# Teams (Public)

## Understanding Teams in Keeper

### What Are Teams in Keeper?

**Teams** in Keeper are groups of users that simplify the management of **shared folders, permissions, and security policies** within an organization. Instead of assigning permissions individually, you can manage access at a team level, ensuring a scalable and efficient way to handle credentials.

### How Teams Are Used in Keeper

- **Access Control:** Assign users to teams to **control who can view, edit, or share records** in shared folders.
- **Simplified User Management:** When a new employee joins a department, adding them to the relevant team automatically **grants them access** to the right records.
- **Security & Compliance:** Teams help enforce **least privilege access**, ensuring users only have access to what they need.
- **Role-Based Management:** Teams can be paired with **Roles** to enforce specific security policies, such as requiring **MFA for sensitive teams** (e.g., Finance or HR).

---

## Best Practices for Using Teams

### **1.** Align Teams with Business Departments or Functions

Create teams based on **departments** (e.g., Finance, IT, Sales) or **job functions** (e.g., Support Staff, Developers) to ensure proper access control.

### **2.** Use Teams to Manage Shared Folder Access

Instead of assigning access individually, **grant shared folder permissions to teams**. This makes onboarding and offboarding users easier.

### **3.** Implement Security Policies per Team

For teams handling sensitive information (e.g., Finance, HR, IT), **enforce additional security measures** such as:

- Requiring **multi-factor authentication (MFA)**
- Restricting **record sharing outside the organization**
- Enabling **audit logs** for monitoring access

## **4.** Regularly Review and Update Team Memberships

Ensure that **only the right users** are part of each team. Remove old members immediately when they leave or change roles.

## **5.** Combine Teams with Roles for Fine-Grained Access Control

- **Teams** control access to **specific records and shared folders**
- **Roles** define **what users can do** (e.g., enforce MFA, restrict sharing)
  Using them together ensures better security and usability.

---

# Example Team Structure

For a small SME where **Globe2 handles global administration**, an efficient **team structure** could look like this:

| Team Name | Purpose | Example Access |
|---|---|---|
| **Management** | Executive team members who need access to company-wide credentials. | Access to all **business-critical logins** (e.g., banking, contracts, key systems). |
| **IT / Security** | Internal IT lead or security champion. | Access to **infrastructure-related credentials** (e.g., servers, domain registrations, cloud services). |
| **Finance & HR** | Handles financial data, payroll, and HR systems. | Access to **accounting software, payroll systems, and sensitive employee data**. |
| **Sales & Marketing** | Manages CRM, social media, and marketing tools. | Access to **CRM, social media accounts, and marketing automation tools**. |
| **Operations & Support** | Handles daily business operations and customer support. | Access to **support platforms, scheduling tools, and inventory systems**. |

## How This Structure Works in Practice

- A new **sales employee** joins → They are added to the **Sales & Marketing Team**, automatically gaining access to **CRM & social media credentials**.
- An **HR team member** needs payroll software access → They are added to the **Finance & HR Team**.
- The **business owner** gets visibility over **Management Team** credentials but cannot manage users or licenses.

---

Revision #2
Created 16 March 2025 19:53:26 by Doug

Updated 24 March 2025 14:56:10 by Doug