Reviewed and Prioritised Audit Findings

Vulnerabilities Ranking Table		
Vulnerability	**Recommended Policy**	**Justification**
Several accounts were identified for employees that are no longer employed by ACME.	When an employee leaves the company: Review all access permission Retrieve data from the employee if appropriate Terminate access and reset all passwords	The former employee may gain unauthorised access to proprietary and confidential information and equipment. Anyone with the former employee's credentials can gain unauthorised access to the internal system.
Several user accounts allowed unauthorised and escalated privileges and accessed systems and information without formal authorization.	Assign the least privilege to perform the task Log when elevated privileges are used	The least privilege allows the user to perform all the necessary tasks without the risk of causing systemic changes unintentionally.
Several devices and systems allowed unsecure remote access.	Disable unsecured remote access, such as Telnet Require secure remote access, such as SSH and VPN	Unsecured remote access transmits the data in plaintext. The transmission of plaintext can expose sensitive information, such as user credentials, for malicious actors to conduct reconnaissance and attacks.
Forty percent of all organisation passwords audited were cracked within 6 hours.	New password policy: Implement 2FA or MFA User passphrases Change passwords only after evidence of compromise No reuse of old passwords No reuse of passwords on different applications Enable copy/paste passwords Educate users on basic cybersecurity	When the passwords are cracked, the attacker can gain unauthorised access and change the passwords to lock out the authorised users.
Several wireless hotspots used WEP for encryption and authentication.	Upgrade wireless hotspots to the most secure encryption and authentication available	WEP is prone to man-in-the-middle attacks and the key is easily cracked and hard to distribute to the users.

Company servers were not updated with the latest patches.	Establish a plan to update / test the latest patches at regular intervals.	Updating regularly can protect the data, fix security vulnerabilities, and improve the stability of the OS and applications.