Security Audit Report: TechNova Solutions

Scope and Goals of the Audit

Scope: The audit covers TechNova Solutions' digital infrastructure, focusing on internal communication tools, customer data protection, cloud services, and remote work protocols. The audit excludes physical office security systems and third-party vendors' platforms.

Goals: The goals of this audit are to evaluate TechNova Solutions' ability to maintain secure digital communications, identify vulnerabilities in customer data storage and access, and ensure security best practices are upheld in remote working environments.

Current Assets

- Cloud-hosted CRM system and customer databases

- Employee laptops and mobile phones

- Internal chat and collaboration tools (Slack, Zoom, Trello)

- Office 365 email and document management

- Remote access VPN servers

- Internal documentation and wikis stored on Notion

Risk Assessment

Risk Description: TechNova lacks uniform access controls and encryption policies across remote devices. Certain remote workstations lack current antivirus protection, and some employees access the CRM system from unsecured networks.

Control Best Practices

- Implement multifactor authentication (MFA) across all user logins

- Enforce device encryption and update management for all remote workstations

- Segment access to CRM data based on job function and employ least privilege principles

- Require VPN usage for any access to internal systems

Risk Score

The estimated risk score is 7 out of 10. While many systems are cloud-based and professionally managed, the decentralized nature of remote work and inconsistent endpoint security increases the likelihood of data exposure.

Additional Comments

- CRM contains sensitive customer information, which requires role-based access controls

- No formalized incident response plan is in place for remote environments

- Internal communication tools should enforce secure password requirements and encryption

- Regular security training is needed for employees to prevent phishing and data mishandling