100 XP

Secure Microsoft Teams with three tiers of protection

3 minutes

In every company, data of different types is likely to require different levels of protection. For example, your physical locations, addresses, and reception phone numbers should be public, but employee details should be carefully protected.

Suppose you want to analyze the data that will be stored in Teams and classify it so that you can plan how much protection to implement. You want to harden your Teams data as much as possible without reducing productivity or inconveniencing customers.

Here, you'll learn about Microsoft's recommended three tiers of protection for data in Teams.

Classify and secure data in three tiers

Microsoft recommends three tiers for protecting data, identities, and devices. The three tiers are:

- Baseline
- Sensitive
- Highly sensitive

Based on these three tiers, the table below shows four configurations for Microsoft Teams and their associated SharePoint sites. The baseline tier has two options: one for public teams and one for private teams. Use this as a guide and adjust the configurations to meet your organization's requirements. You might not need every tier.

Setting	Baseline (public)	Baseline (private)	Sensitive	Highly sensitive
Team	Public	Private	Private	Private
Restrict access to	In-tenant users, including B2B users	Members of the team, others can request access	Members of the team	Members of the team

Setting	Baseline (public)	Baseline (private)	Sensitive	Highly sensitive
Create private channels	Owners and members	Owners and members	Owners	Owners
Site-level guest access	New and existing guests (default)	New and existing guests (default)	New and existing guests *or* only people in your organization, depending on your needs	New and existing guests *or* only people in your organization, depending on your needs
Site sharing	Site owners	Site owners	Site owners	Site owners
Files and folder sharing	Owners, members, and people with edit permissions	Owners, members, and people with edit permissions	Owners, members, and people with edit permissions	Site owners, access requests Off
Site-level unmanaged device access	Full access from desktop apps, mobile apps, and the web (default)	Full access from desktop apps, mobile apps, and the web (default)	Limited, web-only	Block access
Default sharing link type	People in your organization	People in your organization	Specific people	People with existing access
Sensitivity labels	None	None	Used to classify the team, control guest sharing, and unmanaged device access. Label can also be used to encrypt files.	Used to classify the team, control guest sharing, and unmanaged device access. Label can also be used to encrypt files.

Learn more

- Configure Teams with three tiers of protection

Next unit: Knowledge check

Continue