Global Tech Partners

Example Cybersecurity Training Workshop Schedule

Time	Session title	Session description
Morning: Foundations and Tiers 1, 2		
9:00 - 9:30	Welcome: Why SMB1001 now?	Overview of the current threat landscape for SMBs, the limitations of traditional standards like ISO 27001 for smaller firms, and the value proposition of the flexible, tiered SMB1001 framework.
9:30 - 10:45	Domain 1 & 2: Basic controls (Levels 1 & 2)	Deep dive into the technology management such as firewalls, anti-virus, patching and Access Management controls required for the first two tiers. Focus on setting up basic, affordable preventative defences.
10:45 - 11:00	*Break*	
11:00 - 12:30	Domain 3: Backup and recovery essentials	Focus on implementing a backup and recovery strategy for important digital assets. Covers backup frequency (≤ 7 days) and the requirement for annual restorability testing.
12:30 - 1:30	*Lunch Break*	
Afternoon: Policy, Risk & Advanced Tiers 3/4/5		
1:30 - 2:45	Domain 4: Policies, Processes, and Plans (PPP) (Level 2-3)	Creating and implementing essential documents such as a Confidentiality Agreement, Invoice fraud policy, and a formal cyber security Incident Response (IR) plan. Introduction to the 'Digital asset register'.
2:45 - 3:00	*Break*	
3:00 - 4:00	Domain 5: Education and advanced controls (Level 3-5)	Training requirements, from annual cybersecurity awareness to IR plan testing/training. Covers advanced Level 5 controls like penetration testing, application control, and enabling a digital trust program with suppliers.
4:00 - 4:45	SMB1001 Tiering and certification roadmap	Practical guidance on determining the right starting tier based on a company's profile and client needs. Q&A session.