STEP 2

J-CLICS Check List for Industrial Control Systems of Japan

Control Systems Security Check List

J-CLICS is a security checklist for industrial control systems. The purpose of this checklist is to help you identify and understand security issues by answering each of the questions.

STEP 1 is intended for everyone who works with industrial control systems. STEP 2 is intended primarily for technical personnel (administrators) who work with industrial control systems.

Thanks to help from industrial control system users, the questions on this checklist have been distilled into those that are necessary on the line. This checklist should be used as one method for evaluating the security level of industrial control systems and the security management posture. Please note that successfully passing all questions on this checklist **does not guarantee that certain standards, including international standards, are being followed, and it absolutely does not mean that the implemented industrial control system security measures are perfect**.

The rationale for each question is explained in the J-CLICS Guidance. Please refer to the guide when reviewing security measures and use it as a security training resource.

Answer each of the following questions with a ✓ for yes or X for no.

No.		Question	✓ / X	Corresponding Guidance Page No.
		Understanding of the System and Business Risks		
1	1	Do you understand the configuration of the industrial control system (*1) and manage its latest state, including the change history?		P. 5
		Understanding of Threats		
2	1	Do you understand the possible threats (*2) to each component of the industrial control system?		P. 8
		Network Architecture		
3	1	Do you understand the communication specifications (*3) and connection specifications for all equipment connected to the industrial control system?		P. 11
		Firewall		
4	1	Is a firewall set up at the boundary between the industrial control system and other networks (*4) to block unnecessary communication?		P. 13
		System Monitoring		
5	1	Do you regularly check and analyze the industrial control system's operating status (*5) and logs even during normal times?		P. 16
		Measures for Viruses		
6	1	Are antivirus measures in place for the industrial control system?		P. 19
		Security Patches		
7	1	Do you have an established procedure to apply patches to the industrial control system and applications running on it based on vendor-provided information, and does this procedure take into consideration the adverse effects on your business that may result from applying such patches?		P. 22
		System Enhancement		
8	1	Do you suspend or disable unused OS services and communication ports upon initially installing or upgrading the OS and applications used on the industrial control system?		P. 25
		Backup and Recovery		
9	1	Do you back up the data necessary to restore the industrial control system (*6) as recommended by the vendor?		P. 28
		Processes for Transferred Personnel		
10	1	Do you document and implement procedures for account addition/deletion and password changes in the event of personnel transfers, including making changes to the roles or responsibilities of personnel registered in the system?		P. 31

***1 Includes information assets, software assets, and physical assets**
***2 Threats from natural disasters, fire, theft, etc.**
***3 Senders, receivers, protocols used, etc.**
***4 Office networks, the Internet, remote access, etc.**
***5 CPU load, disk space management, system logs, etc.**
***6 Parameters, operational data, etc.**