THE BOOK ON **IT SECURITY**
The Essential Guide for Everyone

Small Business Security Audit Framework

Designed for business owners and managers. Use this framework to assess your company's security culture, employee access policies, and data protection strategies.

Part 1: Security Culture & Employee Awareness

- ☐ **Lead by Example:** Management clearly communicates the importance of security and actively participates in safeguarding company data.
- ☐ **No-Blame Reporting:** We have fostered a fear-free environment where employees are encouraged to report suspicious emails or their own mistakes without fear of being punished or fired.
- ☐ **Anti-Phishing Training:** Employees receive regular, ongoing training to recognize the signs of phishing, social engineering, and fake emails that mimic trusted vendors or colleagues.
- ☐ **Safe Email Forwarding:** We have established clear rules regarding the careless forwarding of internal emails, contracts, and sensitive financial records to unauthorized or external addresses.

Part 2: Access Policies & Identity Management

- ☐ **The Principle of Least Privilege:** Employees use standard user accounts for their daily work. Administrative privileges are strictly limited and reserved only for authorized IT management.
- ☐ **Mandatory Multi-Factor Authentication (MFA):** We require two-factor or multi-factor authentication for all remote access, corporate email accounts, and cloud services.
- ☐ **Strict Offboarding Procedures:** When an employee leaves the company or changes roles, their access rights, passwords, and system privileges are revoked and updated immediately.

- ☐ **No Shared Accounts:** Employees do not share login credentials. Every user has a unique account so that all system changes and access attempts can be accurately logged and traced.

Part 3: Infrastructure & Data Protection

- ☐ **Physical Server Security:** Our central domain server and critical networking equipment are kept in a physically secured, locked room with restricted access.
- ☐ **The 3-2-1 Backup Strategy:** We maintain at least three copies of our critical business data, stored on two different media, with one copy kept off-site or in a secure cloud.
- ☐ **Tested Disaster Recovery:** We don't just back up data; we routinely test our data restoration procedures to ensure we can quickly recover from a ransomware attack or hardware failure.
- ☐ **Website & CMS Maintenance:** Our company website, Content Management System (CMS), databases, and plugins are updated regularly to close vulnerabilities that attackers could exploit.
- ☐ **Network Segmentation:** Our internal business Wi-Fi is strongly encrypted and strictly separated from the 'Guest' network used by visitors or personal employee devices.

"Prevention is always safer and more cost-effective than fixing problems after they occur."

PAUL ROSENTHAL
AWARD-WINNING AUTHOR