SME Vulnerability & Patch Management Toolkit – User Guide

1. Introduction

This guide explains how to use the SME Vulnerability & Patch Management Toolkit.
It is written for non-technical business owners, office managers, IT coordinators, and anyone responsible for keeping systems secure.
No cybersecurity experience is required.

2. What the Toolkit Does

The toolkit helps you understand whether your computers are secure, whether your software is up-to-date, and how prepared your business is against cyber threats.
It includes checklists, policies, step-by-step procedures, automated tools, and reporting templates.

3. Who Should Use It

The toolkit is suitable for:
- Small and medium business owners
- Office managers
- IT administrators
- External IT support providers
- Compliance and audit teams

4. What's Included in the Toolkit

The toolkit contains:
- Easy assessments and checklists
- Policies and step-by-step procedures
- Templates for patch tracking and risk acceptance
- Automated tools for security checks
- Sample data to help you understand correct usage

5. Step-by-Step: How to Use the Toolkit

Step 1: Fill out the assessments
Use the vulnerability questionnaire and patch checklist to understand gaps.

Step 2: Put policies in place
Policies formalize your patching approach and are useful for audits.

Step 3: Use the procedures
Follow the simple step-by-step instructions to deploy and verify patches.

Step 4: Run automated checks (Windows)
Use the PowerShell scripts—especially un_vuln_patch_suite.ps1—to scan systems and generate reports.

Step 5: Maintain your registers
Track vulnerabilities, patches, and risks in the provided spreadsheets.

Step 6: Use the standards mapping
Helps you understand how your practice aligns with ISO 27001, CIS Controls, and NIST.

6. Requirements

For Windows tools:
- Windows 10/11 or Windows Server
- PowerShell
- Administrator rights

For Python tools:
- Python 3.10+
- Install required packages with: pip install -r requirements.txt

7. Common Scenarios

“I want to check if our systems are secure”
→ Run the orchestrator script: un_vuln_patch_suite.ps1

“I need to show auditors we have a patching process”
→ Use the policies, SOPs, and patch register template.

“A patch causes an issue”
→ Use the Exception & Risk Acceptance Form.

“I need to know what to patch first”
→ Check the prioritisation matrix and Top 10 Missing Patches report.

8. Best Practices

- Patch critical systems within 48 hours
- Keep a simple register of all vulnerabilities
- Test patches before rolling out to production
- Document exceptions clearly
- Review security posture monthly

9. Final Notes

The toolkit is flexible and can be adapted to any SME environment.
It provides the structure, documentation, and automation needed to meet basic cybersecurity and audit requirements without requiring specialist skills.