STEP 1

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 this 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 Guidebook Page No.
		Physical Security		
1	1	Is access to the control room (*1) restricted to authorized personnel?		P. 6
	2	Are visitors to the control room (*1) always accompanied by an authorized person?		P. 8
	3	Is access to the control room (*1) managed (regular checking by record and by administrator)?		P. 10
		Equipment Connection Procedures		
2	1	Are procedures followed to check that equipment (*2) has not been infected with a virus before connecting it to the industrial control system network?		P. 16
	2	If industrial control system equipment is installed in the same rack as information system equipment, is each piece of equipment labeled (with a tag, sticker, etc.) to identify the system to which that equipment belongs?		P. 19
		Passwords and Accounts		
3	1	Is there an industrial control system password policy in place that stipulates a required password strength and expiry period?		P. 23
	2	Are strong passwords (*3) used?		P. 25
	3	Is the password to the industrial control system changed regularly?		P. 27
		Ensuring of Responsiveness		
4	1	Do you understand the procedure for monitoring the security of an industrial control system and what to do in the event of an alert or an abnormality? Are you conducting drills to prepare for such incidents?		P. 32
		Third-party Risk Management		
5	1	Are the rules for ensuring remote connection security followed?		P. 36
		Continuous Evaluation and Improvement (*Kaizen*)		
6	1	Do you regularly use J-CLICS (or any other checklist prepared within the company or other industry associations, etc.) to self-assess the industrial control system's security?		P. 40

***1 "Control room" refers to the place where the control equipment or operation terminals are located.**

***2 USB memory devices, PCs used for maintenance, external hard disk drives, external CD/DVD drives, etc.**

***3 A password that is not easy to guess, that is at least 8 characters long, that contains at least two types of characters (alphabets, numbers, and symbols), and that does not include the relevant account name or similar information.
(If the maximum password length that can be used on the target device is less than 8 characters, use the maximum number of characters.)**