V. Risk Assessment

1. Multi-Factor Authentication (MFA)

- **Status:** Partially implemented
- **Recommendation:** Enable MFA across all admin, email, and payment accounts

2. Data Backup

- **Status:** Partially implemented
- **Recommendation:** Set up automated, encrypted weekly backups

3. Antivirus Software

- **Status:** Mostly Implemented
- **Recommendation:** Configure for automatic scans and updates

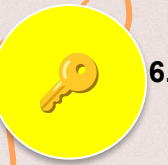
4. Software Updates

- **Status:** Mostly Implemented
- **Recommendation:** Enable auto-updates for OS, software, plugins

5. Phishing Awareness Training

- **Status:** Not Implemented
- **Recommendation:** Quarterly 15-min training sessions

V. Risk Assessment (cont'd)



6. Password Management

- **Status:** Basic passwords
- **Recommendation:** Use a password manager + strong policies

7. Incident Response Plan (IRP)

- **Status:** Not Implemented
- **Recommendation:** Create 1-page IRP with detection, containment, recovery steps

8. Data Encryption

- **Status:** Partially Implemented
- **Recommendation:** Encrypt customer records and backups

9. Vendor Risk Management

- **Status:** Partially Implemented
- **Recommendation:** Use vendor security checklist (MFA, HTTPS, breach history)

10. Social Media Security

- **Status:** Not Implemented
- **Recommendation:** Enable MFA, restrict access, monitor for impersonation

VI. Assets, Risks, and Controls (NIST Framework)

Assets

- E-commerce site (jendore.com)
- Customer & payment data
- Business email & admin accounts
- Social media platforms
- Employee laptops & mobile devices

Risks

- Phishing & email compromise
- Malware/ransomware
- Vendor platform / 3rd party vulnerabilities
- Credential theft
- Social media hijacking