ASA CYBERSECURITY CHECKLIST

AMERICAN SUPPLY ASSOCIATION | CYBERSECURITY TASK GROUP

MINIMAL MATURITY (ESSENTIAL CONTROLS)

- ☐ Multi-Factor Authentication (MFA) enabled for all critical systems
- ☐ Regular patching for servers, endpoints, and applications
- ☐ Antivirus/Endpoint Detection & Response (EDR)
- ☐ Daily backups with periodic test restores
- ☐ Basic phishing awareness training
- ☐ Strong password standards
- ☐ Web filtering enabled
- ☐ Inventory of devices and applications
- ☐ Documented incident response plan
- ☐ At least one tabletop exercise per year
- ☐ Data Loss Prevention (DLP)

AVERAGE MATURITY (STRUCTURED PROGRAM)

- ☐ Automated patching program
- ☐ Centralized logging for critical systems
- ☐ Monthly phishing simulations
- ☐ Basic network segmentation
- ☐ Vendor risk assessment process
- ☐ Privileged access management (PAM)
- ☐ Documented backup testing schedule
- ☐ Role-based recovery playbooks
- ☐ Basic SIEM or log-monitoring capability

ADVANCED MATURITY (HIGH RESILIENCE)

- ☐ Managed Detection & Response (MDR) or internal SOC
- ☐ Continuous vulnerability scanning and reporting
- ☐ Zero Trust architecture components implemented
- ☐ Dedicated cyber staff
- ☐ Full incident response playbooks with named roles
- ☐ Immutable/offline backups
- ☐ Threat hunting activities
- ☐ Regular third-party penetration tests

HOW TO USE THIS CHECKLIST

- This checklist is a self-assessment tool to help organizations understand their current cybersecurity maturity and identify areas for improvement.
- The maturity levels are progressive. Organizations are not expected to meet all items at once.
- Check items that are meaningfully in place today, not aspirational or partially implemented controls.
- This checklist is not an audit, certification, or compliance requirement. It is intended for internal planning and discussion.

GLOSSARY OF TERMS

Multi-Factor Authentication (MFA): A security method requiring multiple verification factors.

Patching: Applying updates to fix vulnerabilities and improve security.

EDR: Advanced endpoint protection with threat detection and isolation.

Backups: Restorable copies of critical company data.

Phishing Training: Teaching employees to recognize malicious emails.

Password Standards: Rules ensuring strong, hard-to-guess passwords.

Web Filtering: Blocking known malicious or suspicious sites.

Asset Inventory: List of all hardware/software needing protection.

Incident Response Plan: Documented steps to follow during a cyber incident.

Tabletop Exercise: Simulated cyberattack rehearsal with leadership.

Centralized Logging: Collecting logs into one system for analysis.

Network Segmentation: Dividing networks to limit breach spread.

Vendor Risk Assessment: Evaluating partner cybersecurity hygiene.

PAM: Restricting the use of privileged (admin) accounts.

Backup Testing: Verifying that backup data restores properly.

SIEM: System that aggregates and analyzes logs for threats.

MDR: Managed service that monitors and responds 24/7.

SOC: Team monitoring threats continuously.

Vulnerability Scanning: Automated detection of system weaknesses.

Zero Trust: Never trust; always verify users and devices.

Immutable Backups: Backups that cannot be changed or deleted.

Threat Hunting: Proactively searching for hidden threats.

Penetration Testing: Ethical hacking to find vulnerabilities.

Data Loss Prevention (DLP): Controls that prevent sensitive data from leaving the organization without authorization.