Organization Feedback

Cyber Hygiene Score: 12.50%

Severity Level: Immediate and decisive cybersecurity action is required.

What You're Doing Well

- **Regular Updates:** Most of your operating systems, software, and applications are frequently updated, reducing vulnerabilities.
- **Data Backup Frequency:** Backups are mostly performed regularly, which is a solid foundation to prevent data loss.

Areas to Improve

Access Control

- **Multi-Factor Authentication (MFA):** Not currently implemented. Start using MFA for all critical systems to enhance security layers.
- **Password Policies:** No current enforcement of strong password policies. Implement rules for password length, complexity, expiration, and reuse restrictions.
- **Password Managers:** Not in use. Provide and mandate a password manager for secure management of credentials.

Awareness

- **Employee Training:** Cybersecurity awareness training is absent. Regular training sessions are essential to improve staff knowledge and vigilance.
- **Simulated Phishing Attacks:** Not conducted. Implement phishing simulations to test and strengthen employee responses.
- **Role-Specific Training:** Lack of tailored cybersecurity training. Provide specialized training according to employee roles.

Backup and Recovery

• **Backup Procedures:** Partially implemented. Standardize a comprehensive backup and recovery strategy.

• **Secure Storage:** Backups are not securely stored. Ensure backups are kept in offsite or cloud locations.

• **Backup Testing:** Not practiced. Regularly test backups to ensure data recovery reliability.

Other Areas

• **Access Reviews:** Conduct regular reviews of user access privileges.

• **Inactive Accounts:** Immediate deactivation of accounts for former employees is weak. Improve this process to prevent unauthorized access.

• **Least Privilege Principle:** Ensure employees only access necessary data and systems.

• **Centralized Updates:** Implement a system for managing software updates organization-wide.

• **Vulnerability Scans:** Not currently performed. Regularly scan systems for vulnerabilities.

• **Endpoint Protection:** Partially installed. Ensure comprehensive installation and updates of protection solutions.

• **Data Protection:** Encryption practices are absent. Protect sensitive data both at rest and in transit.

• **Incident Reporting and Response:** Establish a clear incident response plan and educate employees on reporting protocols.

• **Secure Wi-Fi Policies:** Currently not enforced. Ensure your Wi-Fi networks are secure, using WPA3 and separating guest networks.

• **Remote Access Security:** Not ensured. Secure remote access through VPNs or other secure methods.

• **Incident Logging and Analysis:** Not implemented. Start logging incidents for analysis and pattern detection.

• **Cyber Insurance:** Not in place. Consider a cyber insurance policy for financial protection against incidents.

• **Security Regulations Compliance:** Not adhered to. Follow relevant industry-specific cybersecurity standards.

• **Vendor Management:** Assess and require vendors to meet cybersecurity criteria.

• **Physical Security:** Improve physical security of devices to prevent unauthorized access.

Potential Risks

- **Unauthorized Access & Credential Theft:** Due to ineffective access controls.
- **Phishing Attack Vulnerability:** Low cybersecurity awareness increases risk.
- **Data Loss Risk:** Backup and recovery plan deficiencies could lead to permanent data loss.
- **General Cyber Threat Exposure:** Various security weaknesses heighten vulnerability to attacks.

Action Plan

Immediate (0–30 Days)

- Implement MFA for all critical accounts.
- Establish strong password policies with requirements for complexity, rotation, and length.
- Initiate comprehensive cybersecurity awareness training for employees.

Short-Term (60–90 Days)

- Automate backups and focus on testing data recovery processes.

Medium-Term (3–6 Months)

- Conduct an extensive cybersecurity assessment to identify and address any vulnerabilities.
- Enhance vendor assessment and management practices.
- Draft and start implementing a formal incident response plan.

By addressing these areas promptly, your organization will greatly enhance its cybersecurity posture and resilience against cyber threats.