State of Idaho Microsoft 365 Copilot: Best Practices

For Idaho State Government Employees

What You're Using

Product: Microsoft 365 Copilot for Government

Five Critical Security Rules

1. **Never Enter Highly Sensitive Data**
   - Do NOT enter: Confidential investigations, highly sensitive personnel matters, information that (if disclosed) could result in death, disability, or serious injury
   - Instead: Use appropriate systems designed for highly sensitive information
2. **Understand What Copilot Can Access**
   - Copilot can access your Outlook emails, SharePoint files, Teams chats, OneDrive documents, essentially anything YOU have permission to access
   - Copilot cannot access files you don't have permission to see
3. **Apply Sensitive Labels to All Documents**
   - Label documents appropriately: "Public," "Internal Use Only," "Confidential"
   - Why it matters: Copilot cannot access documents with encrypted sensitivity labels
   - User-defined permissions: Can block Copilot from accessing specific files
   - Action recommended: Label ALL government documents appropriately
4. **Review All Outputs Before Sharing**
   - Copilot can make mistakes or provide inaccurate information
   - Verify all facts independently before using
   - Check outputs for accuracy and appropriateness
   - You are responsible for what you send or share
5. **Do Not Ignore Data Loss Prevention Warnings**
   - STOP immediately at any warning message
   - Read and understand what triggered the warning
   - Never attempt to bypass security warnings
   - Contact IT if you have questions about a warning

Safety Checklist

Before Using Copilot:

- Is this content appropriate for AI assistance?
- Does the document have the correct sensitivity label?
- Do I have proper authorization to access this?

After Using Copilot:

- Have I verified the accuracy of outputs?
- Have I applied proper sensitivity labels?

Where Copilot Appears

Copilot is integrated into: Outlook, Word, Excel, PowerPoint, Teams, OneNote, SharePoint

Appropriate Use Guidelines

Task	Appropriate?	Notes
Drafting emails	Yes	Review output before sending
Summarizing email threads	Yes	If emails are at appropriate level
Creating Excel formulas	Yes	Verify formula works correctly
Analyzing data with proper labels	Caution	Only with appropriate labels applied
Summarizing meetings	Yes	If meeting was not confidential

Web Search Feature

Your IT administrator may enable or disable web search:

- If enabled: Queries may go to Bing (outside Microsoft 365 boundary)
- If disabled: Copilot only searches within your organization
- Check your agency or department's policy on web search usage

Conversation History

- Your Copilot conversations are retained for 30-90 days
- Conversations may be audited for compliance
- Treat Copilot conversations like work email
- Maintain professionalism in all interactions

Your Responsibilities

You are responsible for:

- Applying correct sensitivity labels to documents
- Following data classification and handling policies
- Verifying all Copilot outputs before using them
- Protecting citizen and employee privacy

Remember:

- Government version keeps data in specific regions
- Copilot can make mistakes, always verify facts

What Your IT Team Should Configure

Your IT administrator should have enabled:

- Single Sign-On with your state email address
- Multi-Factor Authentication recommendation
- Sensitivity labels and auto-labeling policies

- Data Loss Prevention rules and monitoring
- Audit logging and reporting

Questions? Contact your IT Help Desk or Security Team

Document Version: October 2025 | State Government Use