# Organization Feedback

## Cyber Hygiene Score

72.79%

**Improving:** A good foundation exists; targeted improvements will strengthen security.

## Introduction

Your organization currently maintains a moderate level of cybersecurity hygiene, as reflected by your score of 72.79%. While you have laid a strong foundation with several good practices, there are still areas requiring attention to further fortify your defenses. Continuous improvement in cybersecurity is vital, as it helps protect your business, your clients, and their data from ever-evolving threats.

## What You're Doing Well

Your organization has implemented several commendable cybersecurity practices. These strengths form the backbone of your existing security posture.

- **Strong Password Policies:** You enforce policies for password length, complexity, expiration, and reuse restrictions. These measures help prevent unauthorized access.

- **Timely Deactivation of Accounts:** Inactive or terminated employee accounts are promptly deactivated, reducing the risk of unauthorized access.

- **Least Privilege Principle:** Employees have access only to the systems and data required for their roles, minimizing potential damage from insider threats or compromised accounts.

- **Regular Vulnerability Scans:** Regular scanning helps identify and mitigate vulnerabilities before they can be exploited.

- **Antivirus and Endpoint Protection:** Up-to-date antivirus and endpoint protections form a critical defense against malware.

- **Data Classification Policy:** Implementing a data classification policy helps in managing and securing sensitive data effectively.

- **Data Encryption:** Sensitive communications and files are encrypted, safeguarding against data breaches during transit or at rest.

- **Backup Processes:** Systems for data backups and secure offsite storage ensures data recovery in case of incidents such as ransomware.

- **Cybersecurity Awareness Training:** Your employees receive training, equipping them to recognize and report threats, enhancing overall vigilance.
- **Secure Wi-Fi Policies:** By enforcing secure network practices, you limit unauthorized access to your systems.
- **Device Security:** Physical and endpoint security solutions across devices reduce the risk of loss or theft.
- **Incident Response Planning:** Having a documented plan ensures a quick and efficient response to any security incidents.

## Areas to Improve

Focusing on these key areas will further enhance your security posture.

### Identity & Access Management

- **Multi-Factor Authentication (MFA):** Implement MFA for all critical systems to add an extra layer of security.
- **Regular Review of Access Privileges:** Increase the frequency of access privilege reviews to eliminate unnecessary permissions.
- **Password Managers:** Encourage use of password managers to enhance password security and ease of use.

### Software & Patch Management

- **Centralized Update System:** Establish a centralized system for managing software updates to ensure timely patching of vulnerabilities.

### Backup & Recovery

- **Backup Testing:** Regularly test backups for restoration success to ensure data recovery processes are reliable.

### Security Awareness & Training

- **Simulated Phishing Attacks:** Conduct exercises to test and enhance employee phishing awareness and response.
- **Role-Specific Training:** Provide tailored training to address specific security challenges relevant to diverse job functions.

### Incident Response & Business Continuity

- **Incident Logging and Analysis:** Implement logging and analysis to identify patterns and preempt extensive security incidents.
- **Cyber Insurance:** Consider a policy to mitigate potential financial losses resulting from cyber events.

### Third-Party Risk

- **Vendor Assessments:** Evaluate the cybersecurity practices of vendors and partners prior to sharing access or data to ensure comprehensive security.

## Potential Risks and Risk Scenarios

- **No major risks identified at this time:** Continue your current efforts to maintain a robust defense against potential threats.

## Action Plan

### Immediate (0–30 Days)

- Implement MFA on key systems with immediate effect.
- Initiate a round of access privilege reviews.
- Set up a process to conduct regular backup restoration tests.
- Schedule a simulated phishing exercise for employees.
- Review and assess third-party vendor cybersecurity practices.
- Begin documentation of regular logging and analysis for incidents.

### Short-Term (60–90 Days)

- Deploy centralized patch management solutions.
- Conduct specific role-based cybersecurity training sessions.
- Re-evaluate current cyber insurance options.
- Establish a password manager policy and encourage its use among staff.
- Formalize detailed logging protocols for incident tracking.
- Review and update network security configurations.

### Medium-Term (3–6 Months)

- Evaluate the effectiveness of cyber insurance and make necessary adjustments.
- Implement any remaining aspects of a centralized update management system.

- Develop a vendor security scoring system.
- Institute regular penetration testing to assess all layers of security.
- Conduct a cybersecurity audit to evaluate improvements and gaps.
- Strengthen business continuity planning by engaging in scenario-based drills.

## Conclusion

Your organization is on the right path to robust cybersecurity management. Continue your efforts, and consider reassessing your security posture every 6–12 months. Remember, even small, incremental steps can significantly lower the risk of cybersecurity threats. By addressing the identified areas of improvement, you will further protect your business, ensure compliance, and maintain the trust of your clients.