cloudcontext

Microsoft Copilot Deployment Checklist

Essential security and access checks for a safe Copilot deployment.

1. Confirm Your Data Is Ready

Before Copilot touches anything, make sure your data house is in order.

- [ ] Review SharePoint, OneDrive & Teams permissions
- [ ] Remove broad access groups like "Everyone" where not required
- [ ] Identify sensitive data locations (HR, payroll, exec docs)
- [ ] Fix legacy or forgotten permissions
- [ ] Validate that users only have access to what they genuinely need

2. Run a Security & Data Health Assessment

This is not optional. It's the foundation of a safe deployment.

- [ ] Perform a security assessment of Microsoft 365
- [ ] Perform a data health assessment across key workloads
- [ ] Identify overshared content and risky permissions
- [ ] Address findings before enabling Copilot for users

3. Lock Down Identity & Access

Copilot relies heavily on identity. Weak identity controls equal big risk.

- [ ] Enforce Multi-Factor Authentication (MFA) for all users
- [ ] Review and restrict conditional access policies
- [ ] Apply geo-blocking where appropriate
- [ ] Disable legacy authentication
- [ ] Ensure secure sign-in from compliant devices only

4. Apply Sensitivity Labels & Data Protection

Teach Copilot what matters by protecting your data properly.

- [ ] Define sensitivity labels (Public, Internal, Confidential, Highly Confidential)
- [ ] Apply labels to documents, sites, and Teams
- [ ] Ensure confidential data is not accessible by default
- [ ] Validate labels are enforced, not just created

5. Harden Your Endpoint & Tenant Security

Copilot should sit on top of a secure environment, not patch over gaps.

- [ ] Confirm Microsoft Defender is configured and active
- [ ] Review Attack Surface Reduction (ASR) rules
- [ ] Ensure endpoint compliance policies are enforced
- [ ] Validate devices accessing Copilot meet security standards

6. Review Admin & Privileged Access

Admins using Copilot without guardrails can see far more than intended.

- [ ] Implement Role-Based Access Control (RBAC)
- [ ] Use Privileged Identity Management (PIM) for admin roles
- [ ] Ensure admins are not permanently privileged
- [ ] Separate admin and day-to-day user accounts

7. Start Small With a Controlled Rollout

Do not deploy Copilot to everyone on day one.

- [ ] Select a pilot group with lower data risk
- [ ] Monitor Copilot prompts and outputs
- [ ] Gather feedback from real usage
- [ ] Fix issues before wider rollout

8. Educate Users Before Go-Live

Copilot is powerful. Users need guardrails, not just access.

- [ ] Explain what Copilot can and can't do
- [ ] Set expectations around data handling
- [ ] Provide simple usage guidelines
- [ ] Reinforce that Copilot follows existing permissions

Final Check

- [ ] Security reviewed
- [ ] Data permissions cleaned
- [ ] Identity locked down
- [ ] Pilot tested
- [ ] Users briefed

Then, and only then, deploy Copilot with confidence.

For help with Copilot deployment or security, visit our website or call us on 1300 364 703.