DR EUNICE SARI, *Co-Founder of Customer Experience Insight*
LinkedIn/Website cxinsight.com.au

Eunice is a Digital Transformation Expert with 20-years of experience in global industries and academics

1. KNOWLEDGE ILLUMINATES

We need to empower our employees by educating them about Generative AI Security. While there is much information related to general security, train your employees on specific risks of Generative AI, primarily related to phishing attempts targeting AI data, data privacy concerns, responsible Generative AI and best practices for safe Generative AI usage. We will incorporate our privacy principles in the development and use of our AI technologies.

2. ENCRYPTION IS THE KEY

We need to secure the data storage pertinent to our generative AI system. Our system often deals with sensitive information. Thus, it is crucial to implement robust encryption methods for data at rest (stored) and in transit (being transferred). Cloud-based encryption solutions are one of the solutions that can be added to security and convenience.

3. TRUSTWORTHY TOOLS

We need to discern which Generative AI tools and models are from reputable vendors with a proven security track record. Not all AI tools and models are created equal. We must read the security documentation properly and verify its authenticity to avoid malware or compromised software.

4. PATCH IT UP

We need to keep our Generative AI system and framework up to date to ensure their security. To address vulnerabilities, we can update our Generative AI frameworks, libraries, and supporting software.

5. FOR YOUR EYES ONLY

We must limit access to our Generative AI systems and data to authorised personnel only. These people will be the gatekeepers who will control the security of our system. We must enforce strong authentication measures like complex passwords and multi-factor authentication (MFA) to access our system.

6. BACK UP AND BE AT EASE

We need to regularly back up any critical data our Generative AI System uses. We will allow notice and consent, and encourage architectures with privacy safeguards. This would give us peace of mind in case of a cyber-attack, system failure, or accidental data loss, allowing us to recover quickly.

7. ON THE LOOK OUT

We need to regularly monitor our Generative AI system for suspicious activity that might indicate unauthorised access attempts or attempts to exploit vulnerabilities in your Generative AI systems. We will design our AI systems to be appropriately cautious, and seek to develop them by best practices in AI safety research.

8. SPEAK UP!

We need to foster a culture of cybersecurity awareness in our business by encouraging open communication. We must ensure that your employees, business partners, and stakeholders feel empowered to discuss and express security concerns related to the Generative AI system.

9. CHECK AND RE-CHECK

We need to assess the security practices of our third-party vendors and service providers involved in our Generative AI solutions. Properly evaluating security protocols is critical to ensure that they meet our standards and do not introduce new and unknown security risks. In appropriate cases, we will test AI technologies in constrained environments and monitor their operation after deployment.

10. BE BUILT AND TESTED FOR SAFETY

We will continue to develop and apply strong safety and security practices to avoid unintended results that create risks of harm. Our goal is to design our Generative AI systems to be appropriately cautious. We will test our Generative AI technologies in constrained environments and monitor their operation after deployment.