# Organization Feedback

## Cybersecurity Feedback for SMEs

---

**Score: 50.00%** Your cyber hygiene self-assessment indicates progress but significant areas require improvement to enhance your organization's security posture.

---

**What You're Doing Well** - Your journey in improving cybersecurity has commenced. We are here to help you identify and bolster your strengths.

---

## Areas to Improve

**Access Control** - **Multi-Factor Authentication (MFA)**: Aim to fully implement MFA for all critical systems to add an extra layer of security beyond passwords. - **Password Policies**: Fully enforce a robust password policy that includes guidelines on length, complexity, expiration, and reuse restrictions. - **Password Managers**: Provide and mandate the use of password managers to safely store and manage passwords.

**Awareness** - **Employee Training**: Increase the frequency and extent of cybersecurity awareness training to keep employees informed and prepared. - **Phishing Simulations**: Conduct regular simulated phishing attacks to test and improve employee vigilance. - **Role-Specific Training**: Ensure employees receive training tailored to their specific roles and associated risks.

**Backup and Recovery** - **Data Backup Process**: Develop a comprehensive backup and recovery strategy and ensure it is fully implemented. - **Backup Frequency**: Establish regular and automated data backup schedules to prevent data loss.

**Other Critical Areas** - **Access Privilege Review**: Perform regular reviews of user access privileges to ensure least privilege principles are followed. - **Account Deactivation**: Immediately deactivate accounts of inactive or terminated employees to mitigate unauthorized access risks. - **Software Updates**: Establish a centralized system for managing software updates and ensure regular updates and patches are applied. - **Vulnerability Scans**: Schedule regular vulnerability scans to identify and remediate potential security issues. - **Antivirus Protection**: Ensure antivirus and endpoint protection solutions are properly installed and frequently updated. - **Data Encryption**: Implement encryption for sensitive files and communications both at rest and in transit. - **Incident Reporting**: Educate employees on how to report security incidents or suspicious activities effectively.

---

**Potential Risks** - **Credential Theft**: Due to insufficient access controls. - **Data Loss**: Resulting from unreliable backup processes. - **Phishing Attacks**: Targeting inadequately trained staff. - **System Compromise**: Due to unpatched vulnerabilities.

---

## Action Plan

**Immediate (0–30 Days)** - **Implement MFA**: For all critical systems to enhance access security. - **Initiate Training**: Begin regular cybersecurity awareness sessions for employees. - **Enforce Passwords**: Set up strong password policies across your organization.

**Short-Term (60–90 Days)** - **Automated Backups**: Establish automated backup systems and test data recovery processes. - **System Patching**: Regularly update and patch outdated systems and software.

**Medium-Term (3–6 Months)** - **Access Review**: Conduct regular reviews of user access privileges to maintain minimal access. - **Data Encryption**: Ensure sensitive data is encrypted during storage and transmission.

---

By addressing these areas, you will not only enhance your cybersecurity posture but also improve overall resilience against potential threats. Please reach out for any support or clarification needed as you work through these improvements. We're here to help ensure your organization's cybersecurity is strong and effective.