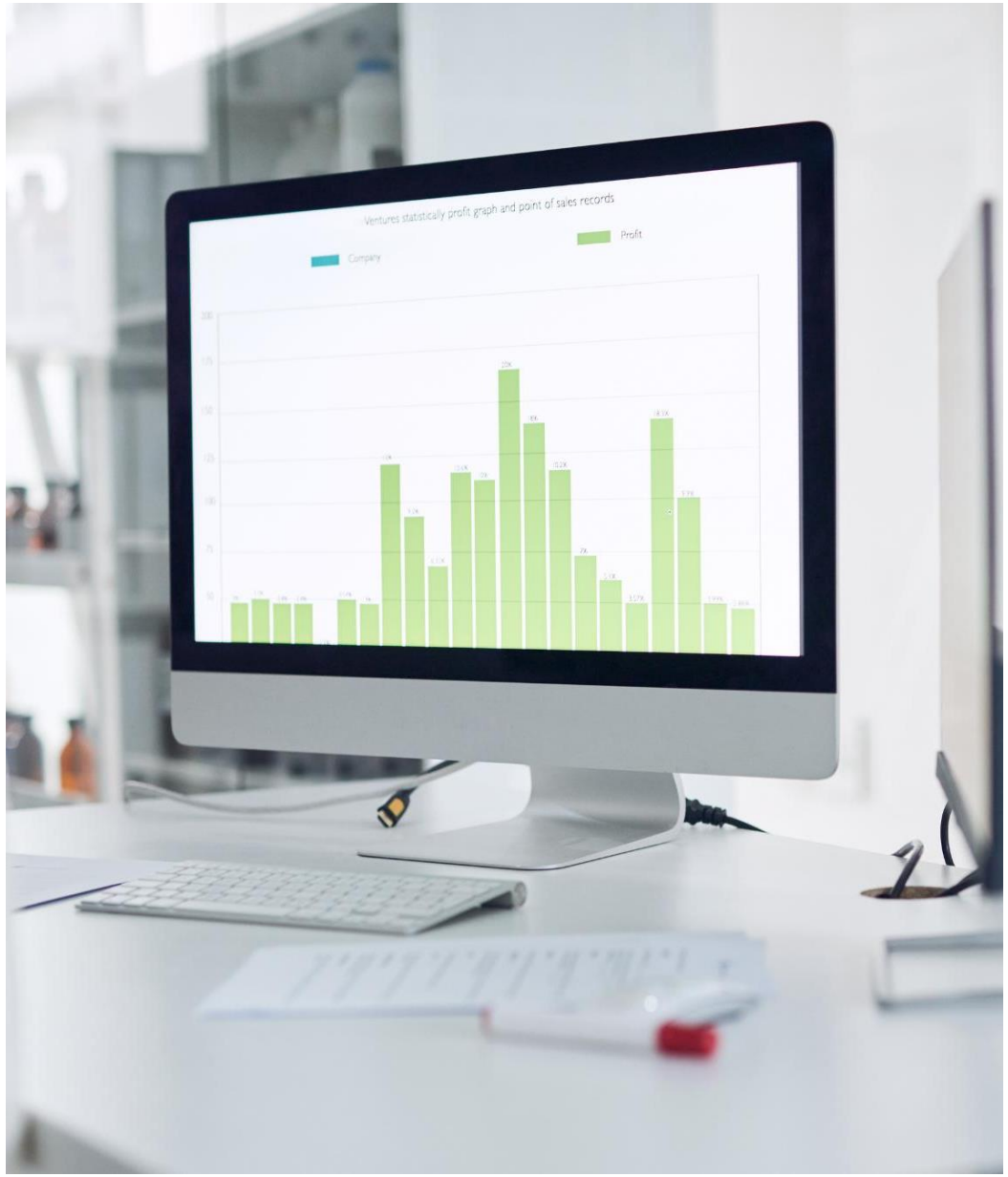
Microsoft 365 Security Configuration and Governance

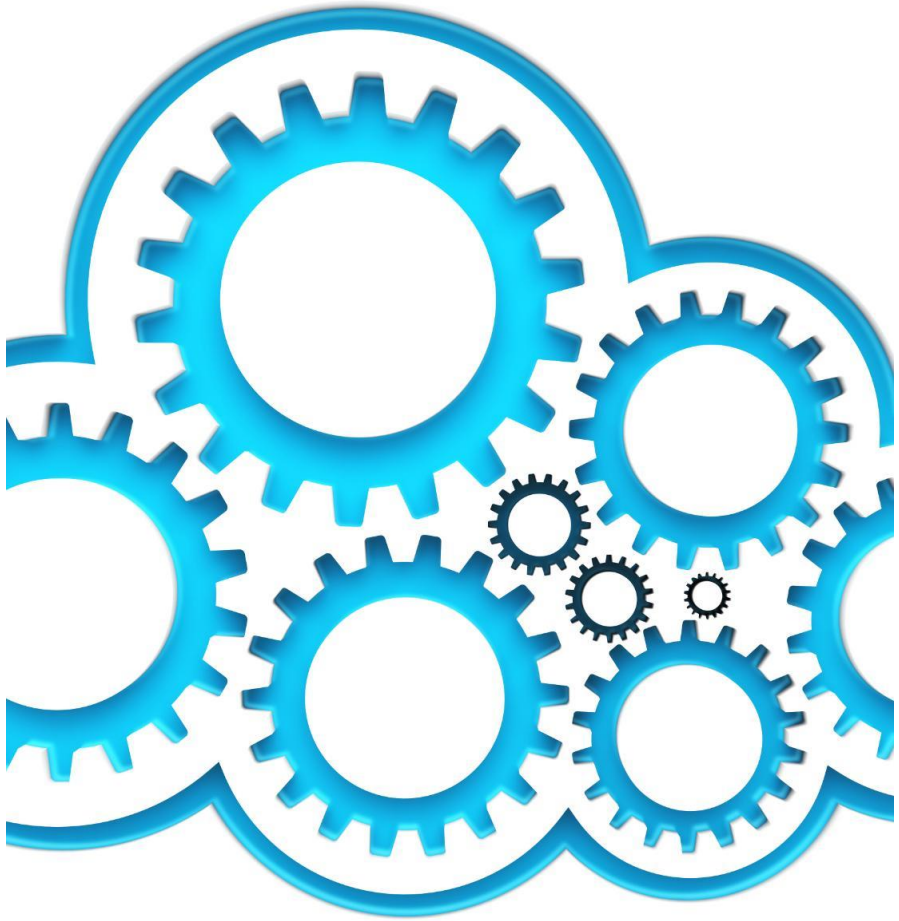
Key strategies for securing Microsoft 365 environments



Agenda Items

- Default Settings and IT Control
- Template Settings for IT Control
- Teams and SharePoint Online Settings
- Advanced Management for Oversharing and Expired Content

Default Settings and IT Control



Optimized Default Settings

Default Settings Overview

Default settings in Microsoft 365 aim to enhance collaboration but may limit IT control during rollout.

Controlled Cloud Journey

Companies can start their cloud journey with a template that balances collaboration and IT control effectively.

IT Control and Functionality

Maintaining IT control allows better management of functionalities and user interactions with external entities.

Basic Security Requirements

Initial Security Setup

This template provides an initial setup ensuring that fundamental security requirements are addressed immediately.

Governance Engagement

While this overview is not a complete governance review, it serves as a starting point for security compliance.

Ongoing Security Review

A full security review will still be necessary to cover all aspects of security and compliance.

Template Settings for IT Control

Admin Account Security

Importance of MFA

Enabling multi-factor authentication (MFA) on all admin accounts significantly enhances security by adding an extra layer of protection.

Preventing Unauthorized Access

MFA helps in preventing unauthorized access to sensitive admin accounts, reducing the risk of data breaches.

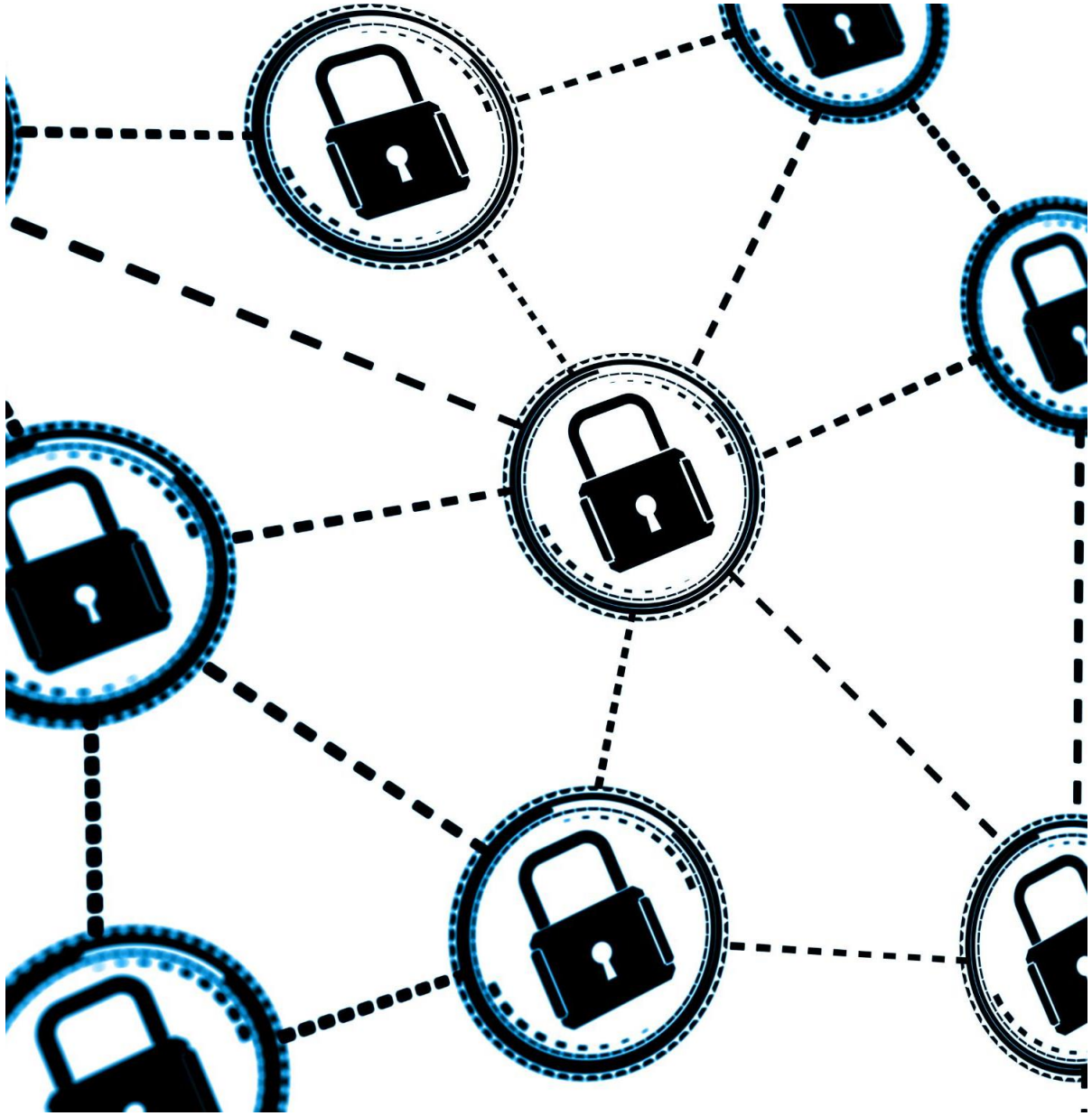
Conditional Access and Licensing Control

Risk-Based Conditional Access

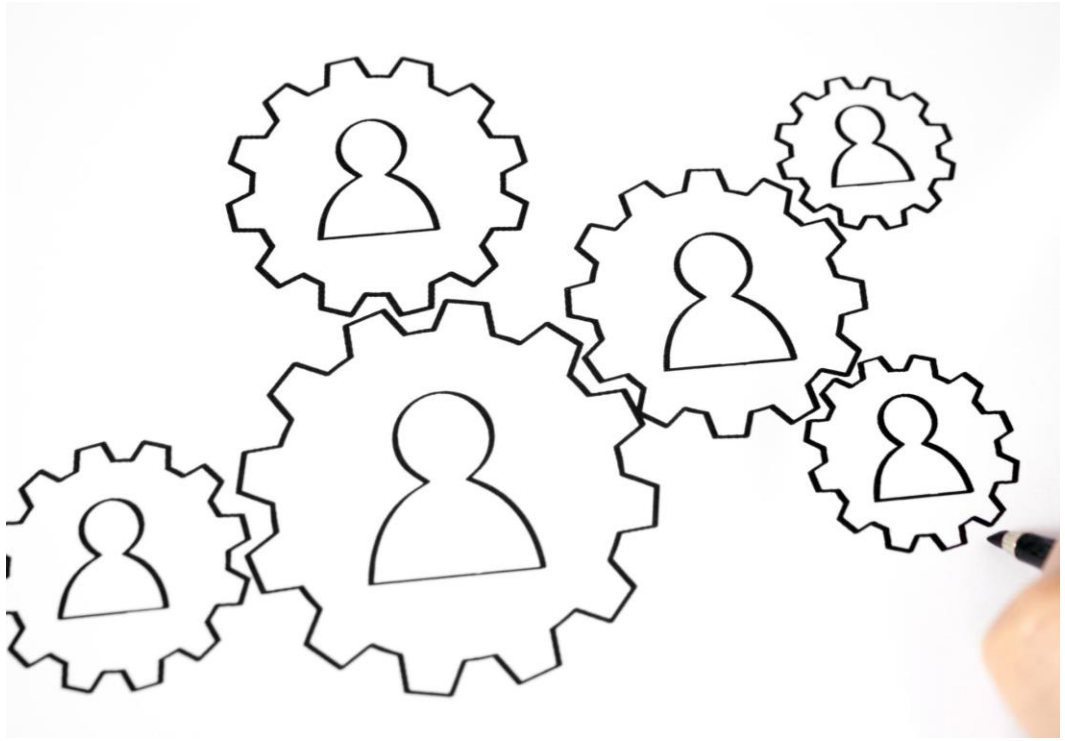
Implementing risk-based conditional access allows for more secure access for end users based on available licensing.

Licensing Assignment Control

Creating groups to manage licensing assignments allows for better control of which workloads are enabled or disabled.



Group Membership Restrictions



MS Teams Creation Restrictions

Limit the creation of Microsoft Teams based on user group membership to maintain organized collaboration.

SharePoint Team Sites Limitations

Restrict the creation of SharePoint Team Sites according to group membership for better management.

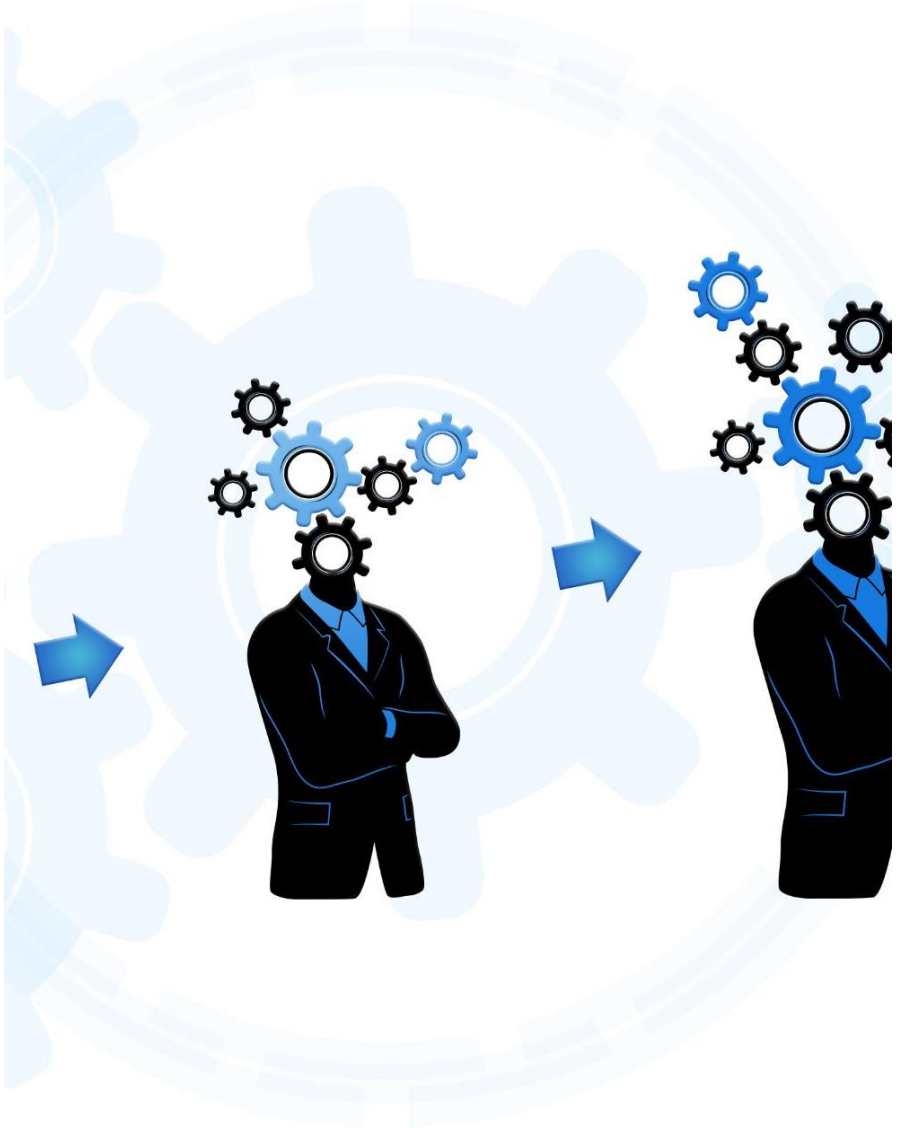
SharePoint Site Template Control

Only users with SharePoint Admin or Global Admin roles can create specific SharePoint Site templates.

Guest Access Restrictions

Control who can create new guest accounts and share with external users based on group membership.

Teams and SharePoint Online Settings



Teams and SharePoint Governance

Best Practices Overview

Implementing best practices ensures effective collaboration and data management in Teams and SharePoint environments.

Governance Recommendations

Governance recommendations provide guidelines for managing user access, data security, and compliance in Teams and SharePoint.

Settings Configuration

Proper settings configuration helps in optimizing performance and enhancing user experience in MS Teams and SharePoint.

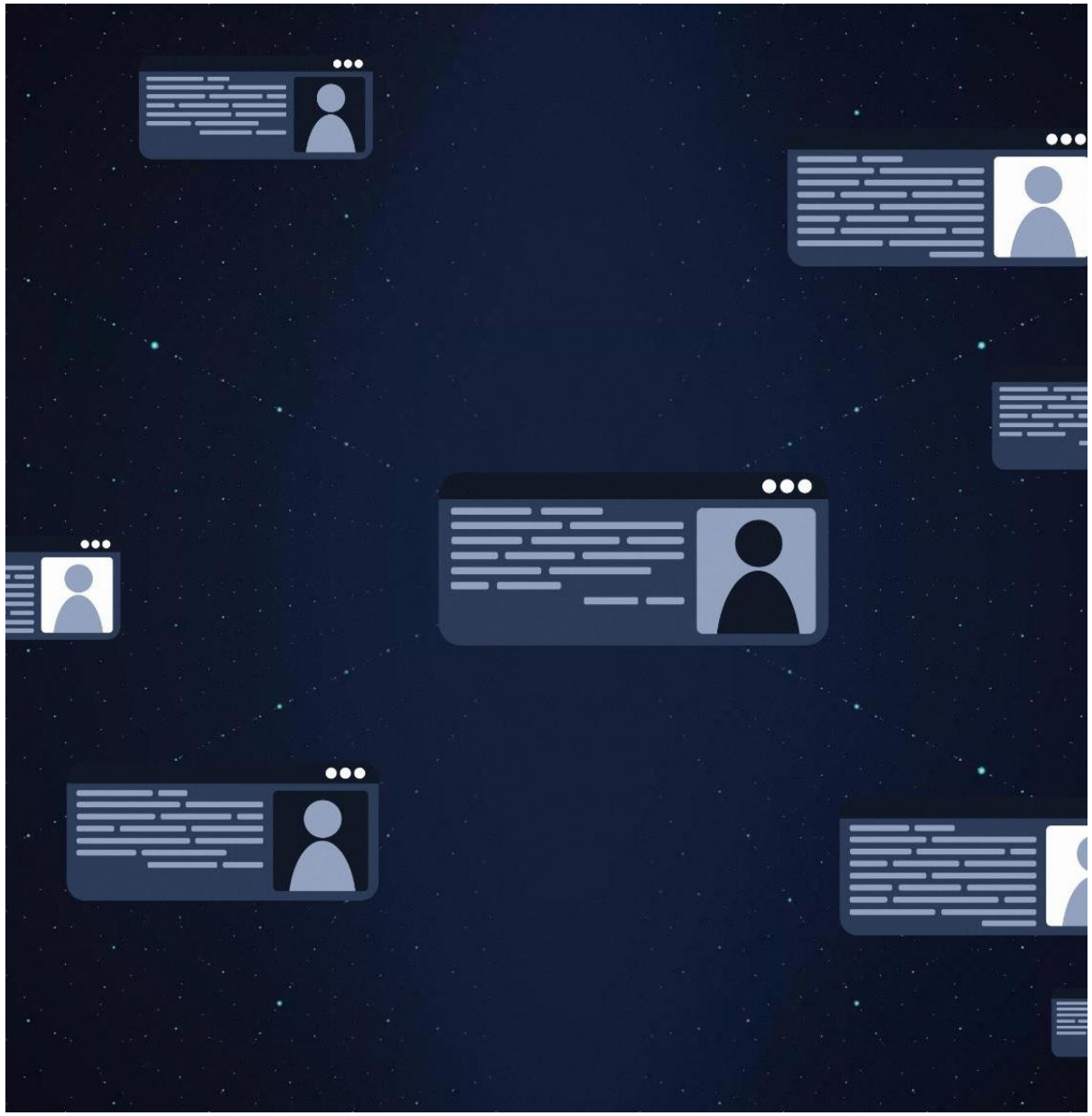
Release Preferences and Naming Conventions

Release Preferences

Release preferences determine which users receive new features and updates from O365, based on their group membership within the organization.

Naming Conventions

Establishing manual naming conventions for Teams and Communication Sites helps maintain consistency and clarity across organizational tools.



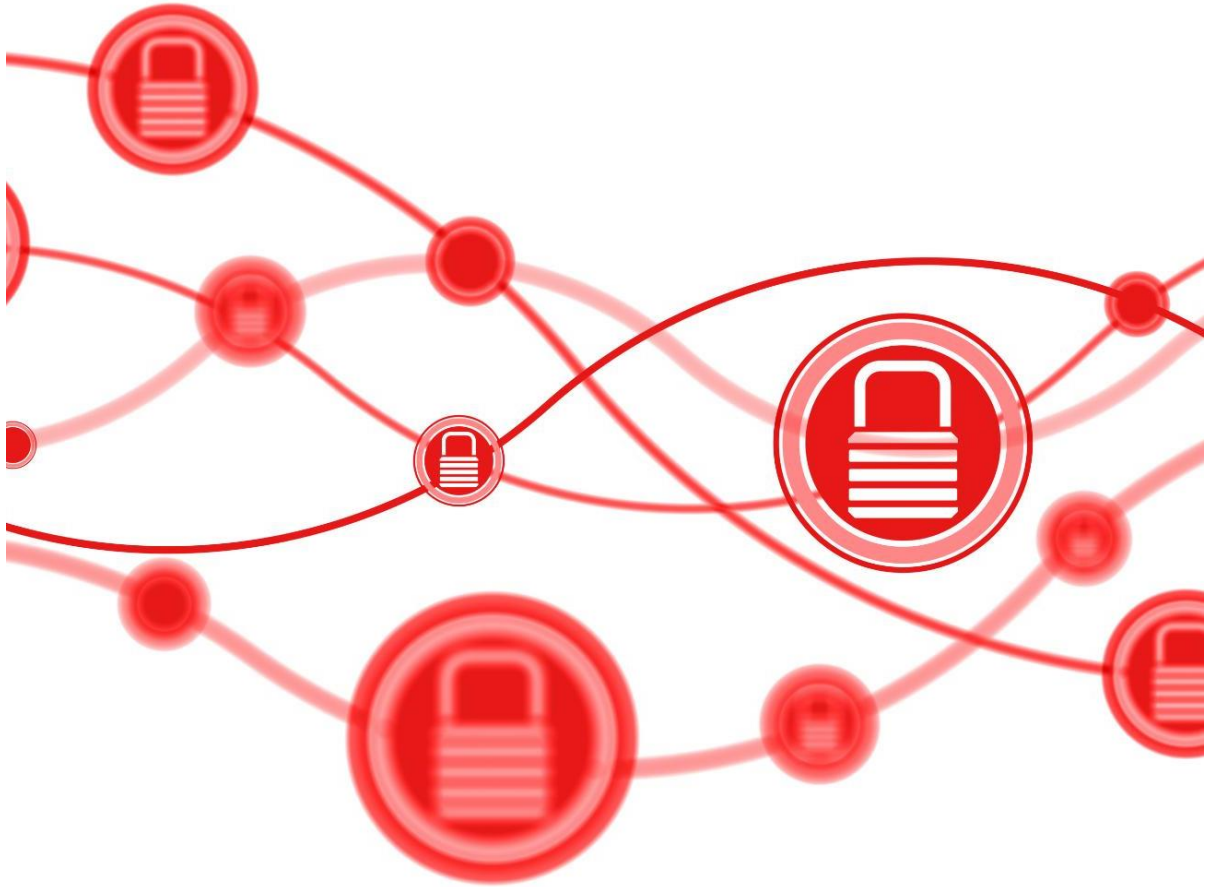
External Access and Sharing Policies

External Access Overview

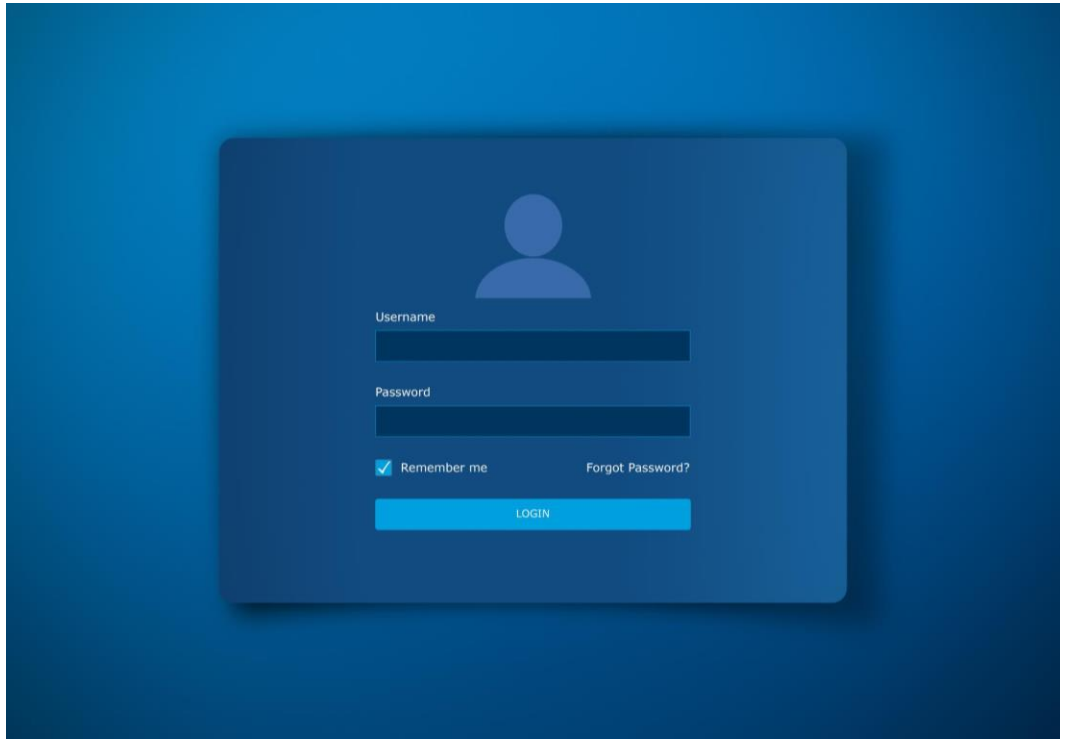
External access allows Teams users to communicate with individuals outside their organization, enhancing collaboration.

External Sharing Mechanism

External sharing enables users to share SharePoint sites with guests, requiring sign-in or verification for access.



SharePoint and OneDrive Settings



SharePoint Pages

SharePoint allows users to create and manage pages for collaboration and information sharing within teams.

Notifications Settings

Both SharePoint and OneDrive provide customizable notification settings to keep users informed about changes and updates.

Storage Limits

SharePoint has storage limits that can affect the amount of content users can store and manage effectively.

OneDrive Sync

OneDrive settings include options for syncing files across devices, ensuring access to the latest versions.

Teams Settings and Retention Policies

Teams Settings Overview

Teams settings encompass default meeting and messaging policies along with application policies that streamline communication.

Meeting and Messaging Policies

Default meeting and messaging policies ensure compliance and consistency in team communication and collaboration.

Retention Policies Explanation

Retention policies act as a catch-all to manage data retention and compliance requirements effectively.

Roles and Responsibilities

Teams Admin Role

The Teams Admin manages and oversees the Microsoft Teams environment, ensuring efficient communication and collaboration tools are in place.

SharePoint Admin Role

The SharePoint Admin is responsible for managing SharePoint sites, ensuring users have access to necessary resources and maintaining site security.

Site/Team Owners Role

Site and Team Owners have the responsibility of overseeing their respective teams, managing content, and facilitating collaboration among team members.

Advanced Management for Oversharing and Expired Content

Tenant Default Sharing Options

Specific People Sharing

Changing the tenant default sharing option to 'Specific People' enhances security by limiting access to designated individuals only.

Expiration of Links

Changing 'Anyone Links' to expire within 30 days helps mitigate risks associated with long-term access to shared content.

Site Identification and Reporting

Identifying Popular Sites

This step involves identifying the most frequented sites within the organization to analyze user engagement and trends.

Inactive Sites Monitoring

Identify sites that haven't been utilized for over six months to assess their relevance and potential for reactivation.

Comprehensive Reporting

Running a report across all organizational sites to gather insights and identify patterns in usage and performance.

Permissions and Sensitive Content

Permissions Overview

Identify the number of users with permissions to access and share content on the site, ensuring proper access management.

Sensitive Content Identification

Assess which content has sensitivity labels and determine if sensitive information is hosted on the site.

Sharing Permissions

Evaluate if only authorized users can share content and if default sharing options align with organizational needs.

External User Access

Determine if external users should have access to specific content and the implications of such access.

Purview DLP Policy and IT Processes

SharePoint DLP Policy Activation

Activate the SharePoint Purview DLP policy in simulation mode to monitor sharing of labeled or unlabeled data effectively.

Oversharing Identification Process

Establish a process for identifying oversharing incidents to guide IT in managing critical sites and data.

Inactive Site Management

Determine unused sites for more than six months and implement automatic options for IT to handle these sites effectively.

Conclusion

Importance of Security Configuration

Effective security configuration is essential to safeguard organizational data in Microsoft 365, reducing vulnerabilities.

Managing Permissions

Properly managing permissions is crucial to ensure that only authorized personnel access sensitive information and resources.

Clear Governance Policies

Maintaining clear governance policies helps organizations enforce compliance and establish accountability within their teams.