass migration of users from existing collaboration tool to Teams • Implements Microsoft Teams and uses powershell command lets to assign policies to users in batches

Recommended Teams Policies configurations

Dynamic Membership for Teams

- Creating new office 365 group with dynamic membership in Azure Active Directory is supported and recommended for ease of management.
- Dynamic membership can be applied/enabled to existing teams site (office 365 group)

Sensitivity labels

- Confidential label – Teams group assigned with this label will allow creation of private Teams site creation
- General label – Teams group assigned with this label will allow creation of Public or Org-wide Teams site creation

App Setup Policy

- This policy allow or disallows capability to add applications within Teams sites or channels

App Permissions Policy

- Microsoft Applications – Can be configured to allow or disallow Microsoft applications in Teams app store
- Third Party Applications - Can be configured to allow or disallow Third party applications available in Teams app store
- Custom Applications – Can be configured to allow or disallow custom line of business applications to integrate with Team sites

Recommended Teams Policies configurations

Live Events Policy	• Global (Org-Wide) – Scheduling and transcription can be configured through this policy
Call Park Policy	• Global(Org-Wide) – Call Parking settings can be configured through this policy
Caller ID	• Global (Org-Wide) – Caller ID can be allowed or disallowed through this policy
Teams Policy	• Global (Org-Wide) – Caller ID can be allowed or disallowed through this policy

Teams Tenant level Settings (Current Settings)

External Access	• Default option is set to Allow external users to communicate using the Teams client. Recommendation is to configure Add Domains to allow external communication to a list of specific Domains and to block all other Domains.
Guest Access	• Can allow or disallow Guest users to Calling, Messaging , Meeting and accessing Teams sites and channels
Teams Settings	• Notifications and Feed – can be controlled through this policy • Email Integration – default is set to allow users to send emails to specific channel email addresses.
Teams Upgrade	• Co-Existence with Skype – Islands mode allows co-existence for Skype and Teams. • Teams Only mode moves all workloads to Teams

Recommended Practice Settings for Teams sites/channels

Naming Conventions

- Naming convention for office 365 groups and associated Teams site is recommended to be established before creating new sites. Example for a Teams Site
- Instead of creating multiple teams sites to support projects / continuation projects, use Channels within one Team site and each channel can be a version of a specific product release for Example – Create channels for each JRE release

SharePoint Managed Paths

- During SharePoint site creation, the URL of the managed path includes “/sites/” in the name. path is created that provide a link to that specific site. The best practice is to use “/teams/” instead of “/sites/” when created new SharePoint sites to align with Teams Sites and Channels.

Office 365 Group Provisioning

- The following sequence should be followed when creating a new Teams site
  - Teams support team creates a new office 365 group and assigns the site owners
  - Teams support team then creates the Teams site using the Teams template and notifies owners
  - Owners can then create Channels and add users to the teams site.

Recommended Practices Settings for Teams sites/channels

Teams Standard Template options

- Using a template will help administrators follow a standard naming convention for creation of Teams sites and channels.
- The following options can be configured using the Teams Templates
  - Base template type
  - Team name
  - Team description
  - Team visibility (public or private)
  - Team settings (for example, member, guest, @ mentions)
  - Auto-favorite channel
  - Installed app
  - Pinned tabs

Recommended Practices - Security Settings for Teams Applications

Key security settings to be configured

- Minimize the number of Global administrator accounts and setup Multi-factor authentication to all accounts accessing Azure/Office 365 portal
- Configure chat retention policy to 30 days since Teams Chat (1:1 and Group chats) are persistent unless retention policy is configured
- Implement DLP (Data loss prevention) policies for OneDrive
- Implement Microsoft Cloud App Security (CASB) policies to all Microsoft cloud apps to understand data travel through applications and restrict exfiltration
- Setup Azure Information Protection policies to prevent users from the ability to copy or paste data from corporate applications such as (Email, Teams chat, and channels) over to personal applications such as (personal email, messaging applications, chat on phone)

Recommended Practices – Security Settings for Teams Applications

File sharing settings to be configured

- Validate and configure file sharing settings with internal and external members within SharePoint Admin Center following Infrmation security team requirements
- Leverage Private Teams sites and channels to prevent non-team members accessing sensitive files within the organization
- Ensure that Information Security team file sharing requirements are followed in One Drive for business before enabling file sharing in 1:1 and Group chat

Recommended Practices - Conditional Access Policies

Option 1 – Restrict access to Managed Devices

- Enable Auto enrolment for On-premise devices in Azure
- Setup MFA for all users for accessing cloud applications
- Grant Microsoft Teams application through browser or client app after confirming attempted device is either Azure AD joined or Domain joined

Option 2 – Restrict access to Managed Devices

- Enable Auto enrolment for On-premise devices in Azure
- Setup MFA for all users for accessing cloud applications
- Setup Intune Compliance policy
- Grant Microsoft Teams application through browser or client app after confirming attempted device is either Azure AD joined or Domain joined and that the Device is compliant

Recommended Practices - Conditional Access Policies

Option 3 – Setup Mobile Application Management (MAM)

- Assign Intune licenses to all users
- Setup Intune App protection policy
- Configure settings like restrict cut, copy, paste from other apps for Microsoft Teams . Enable PIN for accessing app setting
- Prevent Microsoft Teams data from Itunes or iCloud backups set to yes
- Restrict saveAs functionality from Teams
- Apply policy to security group or All users
- Remote wipe feature can be leveraged to remotely wipe corporate data from the device