Risk Treatment Plan – Sweet Bean Café

This Risk Treatment Plan outlines the prioritized actions necessary to mitigate the top 10 cyber security and operational risks identified during the recent risk assessment of Sweet Bean Café. The plan focuses on the immediate implementation of high-impact controls to safeguard customer and financial data, maintain Point-of-Sale (POS) system integrity, and ensure ongoing business continuity. All mitigation tasks are assigned a responsible party and a target completion date, with the initiative commencing on 01 March 2025, to ensure swift accountability and remediation.

Priority	Risk Summary	Action	Responsible	Target Date	Status
High	Unsecured Wi-Fi allowing unauthorized access to the network.	Implement **WPA2-Enterprise** security protocols or establish separate VLANs for Guest, Staff, and POS traffic.	IT Consultant	31 Mar 2025	Not Started
High	Lack of anti-malware protection on POS systems.	Install and configure a monitored, centrally-managed **anti-malware solution** on all POS terminals and back-office computers.	Store Manager	15 Mar 2025	Not Started
High	Outdated operating	Audit all devices and	IT Consultant	30 Apr 2025	Not Started

	systems and POS software with known vulnerabilities.	promptly apply all pending **OS and application updates**. Establish a mandatory monthly patching schedule.			
High	Employee reuse of weak or shared passwords across critical systems.	Implement a mandatory **strong password policy** (min 12 chars, complexity) and provide access to a password manager tool for staff.	HR/Training	15 Apr 2025	Not Started
Medium	Loss or theft of a physical POS terminal device.	Secure all POS terminals with physical **security anchors** or locks. Implement a remote wipe capability for emergency use.	Store Manager	31 Mar 2025	Not Started

Medium	No formal process for backing up critical digital data (e.g., recipes, inventory).	Implement a **daily, automated, and encrypted cloud backup** solution for all critical business files and configurations.	IT Consultant	15 Apr 2025	Not Started
Medium	Physical security weakness for network equipment (router/switch/NVR).	Install all network hardware within a dedicated, locked, and **physically secured cabinet** or closet.	Store Manager	31 May 2025	Not Started
Medium	Phishing attempts targeting staff through company email.	Conduct mandatory, hands-on staff **training on recognizing phishing** and social engineering attacks before 30 April.	HR/Training	30 Apr 2025	Not Started
Medium	Lack of formal processes for	Create and document a mandatory user	HR	31 May 2025	Not Started

	employee onboarding and offboarding.	provisioning and **de-provisioning checklist** to ensure timely account creation/revocation.			
Low	Insufficient data retention policy for customer loyalty/marketing data.	Review and formally **document the data retention policy** to ensure alignment with local and regional privacy regulations.	Legal/Owner	30 Jun 2025	Not Started

Start Date of Plan Execution: 01 March 2025
Owner: Owner