Microsoft Copilot Security and Governance Guide

Basic operating rules for safe, accountable Copilot use. Adapt them to your legal, contractual, and regulatory requirements.

01 Approved uses

Use Copilot for approved business tasks such as first drafts, summaries, meeting preparation, and analysis where a qualified person can review the result.

02 Prohibited uses

Do not use unapproved AI tools, bypass controls, impersonate a person, or make fully automated high-impact decisions.

03 Sensitive information

Use confidential, personal, regulated, credential, HR, legal, financial, or client information only when the tool, purpose, access, and location are approved.

04 Human review

A person remains accountable. Verify material facts, calculations, names, dates, sources, tone, and missing context.

05 Accuracy risks

Treat output as a draft. Copilot can produce false statements, incomplete summaries, bad citations, or stale information.

06 Permissions

Copilot can make permitted information easier to discover. Report unexpected access and do not search for information unrelated to your role.

07 Employee responsibilities

Use your assigned account, follow approved use cases, complete training, and report questionable results.

08 Client communications

A responsible employee must approve AI-assisted client communications before they are sent.

09 Documentation

For material decisions, retain source material, the reviewed output, reviewer, date, and approval under existing retention rules.

10 Role changes and departures

Promptly review groups, sites, Teams, mailboxes, OneDrive, sessions, devices, and administrative roles.

Minimum pilot governance

Owner	Business leader and technical contact
Scope	Approved users, use cases, tools, and data sources
Guardrails	Permissions review, MFA, policy, human review, reporting
Evidence	Baseline, target, issues log, and final decision

Talk to PCC Before Deploying Copilot | calpcc.com/contact-us/