CYBERSECURITY READINESS CHECKLIST

Twelve Controls Questionnaire

WINSOR CONSULTING

This is a checklist of the 12 most overlooked or under implemented controls that we have seen at manufacturers in the state of Illinois. The data is compiled from 35+ Illinois manufacturers between the months of March and August 2021. The control indicator (ex. AC.1.003) will be based on the most recent revision of CMMC which includes practices from NIST 800-171, NIST 800-53, ISO 27001, etc.

☐ 1. AC.1.003 Verify and control/limit connections to and use of external information systems

Are you allowing personal devices to connect to your network? Can you be sure outside contractors/vendors aren't plugging into your network and accessing information? If marked as "Implemented", what policy procedure is in place for this?

_____

☐ 2. IA.1.076 Identify information system users, processes acting on behalf of users, or devices

Do all users have a unique username and password? Does the system authorize users access based on what their role is? Are any employees using shared accounts? If accounts are shared, ex. "Shipping", how do you audit user actions?

_____

☐ 3. PE.1.131 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals

Do you have locks on your server room? Are you logging who has access to it? Do employees know who are the authorized individuals?

_____

☐ 4. PE.1.132 Escort visitors and monitor visitor activity

Does your company have a sign in sheet? Do you escort and monitor all visitors that are not employees? Are they required to wear a name badge?

_____

☐ 5.AT.2.056 Awareness Training Program

Does your company have a formal awareness training program? Do you train managers, system admins, and end users of the security risks associated with their activities? Do you review applicable policies, standards, and procedures related to the system security?

_____

☐ 6. AU.2.044 Review audit logs

Do you have a policy/procedure for event types to look for within information system audit records? Are they reviewed and analyzed? Is a frequency for review established in policy? Can you prove that this is taking place?

_____

☐ 7. MP.2.119 Protect system media containing FCI/CUI, both paper and digital

Is this system media securely stored in protected areas? Ensure proper authorization for data in media and print. Do only approved individuals have access to media in FCI/CUI systems? Is there an audit log for when this data is removed or destroyed?

_____

☐ 8. MP.2.121 Control the use of removable media on system components

Are guidelines and restrictions placed on the use of portable storage devices, e.g., thumb drives? Do you scan all removable media for viruses? Do you track company owned removable media and dispose of it properly? This can be met by policy and technical controls.

_____

☐ 9. IR.2.092 Establish an operational incident handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response

Does your organization have an incident response plan that includes everything within this control? Is it periodically reviewed and updated as company changes take place?

_____

☐ 10. RE.2.137 Regularly perform and test data backups

Does your organization schedule backups to run automatically or manually on a regular basis? Do you perform tests to ensure they are operating correctly?

_____

☐ 11 IA.3.083 Use MFA for local and network access to privileged accounts and for network access to non-privileged accounts

Do all admin accounts have MFA implemented? Does outside network access require MFA (ex. VPN or remote connections)?

_____

☐ 12. RM.3.146 Develop and implement risk mitigation plans

Does your organization have a policy in place for mitigating each identified risk? Do you follow this approach to mitigate every identified risk?

_____

Additional notes: