Is Your Microsoft 365/Teams Environment Secure and Configured for Compliance?

Microsoft 365/Teams Security & Configuration Checklist

With the increasing number of cyber threats and the growing importance of regulatory compliance, securing your Microsoft 365 and Teams environment is essential. Here's a checklist to help you ensure proper access control, data security, and compliance across your organization.

1. User Access Control

- ✔ Review and enforce the least privilege access model for all users.
- ✔ Use role-based access control (RBAC) for Microsoft 365 and Teams.
- ✔ Implement conditional access policies for Microsoft 365 accounts.
- ✔ Regularly audit and update user permissions to minimize unnecessary access.
- ✔ Configure access control for external applications integrated with Microsoft 365.

2. Data Retention Policies

- ✔ Set up data retention and deletion policies for emails, documents, and other files.
- ✔ Regularly review retention policies to ensure compliance with industry regulations.
- ✔ Define and enforce retention rules for Teams chat and channel data.
- ✔ Automate data archiving and deletion to reduce manual errors.
- ✔ Ensure proper classification of data to support retention policies.

3. Teams Settings

- ✔ Restrict guest access to Teams where necessary.
- ✔ Set up multi-factor authentication (MFA) for all Teams users.
- ✔ Ensure privacy settings for meetings and channels align with company security standards.
- ✔ Regularly review and adjust Teams settings based on evolving security needs.
- ✔ Disable file sharing features for sensitive Teams channels where appropriate.

4. File Sharing

- ✔ Ensure secure file sharing (with encryption) is enabled across Microsoft 365.
- ✔ Limit file sharing outside the organization (externally) unless necessary.
- ✔ Enforce file sharing policies based on user roles and project needs.
- ✔ Set up alerts for unauthorized file sharing attempts.
- ✔ Regularly audit shared files for potential data leaks or unauthorized access

5. Advanced Threat Protection

- ✔ Configure Office 365 Advanced Threat Protection (ATP) to block phishing and malicious links.
- ✔ Review ATP alerts weekly to identify and respond to emerging threats.
- ✔ Use ATP Safe Links and Safe Attachments to protect users from malicious content.
- ✔ Enable ATP anti-phishing policies to reduce the risk of social engineering attacks.
- ✔ Regularly update ATP configurations to reflect new threat intelligence.

6. Compliance Center

- ✔ Set up and regularly review the Microsoft 365 Compliance Center for data loss prevention (DLP).
- ✔ Ensure appropriate auditing is enabled for all Microsoft 365 services.
- ✔ Implement DLP policies for emails, files, and Teams content to prevent sensitive data leaks.
- ✔ Conduct quarterly audits to verify compliance with organizational security policies.
- ✔ Stay informed on updates and changes in compliance regulations to maintain alignment.

By securing your Microsoft 365 and Teams environment with the right configurations and compliance measures, you'll strengthen your defenses, reduce risks, and ensure your organization meets industry standards.

axiatp