CHANDIKA RAMDOSS *Data Governance and Security Specialist, BGC (Australia) Pty Ltd*
https://www.linkedin.com/in/chandikaramdoss/

Chandika drives data governance and security efforts, focusing on implementing effective data protection strategies and security measures. She enhances organisational awareness and training, ensuring that security practices align with business objectives and supports overall growth and resilience.

TIP 1. MAINTAIN A DATA ASSET INVENTORY

Keep an up-to-date inventory of all data assets to enhance visibility and management. This practice aids in tracking data locations, usage, and ownership, ensuring better protection and compliance with data management policies.

TIP 2. SECURE ACCESS TO YOUR DATA

Restrict physical access to servers and sensitive documents to authorised personnel only. Ensure administrators receive training in secure access management to protect against unauthorised entry and potential breaches.

TIP 3. RUN PHISHING SIMULATIONS

Conduct regular phishing simulations to test and improve employees' ability to recognise and handle phishing attempts. Use the results to provide targeted training and increase overall awareness of phishing threats.

TIP 4. REGULARLY UPDATE SOFTWARE

Regularly update all software and systems with the latest security patches. This practice helps protect against vulnerabilities and reduces the risk of exploits; ensuring your systems remain secure and up to date.

TIP 5. BACK UP YOUR DATA

Back up critical data regularly and store it securely, preferably offsite or in the cloud. This approach helps protect against data loss and ensures your information remains safe in the event of incidents or system failures

TIP 6. RESTRICT ACCESS TO SENSITIVE INFORMATION

Limit access to sensitive information to those who need it for their role. Implement role-based access controls to manage permissions effectively, ensuring that only authorised personnel can access critical data.

TIP 7. USE SECURITY AWARENESS TRAINING

Offer regular security awareness training to keep employees informed about the latest threats and best practices. Ensure they understand their role in data protection and know how to respond to potential security incidents.

TIP 8. CONDUCT SECURITY ASSESSMENTS

Perform periodic security assessments to evaluate and enhance data protection measures. Use security frameworks as a guide to identify and address potential risks, strengthening your overall security posture and protecting against vulnerabilities.

TIP 9. ESTABLISH CLEAR DATA HANDLING PROCEDURES

Create and enforce procedures for handling, storing, and disposing of data. Include guidelines for both physical and digital management to ensure proper data protection and minimise the risk of breaches.

TIP 10. HAVE A RESPONSE PLAN IN PLACE

Develop and document an incident response plan for data breaches or security incidents. Ensure all employees are aware of the procedures and their roles, which helps ensure a swift and organised response in emergencies.