Microsoft Teams Governance Plan Template

Teams Governance Plan for

(your company name)

Created on

(MM/DD/YYYY)

Version

Action Item	Instructions	Action Plan	Responsible Party	Due Date	Notes	Important
Section 1: Define the plan						
Define the purpose	Detail the direction and extent of the governance plan, explaining why it is necessary and how it can improve coordination, security, compliance, and productivity.					
Define the scope	Define the areas covered by the plan, specifying specific departments, teams or entire organization.					
Assign roles and responsibilities	Outline the roles (e.g., Team owner, members, guests) and their responsibilities. This can include admins, IT staff, end users, and third-party vendors. Specify their roles and responsibilities.					
Section 2: Establish policies and procedures						
Establish Teams Lifecycle guidelines	Define how Teams will be created, managed, archived, and eventually deleted. Include policies for naming conventions, expiration, and renewal.					
Develop Team Creation and Management policies	Standardize who can create Teams and how they should be managed. Include policies for naming conventions, expiration, and renewal.					

Action Item	Instructions	Action Plan	Responsible Party	Due Date	Notes	Important
Develop Team Creation and Management policies	Standardize who can create Teams and how they should be managed.					
Develop Data Access and Sharing policies	Ensure data is securely and appropriately shared and accessed. Establish how different types of data (e.g., confidential, public) should be handled and who can access them.					
Develop App Usage policies	Manage the use of third-party apps within Teams.					
Establish guest access policies	Describe how external collaboration will be managed, including how guests will be invited, what they can access, and how their access will be monitored and controlled. Establish the process for revoking guest access when it's no longer needed.					
Create Archiving and Retention Policies	Determine how long data should be kept and when it should be deleted.					
User Behavior Monitoring	Define a process for monitoring user activity to identify any misuse or violations of policies.					
Section 3: Security, privacy, and compliance						
Establish Data Protection Measures	Protect sensitive data from unauthorized access or leaks and establish measures for encryption, multi-factor authentication, and use of secure networks.					
Control Privacy Settings	Determine who can see what information.					
Ensure Regulatory Compliance	Make sure Teams usage complies with relevant laws and regulations.					
Establish Incident Response Plan	Outline steps to take in case of a security incident, including data leaks or inappropriate usage of Teams.					

Action Item	Instructions	Action Plan	Responsible Party	Due Date	Notes	Important
Control External Sharing	Determine who can share data externally, what data can be shared, and how to ensure security of data shared externally, such as the use of data loss prevention (DLP) policies or secure guest access. Include details on how users can securely share data externally, including encrypted emails or secure file transfer protocols.					
Define backup and recovery process	Detail how data will be backed up and the process for data recovery in case of a disaster.					
Establish Change Management	Define who approves changes, how they are communicated, how they are implemented and steps to take when handling unexpected changes or emergencies.					
Section 4: Ongoing training, adoption, and review						
Establish accessibility guidelines	If your organization needs to comply with accessibility regulations, include guidelines for ensuring all Teams content is accessible.					
User Support	Define how users can get help with Teams, whether there's a dedicated support team, and any self-help resources available.					
Establish performance monitoring	Define how the performance of Teams will be monitored and maintained. This includes monitoring system performance such as network bandwidth, user activity, usage trends, and response times. Establish thresholds for performance indicators to ensure optimal operation and user experience. Detail how often performance will be reviewed, who will be responsible for this task, and what actions will be taken if performance falls below acceptable levels. Outline how performance data will be reported and used to enhance Teams' efficiency and effectiveness.					

Action Item	Instructions	Action Plan	Responsible Party	Due Date	Notes	Important
Train employees	Develop and implement training programs to ensure employees know how to use Teams effectively and safely. Establish refresher trainings when there are significant changes to Teams or your policies.					
Create dispute resolution policies	Define how disputes related to Teams use will be resolved. Establish who makes the final decision when there are disagreements over how Teams should be used or who can have access.					
Establish review process	Determine how often the plan should be reviewed, who will be involved in the review process, and how updates will be communicated.					
Set up an ongoing audit process	Determine what reporting will be needed and who will be responsible for it.					

EXAMPLE TEMPLATE

Action Item	Instructions	Action Plan	Important links
Section 1: Define the plan			
Define the purpose	Detail the direction and extent of the governance plan, explaining why it is necessary and how it can improve coordination, security, compliance, and productivity.	The purpose of this governance plan is to ensure secure and efficient use of Microsoft Teams at XYZ Corp, enhancing collaboration while maintaining compliance with industry standards and regulations.	
Define the scope	Define the areas covered by the plan, specifying specific departments, teams, or entire organization.	This plan applies to all departments within XYZ Corp, with a particular focus on the Sales, Marketing, and Customer Support teams that heavily utilize Teams for daily operations.	

Action Item	Instructions	Action Plan	Important links
Assign roles and responsibilities	Outline the roles (e.g., Team owner, members, guests) and their responsibilities. This can include admins, IT staff, end users, and third-party vendors. Specify their roles and responsibilities.	T Department Heads at XYZ Corp are assigned as Team Owners, responsible for managing team membership and settings. All other employees are Team Members who use Teams for daily communication and collaboration.	
Section 2: Establish policies and procedures			
Establish Teams Lifecycle guidelines	Define how Teams will be created, managed, archived, and eventually deleted. Include policies for naming conventions, expiration, and renewal.	At XYZ Corp, Teams will be archived after 12 months of inactivity. If a Team remains archived and unused for a further 6 months, it will be deleted.	
Develop Team Creation and Management policies	Standardize who can create Teams and how they should be managed.	Only Department Heads and IT admins at XYZ Corp are authorized to create new Teams.	
Develop Data Access and Sharing policies	Ensure data is securely and appropriately shared and accessed. Establish how different types of data (e.g., confidential, public) should be handled and who can access them.	Sensitive data, like financial reports, are restricted to the Finance Department and Top Management at XYZ Corp.	
Develop App Usage policies	Manage the use of third-party apps within Teams.	Only IT-approved apps like Planner and OneNote are permitted within Teams at XYZ Corp.	
Establish guest access policies	Describe how external collaboration will be managed, including how guests will be invited, what they can access, and how their access will be monitored and controlled. Establish the process for revoking guest access when it's no longer needed.	Guests at XYZ Corp are allowed to join team meetings but are not permitted to access team files.	
Create Archiving and Retention Policies	Determine how long data should be kept and when it should be deleted.	Team files at XYZ Corp will be retained for a period of 5 years before deletion, in line with our corporate data retention policy.	XYZ Corp. Data Archival and Retention Policy.pdf
User Behavior Monitoring	Define a process for monitoring user activity to identify any misuse or violations of policies.	XYZ Corp's IT department has established a comprehensive user activity monitoring system. We utilize Microsoft's built-in auditing and reporting features in Teams to track activities such as message posts, file sharing, and meeting participation. Any abnormal behavior or policy violations are flagged and reviewed by our IT security team. Regular reports are generated and reviewed monthly to ensure policy compliance and identify any potential areas of concern.	

Action Item	Instructions	Action Plan	Important links
Section 3: Security, privacy, and compliance			
Establish Data Protection Measures	Protect sensitive data from unauthorized access or leaks and establish measures for encryption, multi-factor authentication, and use of secure networks.	XYZ Corp has implemented encryption, multi-factor authentication, and the use of secure networks to protect sensitive data.	
Control Privacy Settings	Determine who can see what information.	Only Team Members at XYZ Corp can view posts and files within their respective Teams.	
Ensure Regulatory Compliance	Make sure Teams usage complies with relevant laws and regulations.	XYZ Corp ensures Teams usage complies with GDPR and other relevant laws and regulations.	
Establish Incident Response Plan	Outline steps to take in case of a security incident, including data leaks or inappropriate usage of Teams.	In case of a security incident, such as data leaks, the IT department at XYZ Corp will isolate the affected systems, assess the impact, and notify the relevant authorities. For more information, read the XYZ Incident Response Plan.	XYZ Corp Incident Response Plan.pdf
Control External Sharing	Determine who can share data externally, what data can be shared, and how to ensure security of data shared externally, such as the use of data loss prevention (DLP) policies or secure guest access. Include details on how users can securely share data externally, including encrypted emails or secure file transfer protocols.	Only authorized staff at XYZ Corp can share data externally, using secure methods such as encrypted emails or secure file transfer protocols.	XYZ Corp Data Loss Prevention Policy.pdf
Define backup and recovery process	Detail how data will be backed up and the process for data recovery in case of a disaster.	All Teams data at XYZ Corp is backed up daily, with a recovery process in place to restore data in case of a disaster. Refer to the XYZ Corp Backup and Recovery Policy for more information.	XYZ Corp Backup and Recovery Policy.pdf
Establish Change Management	Define who approves changes, how they are communicated, how they are implemented and steps to take when handling unexpected changes or emergencies.	The IT department at XYZ Corp approves changes, communicates them via company-wide emails, and implements them during off-peak hours to minimize disruption.	XYZ Corp Change Management Policy.pdf
Section 4: Ongoing training, adoption, and review			
Establish accessibility guidelines	If your organization needs to comply with accessibility regulations, include guidelines for ensuring all Teams content is accessible.	All Teams content at XYZ Corp is created following the WCAG 2.1 guidelines to ensure accessibility.	WCAG 2.1 guidelines.pdf

Action Item	Instructions	Action Plan	Important links
User Support	Define how users can get help with Teams, whether there's a dedicated support team, and any self-help resources available.	XYZ Corp has a dedicated IT support team available during business hours via email, phone, and chat.	
Establish performance monitoring	Define how the performance of Teams will be monitored and maintained. This includes monitoring system performance such as network bandwidth, user activity, usage trends, and response times. Establish thresholds for performance indicators to ensure optimal operation and user experience. Detail how often performance will be reviewed, who will be responsible for this task, and what actions will be taken if performance falls below acceptable levels. Outline how performance data will be reported and used to enhance Teams' efficiency and effectiveness.	XYZ Corp's IT department monitors Teams performance, including network bandwidth, user activity, usage trends, and response times, on a monthly basis.	
Train employees	Develop and implement training programs to ensure employees know how to use Teams effectively and safely. Establish refresher trainings when there are significant changes to Teams or your policies.	XYZ Corp conducts quarterly training programs to ensure employees know how to use Teams effectively and safely.	
Create dispute resolution policies	Define how disputes related to Teams use will be resolved. Establish who makes the final decision when there are disagreements over how Teams should be used or who can have access.	Any disputes related to Teams use at XYZ Corp are resolved by the IT Department Head in consultation with the HR and Legal departments.	
Establish review process	Determine how often the plan should be reviewed, who will be involved in the review process, and how updates will be communicated.	The governance plan at XYZ Corp is reviewed annually, with updates communicated via email and team meetings.	
Set up an ongoing audit process	Establish a system for regular audits of Teams usage and policy compliance.	XYZ Corp conducts bi-annual audits of Teams usage and policy compliance.	
Define reporting requirements	Determine what reporting will be needed and who will be responsible for it.	The IT department at XYZ Corp generates monthly reports on Teams usage, which are shared with the Senior Management team.	