KALUARI
Leading-edge Business Solutions

CYBERSECURITY AWARENESS CHECKLIST

CONTACT INFORMATION:

COMPANY _____ REVIEWER NAME _____

EMAIL _____ PHONE NUMBER _____

CRITERIA

1. Cybersecurity Awareness and Training

- ◯ Conduct regular cybersecurity awareness training for employees.
- ◯ Educate staff on common cyber threats like malware, phishing and ransomware
- ◯ Provide resources and guidelines for recognizing and avoiding cyber threats.

2. Strong Passwords and Authentication Management

- ◯ Ensure employees use strong, unique passwords for all company accounts.
- ◯ Implement two-factor authentication (2FA) where possible.
- ◯ Regularly update and rotate passwords.

3. Malware Protection

- ◯ Install and maintain up-to-date antivirus and anti-malware software.
- ◯ Set up automatic scans and updates for all devices.
- ◯ Monitor systems for signs of malware infection.

4. Phishing Detection and Prevention

- ◯ Train employees to recognize phishing attempts through email and social media.
- ◯ Teach staff to verify suspicious links or attachments before clicking.
- ◯ Utilize anti-phishing tools to filter and block potential phishing emails.

5. Ransomware Defense

- ◯ Regularly back up critical data to secure offsite locations.
- ◯ Create and rehearse an incident response plan in case of a ransomware attack.
- ◯ Keep all software and systems up to date to minimize vulnerabilities.

6.Social Engineering Awareness

- ◯ Educate employees on how to recognize social engineering tactics.
- ◯ Encourage staff to verify the identity of individuals before sharing sensitive info.
- ◯ Limit the amount of personal information shared publicly online.

7. Protection of Personal Information

- ◯ Encrypt sensitive company data, both at rest and in transit.
- ◯ Limit access to personal or sensitive information based on role requirements.
- ◯ Use privacy settings to protect data shared on social platforms and online.

8. Incident Reporting and Response

- ◯ Establish a clear process for reporting cybersecurity incidents.
- ◯ Encourage prompt reporting of suspicious activities or breaches.
- ◯ Regularly review and update the company's incident response plan.

9. Wi-Fi and Network Security

- ◯ Secure all company networks with robust encryption methods (e.g., WPA3).
- ◯ Prohibit the use of unsecured public Wi-Fi to access sensitive company info.
- ◯ Regularly audit network security to identify and patch vulnerabilities.

10. Additional Resources

- ◯ Stay informed on recent data breaches and cyber attacks to update defense strategies.
- ◯ Keep contact information for cybersecurity support readily available (e.g., sales@mailsafi.com).
- ◯ Provide employees with access to cybersecurity guides, checklists, and training materials.

OVERALL PERFORMANCE RATING

- ◯ Exceeds Expectations
- ◯ Meets Expectations
- ◯ Needs Improvement

COMMENTS AND FEEDBACK

EMPLOYEE ACKNOWLEDGMENT

_____

Reviewer Signature

_____

Date