We solve IT

JEC TECHNOLOGIES GROUP

Your Checklist to Safe AI Practices with Microsoft Copilot

10 Ways to Stay Secure When Using AI

Artificial intelligence (AI) tools like Microsoft Copilot can transform the way your business operates, but ensuring the proper security measures are in place can be challenging, which can potentially put your data at risk. AI can expose your business to risks such as leaking sensitive information or, worse, leaving it vulnerable to a cyberattack. To help you securely integrate AI into your operations, here are 10 key steps to consider when your business uses an AI tool such as Microsoft Copilot.

1 Conduct a Security Audit

Schedule an audit of your current infrastructure before implementing AI into your operations. If you haven't done so yet, it's important to do this as soon as possible. The audit will help identify potential vulnerabilities in your current environment. It's recommended that this audit be conducted regularly, at least once a year, to stay ahead of any new risks that might show up. A third-party technology expert specializing in data risk assessments can help speed up this process and uncover any potential risks before your AI implementation.

2 Set Proper User Permissions

Assign specific roles and permissions to employees to control access to Copilot, ensuring only authorized users can interact with sensitive data. These established roles and permissions can greatly reduce the risk of misuse or accidental exposure of confidential information.

3 Use Sensitivity Labels

Apply sensitivity labels to AI-generated outputs, classifying data based on its level of confidentiality. These labels allows sensitive information to be handled with the appropriate level of protection, such as encryption and content markings.

4 Implement Data Access Controls

Limit access to AI outputs based on the job roles and responsibilities. Make sure that only those who need to see certain information can access it. This strategy will help minimize the potential for unauthorized access or internal data breaches.

5 Educate Your Team on Responsible AI Use

Conduct regular employee training sessions on how touse AI tools like Copilot, responsibly. Confirm they understand the importance of following security protocols and avoiding actions that could lead to data exposure or misuse.

6 Monitor User Prompts

Have a system in place to help track how your team is interacting with Copilot and what types of prompts they are using. Monitoring AI prompts that are used in AI tools ensures that individuals aren't inadvertently requesting or generating sensitive information in ways that could pose a potential security risk.

7 Regularly Review AI Activity Logs

Periodically review AI activity logs related to Copilot's use and be on the lookout for any unusual or suspicious actions that could escalate into a possible security threat.

8 Private vs. Public AI – Choose Wisely

When using generative AI tools, always choose secure, private options for handling sensitive business data. For example, Microsoft Copilot offers two versions: Web and Work. Make sure you and your team use the "Work" version to keep confidential information protected.

9 Use Multi-Factor Authentication (MFA)

Here's a classic one - enable phishing resistant multi-factor authentication for all users interacting with Copilot to add an extra layer of security. MFA requires users to verify their identity with more than just a password, reducing the likelihood of unauthorized access to your sensitive data or systems.

10 Stay Informed About AI Security Best Practices

AI is consistently evolving at at rapid rate, and so are the associated security challenges along with them. Stay up-to-date with the latest security best practices, especially those specific to AI and tools like Microsoft Copilot, so your business remains secure against the newest threats coming around the corner.

Secure Your AI Environment

By following this checklist, your business can reduce the risks associated with using AI tools like Microsoft Copilot and also strengthen your overall security posture. Taking proactive steps to protect your business and data is becoming the norm in today's digital landscape. To be fully prepared and equipped to handle any potential risks, consult with a technology expert who specializes in risk migration and cybersecurity. Together, you can build a robust, secure AI environment that allows your business to thrive with confidence in this competitive market.

https://www.jectech.co.za/ | 0108800070