MICROSOFT TRAINING

Microsoft Copilot Security Courses

Master Microsoft Copilot security, protecting data and managing access effectively. Learn to deploy AI responsibly in enterprise environments.

DURATION
2 hours

LEVEL
Intermediate

FORMAT
Instructor-Led

- Globally Recognized Certification
- Expert-Led Hands-On Training
- Flexible Scheduling

Computer Pride | 1st Floor, ICEA Building, Kenyatta Avenue, Nairobi | www.computer-pride.co.ke

COURSE OVERVIEW

Microsoft Copilot is revolutionizing productivity, but integrating AI into your enterprise also introduces unique security and compliance challenges. This intermediate-level course, specifically designed for IT professionals, delves deep into securing your Microsoft Copilot deployment within the Microsoft 365 ecosystem. You will gain a comprehensive understanding of the security architecture underpinning Copilot, learning how to safeguard sensitive data, manage access, and ensure regulatory compliance as your organization leverages AI-powered productivity tools.

This course focuses on practical strategies and configurations for mitigating risks associated with AI interaction, data leakage, and unauthorized access. You'll explore core Microsoft security technologies such as Azure Active Directory (now Microsoft Entra ID), Microsoft Purview, and Microsoft Defender for Cloud Apps, specifically in the context of Copilot. By mastering these concepts, you will be equipped to implement robust security controls, protect intellectual property, and maintain data governance standards, ultimately enhancing your organization's trust and confidence in AI-driven productivity.

Duration	2 hours
Level	Intermediate
Vendor	Microsoft

COURSE CURRICULUM

01 Module 1: Introduction to Microsoft Copilot Security Landscape

- Understanding Copilot's Architecture and Data Flow
- Key Security and Privacy Considerations for AI Integration
- Identifying Potential Risks and Vulnerabilities with Copilot
- Overview of Microsoft's Shared Responsibility Model for Copilot

02 Module 2: Data Governance and Microsoft Purview for Copilot

- Implementing Data Loss Prevention (DLP) Policies for Copilot
- Utilizing Sensitivity Labels and Information Protection for AI-generated Content
- Configuring Data Lifecycle Management for Copilot Interactions
- Managing eDiscovery and Auditing for Copilot Activities

03 Module 3: Access Management and Authentication for Copilot

- Securing Access to Copilot via Microsoft Entra ID (Azure AD)
- Implementing Conditional Access Policies for AI Tools
- Managing Role-Based Access Control (RBAC) within Copilot Ecosystem
- Understanding Principle of Least Privilege in Copilot Deployments

04 Module 4: Threat Protection and Monitoring for Copilot

- Leveraging Microsoft Defender for Cloud Apps (MDA) for Copilot Shadow IT and DLP
- Detecting and Responding to Anomalous Copilot Usage
- Integrating Copilot Security Logs with Microsoft Sentinel
- Proactive Threat Hunting Strategies for AI Environments

05 Module 5: Compliance and Best Practices for Secure Copilot Deployment

- Ensuring Regulatory Compliance (GDPR, HIPAA) with Copilot
- Developing Internal Policies for Responsible AI Use

- Implementing Security Baselines and Hardening Guidelines for Copilot
- Continuous Monitoring and Optimization of Copilot Security Posture

CAREER PATHWAYS

Graduates of this program are prepared for the following roles:

> **Microsoft 365 Security Administrator specializing in AI governance**

> **Data Privacy Officer focusing on AI and Copilot compliance**

> **Information Security Analyst for Microsoft Cloud Environments**

FREQUENTLY ASKED QUESTIONS

Q: How will this course help me prevent sensitive corporate data from being inadvertently exposed by Microsoft Copilot?

This course provides practical knowledge on configuring Microsoft Purview's Data Loss Prevention (DLP) and sensitivity labeling specifically for Copilot. You'll learn to implement policies that automatically identify, classify, and protect sensitive information, ensuring that Copilot's interactions and generated content adhere to your organization's data governance standards, thereby significantly reducing the risk of accidental data exposure.

Q: What foundational knowledge or experience is recommended before enrolling in the Microsoft Copilot Security Courses?

To get the most out of this intermediate-level course, it is highly recommended that participants have a working understanding of Microsoft 365 administration, including familiarity with Microsoft Entra ID (formerly Azure AD), basic concepts of data governance, and an awareness of general cybersecurity principles. Experience with Microsoft Purview or Microsoft Defender products would be beneficial but is not strictly required as key concepts will be covered.

Q: What specific skills will I gain to implement security policies for Copilot within my organization?

Upon completion, you will be able to implement and manage access controls for Copilot users using Microsoft Entra ID and Conditional Access, configure data loss prevention policies and sensitivity labels via Microsoft Purview, monitor Copilot activities for compliance and threats using Microsoft Defender for Cloud Apps and Sentinel, and establish best practices for responsible AI usage to secure your organization's data and intellectual property.

ABOUT COMPUTER PRIDE

East Africa's Premier IT Training Center

With over 15 years of excellence, Computer Pride delivers globally recognized certification programs from leading technology vendors. Located on Kenyatta Avenue in Nairobi's CBD, our state-of-the-art facilities and expert instructors have empowered thousands of professionals across East Africa.

15+	10,000+	50+
Years of Excellence	Professionals Trained	Vendor Certifications

READY TO ENROL?

Take the next step in your technology career.

Location
1st Flr, ICEA Building
Kenyatta Ave, Nairobi

Email
info@computer-pride.co.ke

Phone
+254 705 900 900

www.computer-pride.co.ke