

Deploy CMMC Teams/SharePoint Procedure

Disclaimer and Limitation of Liability

The Microsoft SharePoint site template (“Template”) provided by Pentakt LLC is offered as a free resource for informational and convenience purposes only. By accessing, downloading, or using this Template, you acknowledge and agree that Pentakt LLC makes no representations or warranties of any kind, express or implied, regarding the accuracy, completeness, suitability, or effectiveness of the Template for achieving compliance with any regulatory framework, including but not limited to Cybersecurity Maturity Model Certification (CMMC) requirements.

Use of the Template does not guarantee compliance with CMMC or any other federal, state, or industry-specific standards. Compliance obligations vary based on individual circumstances, and it is the sole responsibility of the user to assess, implement, and validate any controls, policies, or procedures necessary to meet applicable requirements.

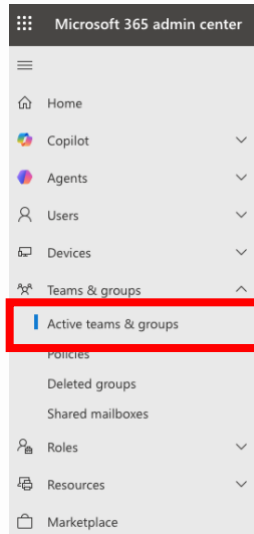
The Template is provided “as is” and “as available,” without warranty of any kind. To the fullest extent permitted by law, Pentakt LLC expressly disclaims all liability for any direct, indirect, incidental, consequential, or special damages arising out of or in any way connected with the use of, or reliance on, the Template.

By using this Template, you agree that Pentakt LLC shall not be held liable for any compliance determinations, audit outcomes, certification results, or any damages or losses resulting from the use or misuse of the Template. You further agree that you use the Template entirely at your own risk.

1. Provision a M365 Team and SharePoint.


STOP! You can also skip to Step 2 to provision the Teams/SharePoint AND deploy site template with the script. Your choice.

- Navigate to admin.microsoft.com (Commercial Tenant) or portal.office365.us/adminportal (GCC/GCC-H Tentant)
 - **Reminder**: Compliance documentation is NOT CUI/ Store in whichever Tenant you have/wish.
- Log in
- On the left menu, click “Show All” and drop down “Teams and Groups”
- Select “Active Teams and Groups”




-
- Select “Add a Team”

Active teams and groups

 About Groups  Using Teams And SharePoint  Where to store files

Teams & Microsoft 365 groups Distribution list Security groups

 Add a team  Add a Microsoft 365 group  Export  Refresh

- - Fill in the prompted information:
 - Name of Team: CMMC
 - Owners: Usually IT and/or Compliance
 - Members: Add all in-scope personnel in your tenant (you can add more later)
 - Team email address: cmmc@yourdomain.com
 - This allows IT or Compliance to mass email updates
 - Privacy: Public (you choose based on the scope of your people)
 - Review and Finish
 - Select “Add a Team”
 - Await provisioning, verify you can view Team and SharePoint
2. Add Site Template to your Microsoft Tenant (AND deploy Teams/SharePoint if not previously deployed):
- Prerequisite: Must have PowerShell 7 and up to date PNP. Script will check and update as required.
- Right click on run.ps1
 - Select Run with PowerShell
 - Complete prompted information
 - STAY by your PC. Every action in script requires credentials.

3. Set up Teams Channels

- We recommend creation of 3 channels within Teams
- Navigate to your Team in Teams.
- Select the 3 menu dots next to your Team name and Select Add Channel
- First channel name is “Change Management Logs”
 - i. Channel Type: Private
 - ii. Layout: Posts
- Second channel name is Cyber Awareness
 - i. Channel Type: Public
 - ii. Layout: Posts
- Third Channel is Publication Review
 - i. Channel Type: Private
 - ii. Layout: Posts

4. Templates for Change Management Logs channel

- Create a Loop Component post
 - i. Click into the channel
 - ii. Select Post in Channel button on the bottom
 - iii. Lower left of the post, next to the emoji icon, select the Loop Component Icon
 - iv. This converts your post to a loop which makes it continuously editable
- In the loop component, use the following template:

Title of Change:

Change Type:

Change Status:

===== Approval =====

Initiated?

Requested?

Approved?

Approval Decision date

===== Change Details=====

Summary of Change:

Purpose of the Change:

Type of Configuration Change:

Backup plan:

Impact of This Change:

Systems/Components Impacted:

Documentation, Training, or Configuration Records Updates?

=====Compliance Questions =====

Were any configurations not performed per policy?

Was the Hardware Inventory Updated?

Was the Software Inventory Updated?

Did you capture new system baselines? Where?

Does any training, procedures, or documentation need to be updated?

Do any software/license inventories need to be updated?

5. Template for Publication Review channel

- Create a Loop Component post
 - i. Click into the channel

- ii. Select Post in Channel button on the bottom
 - iii. Lower left of the post, next to the emoji icon, select the Loop Component Icon
 - iv. This converts your post to a loop which makes it continuously editable
 - In the loop component, use the following template:
<CONTENT TO BE PUBLICALLY POSTED>
Author:
Reviewer:
Poster:
Does this content contain FCI/CUI?
Does this content contain propriety information?
 - Tag users using "@" that are the reviewer and poster so they are notified
 - Content is not considered approved until the Reviewer comments Approved.
6. The Cyber Awareness channels is meant more for users to post screenshots of phishing email or any cybersecurity concerns that all users in the organization can see and assist each other with.
- Not a direct CMMC requirement, but our clients love this channel, and it improves security and awareness without the need for phishing simulations.