For SMEs

5-Minute Information Security Self-Assessment

Is your business prepared for today's cyber threats?

Evolving threats and attacks

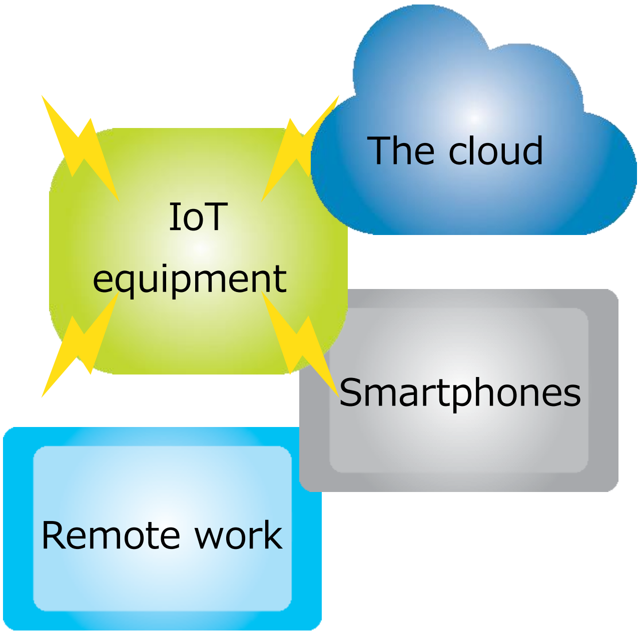
Changes in the IT environment

Targeted attacks

Ransomware

Credential stuffing

Business e-mail scams



IoT equipment

The cloud

Smartphones

Remote work

Don't wait until it's too late.

Check your company's security with this.

5-Minute Self-Assessment!

IPA
Information-technology
Promotion
Agency, Japan

Self-Assessment

1 Please read this before taking the Self-Assessment

How to take the Self-Assessment

The Self-Assessment covers 25 information security measures that are both effective and low-cost to implement for your organization. Review your current practices to see if these measures are properly implemented and begin taking steps to implement measures for any areas that aren't addressed yet while referring to the Explanations & Recommended Actions section.

Benefits of taking the Self-Assessment

- Easily identify any problems that may exist
- Determine countermeasures for the identified problems

Points to note when answering

Don't focus too much on the specific examples in the Self-Assessment. For example, Question No. 16 is about "theft prevention measures." If your organization owns laptop computers, the question is asking whether you take anti-theft measures such as putting laptops away in drawers when not in use.
It also refers to whether you take steps to prevent theft by not leaving other equipment such as USB sticks or external hard drives on desks if your organization does not have laptops. If you do not understand the purpose of a question or find it unclear, refer to the Explanations & Recommended Actions section.

If your company does not use certain 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 multi-function printers 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
- Confidential information from business partners

You must identify and understand what type of information exists in your company, and which is deemed as confidential. This data classification is the first step in information security.

2 Please read this after taking the Self-Assessment

Score: 100 points	You have successfully implemented basic security measures. Consider further steps to strengthen your defenses.
Score: 70-99 points	Well overall, however, there are still areas where security measures may be lacking.
Score: 50-69 points	There are noticeable areas where security measures are not sufficiently implemented.
Score: 49 or fewer points	Incidents such as data breaches could happen any time.

Self-Assessment

5-Minute Self-Assessment Questionnaire

This Self-Assessment sheet helps you identify the information security measures that you should prioritize at your organization.

- Please read Section 1 on the previous page before conducting the Self-Assessment.
- Read the Self-Assessment below and choose your answer.
- This Self-Assessment should be filled out by either an executive or manager.
- Total your score at the bottom of the page and proceed to read Section 2 on the previous page.

Organization: ______________________

Respondent: ______________________

Category	No.	Question	Answer			
			Implemented	Partially implemented	Not implemented	Don't know
Part 1 Basic measures	1	Are the operating systems and software of your computers, smartphones, and other devices always up to date?	4	2	0	-1
	2	Is antivirus software installed on your PCs, smartphones, and other devices, and are the virus definition files*1 up to date?	4	2	0	-1
	3	Are your passwords long and complex to prevent them from being easily deciphered?	4	2	0	-1
	4	Are there appropriate access restrictions in place for sensitive information*2?	4	2	0	-1
	5	Is there a process in place to share information about new threats and attack patterns within your company?	4	2	0	-1
Part 2 Employee measures	6	Do your employees take careful actions against viruses via attachments or URL links in e-mails?	4	2	0	-1
	7	Are measures implemented to prevent mistakes in the destination addresses of e-mails and faxes?	4	2	0	-1
	8	Is sensitive information protected by attaching it to files rather than writing it in the message body of e-mails, and securing those files with passwords or other means?	4	2	0	-1
	9	Are you implementing measures such as setting appropriate encryption methods for your wireless LAN to ensure safety?	4	2	0	-1
	10	Are measures implemented against issues such as virus infections via the internet or inappropriate posts on social media?	4	2	0	-1
	11	Is sensitive information backed up to prevent loss due to computer or server viruses, malfunctions, or operational errors?	4	2	0	-1
	12	Are documents and electronic media containing sensitive information stored safely in a secure location such as a filing cabinet, rather than left on desks, to prevent loss or theft?	4	2	0	-1
	13	When taking documents or electronic media containing sensitive information outside the workplace, are measures taken to prevent theft or loss?	4	2	0	-1
	14	Are precautions taken to prevent unauthorized viewing or unauthorized use of computer screens when stepping away from your desk?	4	2	0	-1
	15	Is access to the workplace restricted to authorized personnel only?	4	2	0	-1
	16	Are measures implemented to prevent theft, such as locking up laptops and other equipment when leaving the office?	4	2	0	-1
	17	Are measures implemented to ensure that no one forgets to lock the office when unoccupied?	4	2	0	-1
	18	When disposing of documents containing sensitive information or media containing sensitive information, are measures implemented to ensure that they cannot be recovered?	4	2	0	-1
Part 3 Organizational measures	19	Does your organization ensure that employees understand their confidentiality obligations and comply with rules such as not divulging information obtained in the course of their work to outside parties?	4	2	0	-1
	20	Are security trainings or awareness programs provided to employees?	4	2	0	-1
	21	Are security measures defined for the use of personal information devices for business purposes?	4	2	0	-1
	22	Are confidentiality clauses included in contracts with business partners that involve the exchange of sensitive information?	4	2	0	-1
	23	Are external services used for cloud services, website operation, and other purposes selected based on their security and reliability?	4	2	0	-1
	24	Is your organization prepared for security incidents by establishing procedures for emergency response, creating response plans, and taking other measures?	4	2	0	-1
	25	Has your organization established rules for information security measures (such as those listed in 1 to 24 above) and made them clear to employees?	4	2	0	-1

A "implemented" total	B "Partially implemented" total	C "Don't know" total
Pts	Pts	(－) Pts
A+B+C Total score		Pts

*1: These are also called "pattern files," which are database files used to detect computer viruses.

*2: Sensitive information refers to information that is necessary for business operations and valuable to the organization, such as trade secrets, as well as information that entails management responsibility, such as personal information of customers and employees.

★After the Self-Assessment, please read the following pages to consider countermeasures.

Explanations & Recommended Actions

Part 1 Basic measures

Items No. 1 to 5 are basic measures that should be taken regardless of the size and structure of the company. It is crucial that these measures are established as company rules as they are not one-time measures and require ongoing implementation.

Prioritize security updates!

No. 1 Vulnerability Management

Always keep your OS and software up to date

Leaving your OS and software outdated can leave security vulnerabilities unresolved, increasing the risk of viruses that exploit these weaknesses. Make sure to apply security updates or use the latest versions of your OS and software.

Action

- Run vendor-provided services such as Windows Update (for Windows OS) or Software Update (for macOS).
- Update the software you are using, such as Adobe Reader and your web browser, to the latest versions.
- Ensure that the software on your computer and the firmware of your router is up to date for remote work.

No. 2 Antivirus Software

Install antivirus software and use it appropriately

There has been an increase in viruses that steal IDs and passwords, perform remote operations, and encrypt files without permission. It is important to install antivirus software and ensure that virus definition files (pattern files) are always kept up to date.

Action

- Set up automatic updates for virus definition files.
- Consider implementing integrated security software.
- Make effective use of the security features that come with your OS.
- Install antivirus software on devices used for remote work and ensure that virus definition files are kept up to date.

No. 3 Password Management

Use strong passwords

There is an increasing number of cases from unauthorized logins due to passwords being guessed, cracked, or leaked from web services. Make your passwords strong, long and complex and do not reuse them.

Action

- Use passwords that are at least 10 characters long, making them as long as possible, and ensure they are complex by including uppercase letters, lowercase letters, numbers, and symbols.
- Do not reuse the same ID and password across multiple services.
- When using VPNs or cloud services during remote work, set a strong password and use multi-step or multi-factor authentication where possible.

No. 4 Device Settings

Review data/file sharing settings

Misconfigured web services for data storage or network-connected multifunction printers are leading to an increasing number of data exposure incidents. Ensure that servers and networked devices are shared with only the people who are allowed to access them.

Action

- Limit the sharing scope of web services, network-connected multifunction printers, cameras, and hard disks (NAS).
- Promptly change (or delete) settings when employees are transferred or terminated.
- Do not share computers used for remote work with others. If sharing is unavoidable, create a separate user account.
- When using public Wi-Fi outside the home or office, turn off file sharing on your computer.

No. 5 Gathering Security Information

Be aware of threats and attack methods, and use this knowledge to develop measures

There has been an increase in sophisticated tactics where attackers send virus-laden emails pretending to be business partners or associates, or set up fake websites that resemble legitimate ones in order to steal IDs and passwords. It is important to be aware of these threats and attack methods and to take appropriate countermeasures.

Action

- Stay informed about the latest threats and attack methods by via the websites and newsletters of security organizations such as IPA (Information-technology Promotion Agency).
- Check the alerts provided by the internet banking and cloud services you are using.
- During remote work, administrators should provide timely warnings to employees, and employees should promptly report any security concerns.

Explanations & Recommended Actions

Part 2 Employee measures

Items No. 6 to 18 are points that employees must be aware of. Handling sensitive information on a daily basis can lead to human error resulting from complacency. It's important to stay alert as the nature of threats changes every day.

This is an e-mail from a well-known customer. You don't have to worry about opening the attached file.

No. 6 E-mail

Be suspicious of any e-mails received from unknown senders

Incidents involving virus infections by opening e-mail attachments or by clicking URL links in the body of an e-mail continue to happen. Be cautious of e-mail attachments and clicking URL links from unknown senders.

Action

- Do not carelessly open attachments or access links in suspicious e-mails.
- Share information about suspicious e-mails within the company.
- Enable a spam filter.

No. 7 E-mail

Prevent sending e-mails to the wrong recipient

There continues to be incidents involving leaking information to third parties by mistakenly sending e-mails or faxes to the wrong person. Be sure to carefully check 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 all the recipients' e-mail addresses.

Action

- Double check the recipient before sending emails or faxes.
- Use BCC to avoid displaying multiple email addresses.
- If your e-mail software has features such as recipient checking, postponing sending, and canceling, enable them.

No. 8 E-mail

Protect sensitive information when sending it in e-mails

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

Action

- Sensitive information must be written in document files and protected with strong passwords. Passwords must be decided in advance or communicated by other means, such as mobile phone short message services (SMS).
- When sending and receiving sensitive information between organizations, use encryption technology such as S/MIME* to prevent eavesdropping and impersonation as well as to detect tampering.

*Secure/Multipurpose Internet Mail Extensions: Technology to prevent eavesdropping and tampering of e-mails

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 illicit connections. Be sure to set the security configuration of wireless LANs properly to prevent eavesdropping and unauthorized use.

Action

- Select a strong encryption method (WPA2 or WPA3).
- If the initial password (network security key, passphrase, etc.) is easy to set, increase the number of characters and use a combination of letters, numbers, and symbols, avoiding words found in dictionaries to prevent it from being easily guessed.
- Turn off mobile routers and smartphone tethering functions when not in use.
- Set a strong, hard-to-guess password for managing Wi-Fi router settings.
  - ✓Verify that the access point (SSID) is legitimate (be careful not to connect to a fake access point).
  - ✓If connection is possible without a password, or if the password is publicly available, do not exchange confidential information or personal information.
  - ✓When exchanging sensitive information, use a website that supports HTTPS communication (TLS/SSL) *1 or VPN *2 communication.

*1 Transport Layer Security/Secure Socket Layer is a technology that encrypts communications over the Internet and prevents eavesdropping and tampering by third parties.

*2 Virtual Private Network is a technology that enables security equivalent to that of a dedicated line connection even when using private virtual lines, the Internet, or public networks.

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 by employees on social media or message boards 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

- Establish rules and precautions when using the internet.
  - ✓When browsing websites, check the server certificate for IDs.
  - ✓Do not post sensitive or personal information on social media.
- Implement technical measures like web filtering and proxies to restrict access to certain websites.

Explanations & Recommended Actions

No. 11 Backup

Conduct backups

Data saved on a PC or server can be lost due to a malfunction, operational errors, virus infection, or other causes. Obtain backups of data to prepare for such unexpected situations.

Action

- Back up sensitive information periodically.
- Only connect devices and media used for backup to the computer when performing backup.
- Prepare multiple devices and media for backup, and store one of them in a remote location.
- Regularly check that the data can be restored without any problems and that the backup method is appropriate.

No. 12 Storage

Handle sensitive information/documents properly

It is dangerous to leave information/documents unattended on a desk as they can be taken or read by someone. Sensitive information/documents must be handled properly, and not left unattended, to prevent others from seeing or coming into contact with them. Specify restricted storage location for information/documents, take them out only when necessary for work, and return them to their proper locations when finished.

Action

- Keep your desks clean and put sensitive documents in a locked container.
- When handling sensitive or personal information at home through USBs, CDs, DVDs, or other types of media, make sure that they are always stored in a secure container and only removed from storage when necessary.

No. 13 Taking Out Information

Take sensitive information in a safe manner

When taking sensitive 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

- Implement a system for recording when sensitive information is taken out of the office.
- Protect devices such as laptops, smartphones, and USB memory sticks with a password.
- Do not leave computers or documents unattended when remote working in public places such as cafes, hotels, or stations.

No. 14 Office Safety

Do not let anyone use devices without permission

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

Action

- Use screen lock on your computer when leaving your seat.
- Shut down the computer when leaving for the day.
- In places with many people, use a privacy filter to prevent others from peeking at the computer screen.

No. 15 Office Safety

Approach people you do not recognize

There is a risk of information being stolen if access to the office is not restricted. Be sure that unauthorized people are not allowed access to the places where sensitive information/documents are stored, especially servers, archives and safes.

Action

- Do not allow unauthorized entry.
- Set up a reception desk.
- Set up cameras at entries and exits, as well as places where sensitive information is stored.

No. 16 Office Safety

Prevent the theft of equipment and accessories

While devices such as laptops, tablets, and USB memory 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

- When leaving work, put your laptop, tablet, and other equipment (CDs, USB memory sticks, external hard drives, etc.) in your desk drawer.
- Convert your laptop and tablet to thin client* devices.

*A system that does not store data on the device

No. 17 Office Safety

Pay attention to locking office doors

Keeping a record of the last person to leave the office also helps to improve the sense of responsibility for the last person to lock the door. Ensure proper management of lock-up and exit records.

Action

- Ensure strict key management.
- The last person to leave the office must lock the office and leave a record of their exit (date, time, and name).
- Install a smart lock*.

*Equipment that allows remote locking and confirmation of entry and exit records online.

No. 18 Safe Disposal of Information

Dispose of sensitive information properly so that it cannot be recovered

Simply throwing documents containing sensitive information into the trash leads to serious information leaks as other people can read the documents. In addition, information saved on electronic devices and media can be restored even if the files are deleted. When disposing of sensitive information, use appropriate destruction methods for each media, such as a shredder or data erasing software.

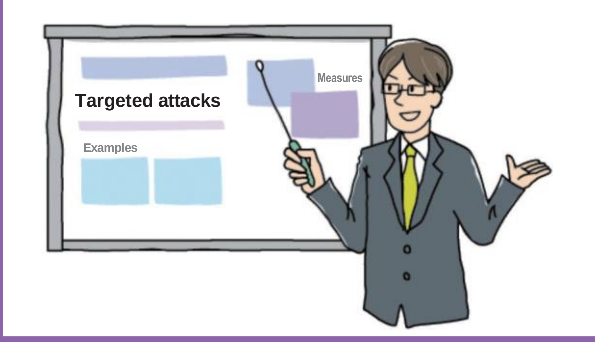
Action

- Use erasure software to erase data and dispose of documents.
- Physically destroy electronic media before disposing it.
- Outsource document destruction and electronic data erasure to a specialist service and obtain a certificate.

Explanations & Recommended Actions

Part 3 Organization measures

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.



No. 19 Confidentiality Obligation

Have employees understand their obligation to maintain confidentiality

In employment regulations and similar documents, there may be specific definitions of what information is considered confidential and the obligations of employees regarding confidentiality. It is important to clearly explain to employees what is prohibited and what should be kept confidential, ensuring they fully understand their responsibilities.

Action

- Explain confidentiality obligations to employees.
- Exchange a confidentiality agreement.
- Clearly identify information that is confidential.
- When handling confidential information during remote work, explain the need to be cautious about the work environment.

No. 20 Employee Education

Conduct information security training for employees

Employees handle information every day in their work, and this routine means there tends to be oversights in managing information securely. Regularly educating employees on this matter is effective in increasing employee awareness.

Action

- Explain confidentiality obligations to employees.
- Exchange a confidentiality agreement.
- Clearly identify information that is confidential.
- When handling confidential information during remote work, explain the need to be cautious about the work environment.

No. 21 Use of Personal Devices

Decide whether to allow the use of personal devices for work

Using personally owned computers or smartphones for work makes it difficult to ensure security and proper management. Decide whether personal devices can be used for work and make efforts to set rules on their use.

Action

- Decide on rules for the approval for using personal devices and when to use them.
- Establish rules for using personal devices, Wi-Fi routers, and home Internet connections for remote work.

No. 22 Management of Business Partners

Request that business partners maintain confidentiality

Do not assume 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

- Enter contracts or memorandums of understanding that clearly outline confidential and other general measures.
- Select business partners who have publicly announced their security policies and confirm the condition of their information security measures.

No. 23 Use of External Services

Use trusted external services

When choosing external services such as cloud services based solely on cost, you may not be eligible for compensation if the service becomes unavailable due to an outage or other issues. When using external services, be sure to carefully evaluate their performance, reliability, coverage, and other factors.

Action

- Confirm information such as the terms of use, compensation, and security measures when choosing business services.
- For remote work or when using cloud services, use the services provided and chosen by your company.

Explanations & Recommended Actions

No. 24 | Preparing for Incidents

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 can lead to a more serious impact of the incident. Use incident information reported in the media as a reference to think about who will do what and when, if the same thing happens in your company. Plan for potential scenarios in advance.

Action

- Create response procedures for the leakage, loss, or theft of sensitive information and keep employees informed.
- Decide on a contact person in case of incidents such as virus infection, loss or theft of computers or documents during remote work and inform remote workers of this contact person.

No. 25 | Establishing 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 detailed rules, employees will have to seek advice from their managers all the time. To allow employees to act according to the rules on their own, it is necessary to clearly document “companywide rules” ensuring that they are accessible and visible to employees at all times.

Action

- Share the information security diagnostic sheet and address rules 1-24 internally.
- Even after rules are set, make updates if there are issues.
- Compile the rules for remote work into regulations and share them internally.

IPA 独立行政法人情報処理推進機構
Information-technology
Promotion Agency, Japan（IPA）

E-mail isec-pr-nw@ipa.go.jp URL https://www.ipa.go.jp/en/

SECURITY ACTION
URL https://www.ipa.go.jp/en/about/activities/security-action.html

2025.5 Version