Benevity Teams App

Security & IT Admin Guide

Self-Help Reference for Enterprise Security and IT Administrators

August 2026 | Version 1.2

1. Introduction

This guide is written for the security architects, IT administrators, and compliance officers at organizations that use Benevity's corporate social responsibility (CSR) platform and are evaluating or deploying the Benevity Microsoft Teams App.

It is designed to answer the most common questions your security and IT teams will have — covering permissions, authentication, data handling, telemetry, infrastructure, and administrative controls — so you can make an informed deployment decision and configure the app to meet your organization's security requirements.

1.1 What is the Benevity Teams App?

The Benevity Teams App is a Microsoft Teams-native extension that allows employees to discover and participate in CSR activities — such as charitable giving, volunteer opportunities, and matching programs — directly within Microsoft Teams, without leaving their existing workflow.

Users at your organization can publish opportunities to specific Teams channels. Employees can view, initiate, and complete CSR actions from within Teams on desktop, mobile, and web.

1.2 Deployment Model

Attribute	Details
Distribution	Microsoft Teams App Store (multi-tenant, organization-wide, or user-assigned)
App type	Microsoft Teams app with a conversational bot (personal and team scopes)
Bot hosting	Google Cloud Platform (Cloud Run) — serverless, auto-scaling container
Channel connector	Azure Bot Service — routes Teams messages to the bot endpoint
Identity provider	Microsoft Entra ID (Azure AD) — multi-tenant OAuth 2.0 / OIDC
Supported platforms	Teams Desktop (Windows/Mac), Teams Web, Teams Mobile (iOS/Android)
Target release	Beta: August 2026 | General Availability: October 2026

1.3 Microsoft Teams Store Distribution and Tenant Deployment Controls

Benevity for Microsoft Teams is distributed exclusively through the official Microsoft Teams Store. It is not distributed via sideloading or custom organizational app upload. This distinction matters for your security evaluation.

What the Teams Store distribution model means

Benevity for Microsoft Teams is listed in the official Microsoft Teams Store, independently verifiable at: https://teams.microsoft.com/l/app/c18f8179-ee22-4b1d-96e9-50f114a13ba6

Before any app is listed in the Teams Store, Microsoft validates it against a defined set of security, functionality, and compliance requirements. For Benevity for Microsoft Teams, that review includes:

- Verification that the Graph permissions requested match what the app's functionality actually requires -- no extra scopes are permitted
- Identity verification of Benevity as a publisher through Microsoft Partner Center, including business verification and domain confirmation
- Functional testing across 400+ test cases covering behavior, user experience, and security
- Ongoing automated health checks after publication; Microsoft can remove an app from the Store if issues are identified and not resolved

This review is not a one-time gate. Microsoft monitors published apps continuously and contacts developers when issues are detected.

Publisher Attestation

Benevity is completing Microsoft's Publisher Attestation program, which requires a formal self-assessment of data handling practices, security posture, privacy controls, and support commitments. Once complete, attested status will surface directly in the Teams Admin Center, giving your IT team on-demand access to this information. Publisher Attestation is targeted for General Availability in September 2026.

Your deployment controls

Your organization's Microsoft 365 administrator controls exactly which users can access the app and when. No employee can install or interact with Benevity for Microsoft Teams until your admin takes affirmative action to allow it.

The standard deployment pattern for enterprise organizations is a ringed rollout:

Stage	Mechanism	Who Has Access
Evaluation	App Permission Policy assigned to named users	IT/security reviewers only
Pilot	App Permission Policy expanded	Defined pilot population
Broad rollout	Org-wide policy or expanded assignment	All intended users

App Permission Policies are configured in the Microsoft Teams Admin Center (admin.teams.microsoft.com). Note that Teams assigns these policies to individual users rather than Azure AD security groups -- your admin will need to enumerate the specific accounts for each stage.

Until your admin enables the app and a user explicitly links their Benevity account, the app has no access to your tenant data or interaction with your employees.

1.4 App Behavior by Deployment Stage

The app's capabilities are gated by two sequential conditions: your administrator allowing the app in your tenant, and individual users linking their Benevity accounts. The table below describes exactly what the app can and cannot do at each stage.

Stage	What the app can do	What the app cannot do
Allowed in Teams Admin Center; no users linked	Nothing. The app is listed in your tenant's app catalog but holds no active permissions and has no user context.	Access any user data, send any messages, or interact with any employee.
Admin account linked; employees not yet granted access	Any linked user can donate, register for volunteer events, and publish Benevity opportunities to Teams channels where they have posting rights.	Access employee accounts, install itself for any user, or take any action without an admin explicitly initiating it.
Active employee users	Linked employees can donate and register for volunteer events from within Teams. Each action requires the employee to initiate it.	Read messages or files, access any data outside the explicit permissions in Section 2, or act on behalf of any user other than the one actively using the app.

No background processes run between user interactions. The app does not poll your tenant, send data to Benevity systems, or perform any action unless a user or admin has actively initiated it in that session.

2. Microsoft Graph API and Teams Permissions

This section lists every permission the app declares or requests, its type, and its business justification.

2.1 Teams App Manifest Permissions

These are declared in the app manifest and are visible to your administrator in the Teams Admin Center when reviewing the app.

Permission	Scope	Why We Need It
identity	Teams app	Receive the employee's basic Teams identity (display name, email, Entra object ID, tenant ID) in the bot activity payload. No directory lookup or Graph call is performed.
messageTeamMembers	Teams app	Allow the bot to open a one-to-one chat with a member of a team where the app is installed. This is how a Donate or Sign Up action taken on a shared channel card is moved into a private conversation, so no transaction detail is visible to other channel members.

2.2 Resource-Specific Consent (RSC)

For team and channel-scoped functionality, the app uses Resource-Specific Consent (RSC), which limits permission grants to specific teams or chats rather than the entire organization:

RSC Permission	Scope	Purpose
ChannelSettings.Read.Group	Team	Read channel settings (for example, channel name) for the team where the app is installed, so published opportunities are routed to and correctly labelled with the intended channel. Read-only. Grants no access to channel messages.

The app requests no permission to read channel or chat message content, in any scope.

2.3 Application (App-Only) Graph Permission

The app requests one application-level Microsoft Graph permission:

Permission		
TeamsAppInstallation.ReadForUser.All	Application (app-only)	Determine whether an employee has personally added the Benevity app in Teams. When they act on an opportunity shared in a channel without having added the app, this allows the app to guide them through installation and account linking before they can enter a donation or volunteer flow.

What this requires from your organization:

- A Global Administrator or Application Administrator must grant tenant-wide admin consent for this permission, via a consent URL Benevity provides.
- This consent is separate from allowing the app in the Teams Admin Center. Allowing the app in Teams does not grant it.
- Consent is per tenant. Consent in one organization's tenant does not apply to another's.
- The app's query is filtered to the Benevity app ID only. It does not enumerate other apps your employees have installed.
- If consent is not granted, Microsoft Graph returns HTTP 403 and the install check does not run. The app falls back to its existing behaviour rather than failing.

2.4 Permissions Explicitly Not Requested

The following high-privilege permissions were evaluated and deliberately excluded from the app's permission model. Each represents a meaningful reduction in risk surface.

Permission	Risk Avoided	Why It Is Not Needed
Delegated Microsoft Graph permissions	Allows the app to read or act on a user's Microsoft 365 data on their behalf	The app does not call Microsoft Graph as the signed-in user. Employee identity is supplied by Teams in the bot activity

		payload, and Benevity account access is authenticated separately through Benevity's own identity provider.
User.Read.All / Directory.Read.All	Directory-wide access to user data across the tenant	No directory access is required. Identity attributes come from the Teams activity payload for the employee actively using the app.
Mail.Read / Files.Read.All	Access to mailbox and file content	The app has no email or file functionality.
Permission to install or uninstall the app for users	Allows the app to add or remove itself for employees without admin action	The Graph permission requested in Section 2.3 is read-only. App installation remains controlled entirely by your Microsoft 365 administrator and your employees. The app cannot install itself.
Teamwork.Migrate.All	Broad ability to import or modify Teams messages at scale	Only standard user-initiated message posting is required.

3. Authentication & Identity

3.1 Sign-In Flow

The Benevity Teams App uses the industry-standard OAuth 2.0 Authorization Code flow with PKCE (Proof Key for Code Exchange) for user authentication. No passwords are transmitted to or stored by Benevity.

- Employee interacts with Benevity app in Teams.
- The app redirects to Microsoft's identity platform (login.microsoftonline.com) for sign-in.
- The user authenticates with their existing Microsoft 365 credentials – including any MFA policies your organization has configured.
- Microsoft issues an access token and a refresh token scoped to the permissions listed in Section 2.
- The app uses these tokens to call Microsoft Graph on behalf of the user. Tokens are never stored in the bot database – they are cached in memory for the duration of the session only.

3.2 Multi-Tenant Architecture

The app is registered as a multi-tenant application in Microsoft Entra ID. This means:

- Each customer organization has its own isolated sign-in flow via its own Entra ID tenant.
- User data from one tenant is never accessible to users or admins in another tenant.

- Your organization's Conditional Access policies, MFA requirements, and device compliance policies are enforced by Microsoft at sign-in — Benevity does not bypass these controls.

The relationship between Microsoft 365 tenants and Benevity clients is strictly one to one. Each Microsoft 365 organization (tenant) is mapped to exactly one Benevity client, and each Benevity client is mapped to exactly one tenant.

> **Single Sign-On:** *The app supports Microsoft Teams SSO. Users who are already signed into Teams are not prompted to sign in again — Teams silently passes an authentication token to the app, providing a seamless experience without additional credential entry.*

3.3 Token Handling

Token Type	Lifetime	Storage
OAuth Token (Auth0)	Default configuration	GCP Storage

3.4 Your Conditional Access Policies Are Respected

Because authentication is handled entirely by Microsoft Entra ID, all Conditional Access policies you have configured in your tenant apply automatically to the Benevity Teams App. This includes:

- Multi-factor authentication (MFA) requirements
- Device compliance and Intune-managed device policies
- Location-based access restrictions (named locations, IP ranges)
- Sign-in risk policies (Microsoft Entra ID Protection)

Benevity does not implement a separate identity layer that could circumvent these controls.

4. Data Handling & Privacy

4.1 Data Collected by the App

Data Category	Examples	Purpose	Retention
User profile	Name, work email, company, preferred language	Personalize app experience; pre-fill forms	Session only; not stored persistently
CSR transaction data	Donation amount, nonprofit, volunteer event registered	Process and confirm CSR actions; generate tax receipts	Retained in the Benevity platform per your data processing agreement
Teams context	Team name, channel name, chat roster	Route published opportunities to the correct channel	Not persisted – used transiently during publish action
Telemetry events	Anonymized event IDs (e.g., opportunity viewed, action initiated)	Product analytics and system health monitoring	1 year for operational logs; up to 7 years for usage analytics

4.2 Data NOT Collected

> **Benevity does not collect:** *Email message content, file contents, calendar events, personal chat messages outside of bot interactions, browsing history, device information, or any data outside the explicit permissions listed in Section 2.*

4.3 Data Residency & Storage

The Benevity Teams App infrastructure runs on Google Cloud Platform (GCP). Data residency regions are configured per your organizational agreement with Benevity. By default:

Data Type	Location	Provider
Bot runtime (in-memory)	GCP us-central1 (or contractual region)	GCP Compute
Application secrets	GCP Secret Manager	GCP
Telemetry/analytics events	GCP Cloud Storage + Data Lake	Google Cloud Platform
CSR transaction records	Benevity platform (region per your DPA)	Benevity (AWS or GCP)

5. Telemetry & Usage Analytics

The Benevity Teams App collects product telemetry to measure feature adoption, identify usability issues, and monitor system health. This section describes exactly what is collected, how it is anonymized, and where it goes.

5.1 Telemetry Events Collected

Event	What is Captured	What is NOT Captured
Opportunity Viewed	Event type, timestamp, surface (channel/chatbot/tab), anonymized opportunity ID	Employee name, personal details, browsing context outside Teams
Action Initiated	Event type, timestamp, action type (donate/volunteer)	Amount, charity, or any transaction content
Inputs Submitted	Event type, timestamp, form completion indicator	Form field values, amounts, and personal inputs
Validation Failed	Error category (not error message content), timestamp	User input content
Transaction Submitted	Event type, timestamp, transaction reference (opaque ID)	Amount, payment method, and personal data
Outcome Resolved	Outcome category (success/failed/blocked), timestamp, duration	Transaction content or personal data
Redirection to Web	Event type, timestamp	Destination URL parameters or user data
Admin Publish Action	Event type, timestamp, success/failure flag, tenant ID	Channel content or employee data
Interaction Latency	Response time in milliseconds	No user data – performance metric only

5.2 Anonymization

- User IDs are used in telemetry events. They are in UUID4 format.
- Tenant IDs are included to enable per-organization analytics, but are stored separately from event payloads in the data lake.
- No message content, form values, amounts, or personal data is included in any telemetry event.

5.3 Telemetry Pipeline

Telemetry events flow from the Cloud Run bot service through the following pipeline:

- Stored in GCP Cloud Storage partitioned by date, tenant, and event type.

Operational metrics (error rates, latency) are sent to GCP Cloud Monitoring with alert policies; no user data is included in these metrics.

6. Infrastructure & Security Controls

6.1 Architecture Overview

Component	Technology	Security Control
Bot service runtime	GCP Cloud Run (serverless containers)	No persistent state; ephemeral containers; auto-scaled; HTTPS enforced (TLS 1.2+)
Teams channel connector	Azure Bot Service (channel registration only – no code hosted here)	HMAC signature verification on every incoming Teams message
Secrets management	GCP Secret Manager	No secrets in code or environment variables; Managed Identity access; audit logs retained 90 days
Container images	GCP Artifact Registry	Vulnerability scanning enabled; zero critical CVEs policy before deployment
CI/CD pipeline	GitHub Actions + GCP Workload Identity	No long-lived service account keys; OIDC-based authentication; production requires 2-reviewer approval

6.2 Network Security

- All communication between the Teams client and the bot service uses HTTPS (TLS v1.2 minimum, TLS v1.3 preferred).
- The bot endpoint on Cloud Run validates the Bearer token on every incoming request from Azure Bot Service before processing any message.
- HMAC signature verification is applied to all Bot Framework activity payloads to prevent spoofing.
- CORS is configured to allow only known Microsoft Teams origins.
- The Cloud Run service does not expose any administrative APIs publicly.

6.3 Vulnerability Management

- All container images are scanned for known CVEs via GCP Artifact Registry scanning before deployment.
- Dependency vulnerability scanning (npm audit) runs in every CI/CD pipeline execution. Critical vulnerabilities block deployment.
- Benevity's security team conducts quarterly penetration tests on the Teams App infrastructure.
- Security patches are applied within 30 days of disclosure for medium/high severity; within 7 days for critical.

6.4 Compliance & Certifications

Benevity maintains the following certifications relevant to the Teams App. Current certificates are available upon request from your Customer Success Manager.

Certification / Standard	Status	Scope
SOC 2 Type II	Certified	Benevity platform and infrastructure, including Teams App services
Microsoft Teams Store Listing	Complete	App validated and published to the official Microsoft Teams Store
Microsoft Publisher Attestation	Pending (GA target)	Formal self-assessment of data handling practices, security posture, privacy controls, and support commitments; surfaces in Teams Admin Center upon completion
Microsoft 365 App Certification	Planned (post GA)	Third-party audit against Microsoft compliance framework covering security, data protection, and operational controls
ISO 27001	In scope for the CY 2026 audit	Information security management system

This document is proprietary and confidential to Benevity.

7. IT Admin Controls & Deployment

7.1 Granting Permissions in Your Tenant

As a Teams Administrator, you control whether and how the Benevity Teams App is available to users in your organization.

1. Sign in to the Microsoft Teams Admin Center (admin.teams.microsoft.com) with Teams Administrator credentials.
2. Navigate to Teams apps → Manage apps and search for "Benevity".
3. Navigate to Permissions → Grant admin consent
4. Set the app status to Allowed for your organization.
5. Navigate to Teams apps → Permission policies to control which users can install the app.
6. Navigate to Teams apps → Setup policies to optionally pin the app for specific user groups.

7.2 Restricting the App to Specific Users

To limit the app to a pilot group or specific departments before an organization-wide rollout:

1. In Teams Admin Center → Teams apps → Permission policies, create a new policy.
2. Under Microsoft apps and Third-party apps, set to "Allow specific apps" and add Benevity.
3. Assign the policy to the target user group via Teams admin or Entra ID group assignment.
4. Users outside the assigned group will not see the app in the Teams store.

7.3 Removing the App

To remove the Benevity Teams App from your organization:

1. In Teams Admin Center → Teams apps → Manage apps, set the app status to Blocked.
2. Existing bot conversations and channel messages will remain, but the app will no longer be functional.
3. To remove the app's consent grants, navigate to Microsoft Entra ID admin center → Enterprise applications → search for Benevity → Permissions → Revoke admin consent.

Revoking consent will sign all users out of the app immediately. User consent grants will also be cleared, requiring users to re-consent on their next sign-in if the app is re-enabled.

7.4 Data Deletion & Off-boarding

When an employee leaves your organization, their Microsoft 365 account is disabled or deleted in Entra ID. The Benevity Teams App will automatically reject any token refresh attempts for that user, effectively revoking their app access within one hour (the access token lifetime).

To request deletion of a specific user's personal data held by Benevity in accordance with GDPR Article 17 (right to erasure), submit a data subject access request via your Benevity Customer Success Manager or at privacy@benevity.com.

This document is proprietary and confidential to Benevity.

8. Frequently Asked Questions

Can the app read our employees' emails or Teams messages?

No. The app does not request Mail.Read or any permission to access email content. It can only send messages to chats and channels where it has been explicitly added, and it can read basic roster information (names and emails of chat members) within those specific chats. It cannot read historical messages.

Does the app store Microsoft 365 credentials or passwords?

No. The app uses OAuth 2.0 and never receives or stores passwords. Authentication is handled entirely by Microsoft's identity platform. The app only receives access tokens and refresh tokens, which are time-limited and revocable.

Can Benevity employees access our users' data?

Benevity engineering and support staff access production systems only via break-glass procedures with full audit logging. Access is role-based, requires approval, and is logged to an immutable audit trail. Benevity does not perform ad-hoc queries on customer data outside of agreed support scenarios.

Is the app available in Government or GCC High environments?

The current release supports Microsoft 365 commercial cloud tenants. Government Community Cloud (GCC) and GCC High support is on the roadmap. Contact your Benevity account team for current availability and timelines.

Does the app work with our MFA / Conditional Access policies?

Yes. Because authentication is handled by Microsoft Entra ID, all your existing Conditional Access policies — including MFA, device compliance, and location-based restrictions — apply automatically. Benevity has no ability to bypass these controls.

Where is the telemetry data stored, and can we request it be excluded?

Telemetry is stored in GCP Cloud Storage and BigQuery in the region specified in your agreement (default: US).. Enterprise customers can discuss telemetry reduction options with their Customer Success Manager. See Section 5 for full details.

What happens if Benevity has a security incident?

Benevity will notify affected customers within 72 hours of confirming a personal data breach, in accordance with GDPR requirements and your Data Processing Agreement. A dedicated incident response team and runbook are maintained. Notification will be sent to the security contact registered in your Benevity account.

Does the app support DLP (Data Loss Prevention) policies?

The app communicates through standard Microsoft Teams bot framework channels, which are subject to your organization's Teams DLP policies configured in the Microsoft Purview compliance portal. Benevity does not intercept or bypass DLP controls.

9. Contacts & Further Information

Query Type	Contact	Response SLA
Security questions & vulnerability reports	security@benevity.com	1 business day
Data privacy & GDPR / data subject requests	privacy@benevity.com	3 business days
Penetration test approval requests	security@benevity.com	5 business days
Data Processing Agreement (DPA) requests	Your Benevity Customer Success Manager	3 business days
General IT admin support	support.benevity.com	Per your support tier SLA
Compliance certificates (SOC 2, ISO)	Your Benevity Customer Success Manager	5 business days

9.1 Useful Links

- Benevity Teams App listing in Microsoft Teams store: https://teams.microsoft.com/l/app/c18f8179-ee22-4b1d-96e9-50f114a13ba6
- Microsoft Teams Admin Center: https://admin.teams.microsoft.com
- Microsoft Entra ID Admin Center: https://entra.microsoft.com
- Benevity Trust & Security: https://benevity.com/security
- Benevity Privacy Policy: https://benevity.com/privacy
- Microsoft Graph Permissions Reference: https://learn.microsoft.com/en-us/graph/permissions-reference

This document is proprietary and confidential to Benevity.