For SMEs

5-Minute Information Security Self-Assessment

Are you ready for cybersecurity threats?

Evolving threats and attacks

- Ransomware
- Password list attacks
- Targeted e-mail attacks

Changes in the IT environment

- The Cloud
- Tablets
- Smartphones

Use the **"5-Minute Self-Assessment Questionnaire"** to check the state of your company's security posture to avoid fatal losses!

ASEAN · JAPAN
Cybersecurity Cooperation

Self-Assessment

1 Please read this before using the Self-Assessment Questionnaire

How to use

We have focused on 25 information security measures that are effective and can be implemented at little cost for the organization.
Please check the implementation status of these items and implement any measures are yet to be implemented while referring to Explanation & Recommended Action in this pamphlet.

What you gain

- It allows you to identify any problems that may exist.
- By identifying the problems, you can find a specific course of action to take as the next step.

How to answer the questionnaire

Please make a judgment without relying on the specific examples in the questionnaire. For example, the question No.16 is about “theft prevention measures.” It is asking if you have taken steps to prevent theft by keeping laptops in drawers if your organization uses laptops. It also asks if you take steps to prevent theft by not leaving accessories such as USB sticks or external hard drives on desks if your organization does not have laptops. Refer to Explanation & Recommended Action if you do not understand the purpose of a question or find it difficult to understand.

If your company does not use devices or services

Some of the devices/services below may not be used in your company depending on the type of business. In those cases, choose “Implemented.”

- No.4 Network connected photocopy machines and hard drives
- No.5 Web services
- No.9 Wireless LANs
- No.23 Cloud services

Even if you think, “We don’t have any ‘confidential information’, the documents below are confidential!

- Employee addresses, and pay slips
- List of payments for each business partner and transaction information
- Your organization’s accounting information
- Customer and business partners' contact lists
- R&D information such as design drawings for new products
- Classified information from business partners

There is information that must be classified as confidential among the basic information of an organization. You must confirm and organize what type of information exists in your company, which is deemed as confidential. This data classification is the first step in information security.

2 Read this after taking the Self-Assessment Questionnaire

If you scored a perfect 100 points	Your basic security measures are already perfect. Moving on to the next level, you should consider improving those measures.
If you scored 70-99 points	Your basic security measures are almost perfect but there are some areas that have incomplete measures.
If you scored 50-69 points	There are conspicuous areas that have inadequate measures.
If you scored 49 or fewer points	You should not be surprised if an incident, such as data breach, happens to the organization at any time.

The actions described in Explanation & Recommended Action are premised on the following.

- The executive (representative) can directly instruct and confirm whether measures are implemented.
- All employees recognize each other.
- The company does not own a server or network equipment that requires complicated configurations in the company.
  - The company does not own any web servers directly connected to the Internet, but using cloud services.
  - There is no application software developed by the company, and it uses only commercially-available application software.
  - Personal computers are allowed to be used for work only when the same level of security measures as company-owned computers are implemented.

Self-Assessment

5-Minute Self-Assessment Questionnaire

A company self-assessment sheet to identify the information security measures that you should prioritize as an organization

- Please read [1] on the previous page before doing assessment.
- Read the questionnaire below and choose your answer.
- This questionnaire should be filled out by either executives or managers.
- Please answer whether items indicated with are implemented by all employees. If an item is implemented only by some employees, choose "Partially implemented."
  Please answer whether items indicated by are implemented by your company.
- Add your score at the bottom of the page and proceed to read [2] on the previous page.

Organization:

Respondent:

Date:

Category	Item No	Question	Answer			
			Implemented	Partially implemented	Not implemented	Don't know
Part 1 Essential measures	1	Do you always keep your OS and software secured, such as applying Windows Update*1?	4	2	0	0
	2	Do you take measures to protect your PC from viruses, such as installing antivirus software and automatically updating the virus definition files?*2	4	2	0	0
	3	Have you set a strong password that is not easy-to-guess such as your name, phone number, or birthday, and do you refrain from using the same password for multiple web services?	4	2	0	0
	4	Do you appropriately restrict access to important information, such as restricting the sharing of network-connected photocopy machines or hard drives to only those who need it?	4	2	0	0
	5	Do you have a system in place to identify new threats and attack methods and share it internally, such as checking and sharing security alerts from product manufacturers or the web services*3 that you use?	4	2	0	0
Part 2 Employee actions	6	Are you careful with phishing e-mails, such as making an effort to not open attachments in suspicious e-mails or to not click links in messages?	4	2	0	0
	7	Do you have a system in place to check and prevent sending e-mails erroneously, such as by double-checking the addresses before sending e-mails?	4	2	0	0
	8	Do you protect important information before sending it out using e-mails, such as by protecting attachments with a password?	4	2	0	0
	9	Do you take steps to use your wireless LANs securely, such as always implementing strong encryption when using them?	4	2	0	0
	10	Do you follow the company rules when you use the Internet at work, such as safe web browsing or responsible social media use?	4	2	0	0
	11	Do you take steps to prevent important information from being lost due to malfunctions or operation errors, such as performing regular backups?	4	2	0	0
	12	Do you take steps to prevent the loss or leaking of important information, such as storing important information in a locked cabinet instead of leaving it on a desk?	4	2	0	0
	13	When taking important information out of the office, do you take steps against theft or loss, such as protecting it with a password or encrypting it and keeping it with you at all times?	4	2	0	0
	14	Do you take steps to ensure others do not use your computer, such as setting the computer's lock screen when you leave your desk?	4	2	0	0
	15	Do you try to prevent unauthorized people from entering the office, such as approaching strangers when you notice someone unfamiliar at the office?	4	2	0	0
	16	Do you take steps to prevent theft when leaving the office for the day, such as locking laptops and accessories in drawers instead of leaving them on the desk?	4	2	0	0
	17	Are the keys to the office managed in proper ways, such as the last person leaving for the day locks the office and makes a record (of his/her name, date and time)?	4	2	0	0
	18	When disposing of important information, do you take steps to render important information unreadable, such as shredding documents or using a data erasing tool?	4	2	0	0
Part 3 Organization management	19	Do you make employees manage confidential information appropriately, such as informing employees when they are hired that they are obligated to maintain confidentiality and that there are provisions for punishment?	4	2	0	0
	20	Do you make employees aware of the importance of information management, such as by regularly explaining its importance?	4	2	0	0
	21	Do you clarify whether employees may use personal devices in their work, such as setting policies on the usage of personal computers and smartphones in the company?	4	2	0	0
	22	Do you require business partners to maintain confidentiality, such as including confidentiality (obligation to maintain confidentiality) clauses in contracts?	4	2	0	0
	23	Do you confirm service safety and reliability before selecting an external service like a cloud service, such as by checking the terms of use and security measures?	4	2	0	0
	24	Have preparations been made in the event of an information security incident, such as drawing up response procedures for the leaking, loss, or theft of confidential information?	4	2	0	0
	25	Do you define the content of information security measures, such as making information security measures (such as item 1 to 24 above) as company policies?	4	2	0	0

*1 A program provided by Microsoft Corporation that fixes defects on Windows software

*2 A database file called a "pattern file" for detecting computer viruses

*3 The generic name of services used via the Internet such as Internet banking, social media, webmail, and calendars

★ There is no guarantee that the measures described in the Self-Assessment Questionnaire offer complete protection.

A Sub total	B Sub total	A+B Total score
Pts	Pts	Pts

Explanation & Recommended Action

Part 1 Essential measures

Items No. 1 to 5 are measures that should be taken regardless of the size and form of the company. It is crucial that these measures are continuously reviewed and not just simply done once. It is necessary to implement them as company rules so that they can be followed by all employees.

Item No. 1 Vulnerability patches

Always keep your OS and software up to date

Neglecting security issues with your OS and software leaves your device vulnerable to virus infections. Be sure to apply patches to your OS and software or use the latest version.

Action Take steps, such as using Windows Update or using the latest version of Adobe Flash Player, Adobe Reader, Java runtime environment, and other software.

Item No. 2 Antivirus software

Install antivirus software and use it appropriately

There is an increasing number of viruses that steal IDs and passwords, operate computers remotely, and encrypt files arbitrarily. Be sure to install antivirus software and ensure that the virus definition file (pattern file) is always up to date.

Action Take steps, such as setting your devices to automatically update the virus definition file or considering installing consolidated security software.

Item No. 3 Password management

Use strong passwords

There is an increasing amount of damage from unauthorized logins due to passwords being guessed, the malicious use of IDs or passwords leaked from a web service. Make your passwords strong, long and complicated, and do not reuse them.

*Weak password: A password that is easy to guess by a third party, such as your name, company name, or simple English words in the dictionary.

Action Take steps, such as making passwords that are a combination of 10 or more characters, numbers, and symbols. Do not use names, phone numbers, birthdays, etc., and do not use the same password for multiple web services and other websites.

Item No. 4 Device settings

Review access control settings

There is an increasing concern of unauthorized people viewing information due to data stored on file servers or online storage services, or incorrectly configured network photocopy machines. Be sure that servers and networked devices are shared with only the people who are allowed to access them.

Action Take steps, such as limiting the scope of sharing cloud services, limiting the scope of sharing network connected devices, and changing settings when employees move to other departments or retire.

Item No. 5 Learning about threats

Learn about threats and attack methods and take steps to counter them.

There is an increasing number of phishing attacks to steal IDs and passwords through e-mail with viruses impersonating business partners or other stakeholders, or leading people to fraudulent websites that mimic legitimate websites. Take steps to counter threats and attack methods by learning about them.

Action Take steps, such as checking security vendors' websites and subscribing to e-mail magazines to learn about the latest threats and attack methods, and confirming alerts provided by Internet banking and other services in use.

Part 2 Employee actions

Items No. 6 to 18 are measures that all employees should be aware of. Human error can easily occur due to the familiarity of handling important information every day. Also, as the nature of threats changes day-to-day, you need to be vigilant at all times.

Item No. 6 E-mail

Be suspicious of any e-mails received from someone you do not know

This may lead to virus infections by opening e-mail attachments or by clicking URL links in the body of an e-mail. Be wary of attachments and clicking URL links from senders you do not know.

Action Take steps, such as not opening attachments or clicking URL links in suspicious e-mails and report any suspicious e-mails to your security department to share information about suspicious e-mails in the company.

Item No. 7 E-mail

Prevent sending an e-mail to the wrong recipient

There will be incidents of leaking information to a stranger by mistakenly sending e-mails or faxes to the wrong person. Be sure to check carefully who you are sending e-mails and faxes to. Also, information leaks occur when you mistakenly give someone a wrong e-mail address. When sending an e-mail to multiple people, make sure to double-check the recipients' addresses.

Action Take steps, such as double checking the addresses before sending e-mails or faxes, and appropriately select To, CC and BCC in the e-mails.

Item No. 8 E-mail

Protect important information when sending it in e-mails

When sending important information by an e-mail, do not write it in the body of the e-mail. Instead, write it to a file, protect it with a password, and attach the file to the e-mail. Notify the e-mail recipient of the password by phoning them or through other means, instead of writing it in the e-mail.

Action Take steps, such as writing important information in a file and protect it with a password. Notify the recipient of the password over the phone or through other means.

Item No. 9 Wireless LAN

Prevent eavesdropping and unauthorized use of wireless LANs

Wireless LANs that do not have proper security settings may be subject to their data being breached or used maliciously for criminal acts by illicitly connecting to them. Be sure to set the security configuration of wireless LANs properly to prevent eavesdropping and unauthorized use.

Action Take steps, such as using encryption settings (e.g.WPA2-PSK) and using a pass phrase that is long and difficult to guess.

Item No. 10 Internet usage

Prevent trouble when using the Internet

Viewing malicious websites or websites with security problems can result in your device being infected with a virus. In addition, companies' brand image can be harmed by practical jokes posted on social media or message boards by employees or by accidentally posting confidential information. It is necessary to prevent harm by putting in place a system and rules that restrict the use of the Internet at work.

Action Take steps, such as creating rules for using the websites and social media, and use web filters to systematically restrict the use of the Internet.

Item No. 11 Backup

Encourage regular backups

Data saved on a PC or server can be lost due to a malfunction, erroneous operation, or virus infection. Make backups of data to prepare for such unexpected situations.

Action Take steps, such as performing backups of important data on a regular basis and storing the backups in a separate location.

Explanation & Recommended Action

Item No. 12 | Storage

Important information/documents must be handled properly

It is dangerous to leave information/documents unattended on a desk as they can be taken or read by someone. Important information/documents must be handled properly to prevent others from seeing or touching them and ensure that they are not left unattended. Specify restricted storage location for information/documents, take them out only when necessary for work, and ensure to store them back when finished.

Action — **Take steps, such as keeping desks neat and tidy, and storing important information/documents in a locked cabinet.**

Item No. 13 | Information transporting

Transport important information in a safe manner

When taking important information outside the company, it can be unexpectedly stolen or inadvertently lost. Take steps in advance when using a laptop or smartphone, such as setting a password or encrypting the data files, so that the information cannot be easily viewed in case it is stolen or lost.

Action — **Take steps, such as making it mandatory to obtain permission to transport important information, securing data with passwords on laptops, smartphones, and USB sticks, and never leaving the baggage unattended.**

Item No. 14 | Office safety

Do not let anyone use devices without permission

Do not leave computers unattended during work. An un-attended PC that can be operated by anyone, such as one that can be logged on without a password, could be misused by others. Take steps to protect PCs from unauthorized use.

Action — **Take steps, such as locking your PC when you leave your desk, shutting down PC when you leave the office for the day, and prevent other people from using your PC.**

Item No. 15 | Office safety

Approach people you do not recognize

There is a danger for information to be stolen if you do not restrict access to unauthorized people entering the office. Be sure that unauthorized persons are not allowed access to the places where important information/documents are stored, especially like servers, archives and safes.

Action — **Take steps, such as approaching someone you do not recognize in the office or setting up a reception desk.**

Item No. 16 | Office safety

Take steps to prevent the theft of equipment and accessories

While devices such as laptop computers, tablets, and USB sticks are convenient and portable, this also puts them at greater risk of being stolen. When these devices are not being used, take steps to store them in the safe places, such as in a lockable drawer.

Action — **Take steps, such as locking laptops, tablets, and accessories (CDs, USB sticks, external hard drives, etc.) in desk drawers when leaving the office for the day**

Item No. 17 | Office safety

Be vigilant of locking office doors

Keeping a record of the time the last person exited the office also helps to improve the sense of responsibility for the last person to lock the door. Make an effort to manage keys and records.

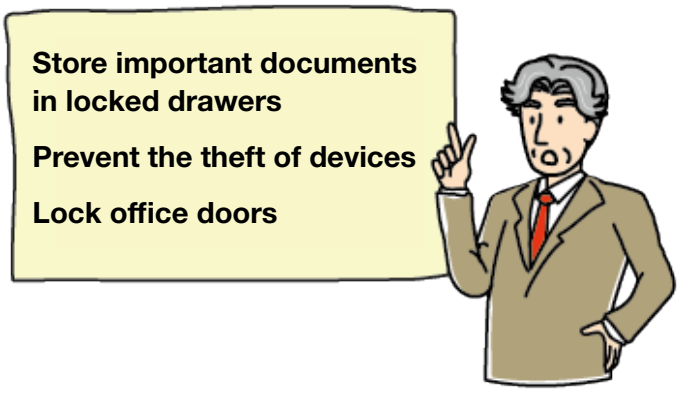
Action — **Take steps, such as managing keys and keeping a record of the last person in the office locking the door (date, time, and name).**

Item No. 18 | Safe disposal of information

Erase important information so that it cannot be recovered

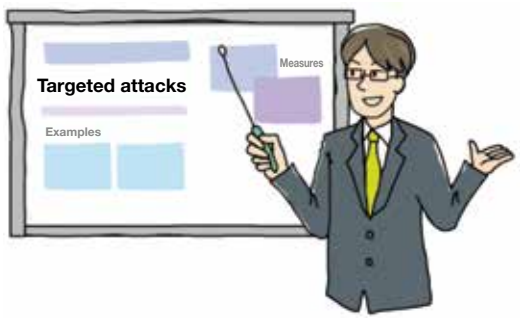
Simply throwing documents containing important information into the trash leads to serious information leaks as other people will be able to read the documents. In addition, information saved on electronic devices and electronic media can be restored even if the files are deleted. When disposing of important information, dispose each medium appropriately, such as by using a shredder or data erasing software.

Action — **Take steps to dispose information, such as by using data erasing software, physically destroying it, or requesting a specialist to erase it.**



Part 3 Organization management

Items No. 19 to 25 are measures to be taken after establishing a policy for the organization. Raise employee awareness by clearly documenting information security rules and sharing them in the office.



Item No. 19 Employee education

Have employees understand their obligation to maintain confidentiality

Although it can be said that company rules already require employees to maintain confidentiality in their work, it is good to inform employees of the company rules clearly to follow.

Action Take steps, such as informing employees of their obligation to maintain confidentiality when they are hired.

Item No. 20 Employee education

Conduct regular employee training

Employees handle information on a daily basis in their work, and this familiarity means there tends to be oversights and often forget about managing information securely. Regular employee education is effective in increasing employee awareness.

Action Take steps, such as regularly explaining the importance of managing information and conducting in-house training.

Item No. 21 Use of personal devices

Decide whether to allow the use of personal devices for work

Ensuring security becomes difficult if personal devices such as PCs and smartphones are used for work, as it is difficult to manage how employees are using them. Decide whether personal devices can be used for work and make efforts to set rules on their use.

Action Take steps, such as establishing a permission system for using personal devices such as PCs and smartphones for work and determine rules for their use if they are allowed for work.

Item No. 22 Compliance with written policy

Request that business partners maintain confidentiality

Avoid assuming that business partners will naturally maintain confidentiality based on the nature of the information. When providing confidential information to business partners, it is necessary to clarify that it is to be treated as confidential.

Action Take steps, such as drafting contracts that clarify the content to be treated as confidential.

Item No. 23 Use of external services

Use trusted external services

If you select external services, such as cloud services, with a priority on cost, you might find that services may not be available due to failures and other problems. Thoroughly examine the performance, reliability, compensation details, and other relevant considerations when using external services for applications that have a significant impact on business continuity.

Action Take steps, such as checking the terms of service, compensation details, security measures, and other relevant things when selecting a vendor.

Explanation & Recommended Action

Item No. 24	Incident handling

Prepare in advance for an information security incident

When an incident happens, there is usually no time to think calmly, and any delays in responding to the incident tend to increase the impact of the incident. Use incident information reported in the media as a reference to think about who will do what and when, assuming that the same thing happens in your company.

Action	Take steps, such as preparing incident response manuals for the leakage, lost, or theft of important information.

Item No. 25	Documented rules

Create rules for information security measures

Even if executives have put in place policies for information security measures, unless they are clearly documented as in-house rules, employees will have to seek advice from their managers all the time. In order to allow employees to act according to the rules on their own, it is necessary to clearly document “company rules” so that employees can refer to them at any time.

Action	Take steps, such as making items No. 1-24 of the Self-Assessment Questionnaire as rules for information security measures and share them in the company and review these rules regularly to improve them when any deficiency is found.

NISC National center of Incident readiness and Strategy for Cybersecurity

IPA Information-technology Promotion Agency, Japan

2019.04