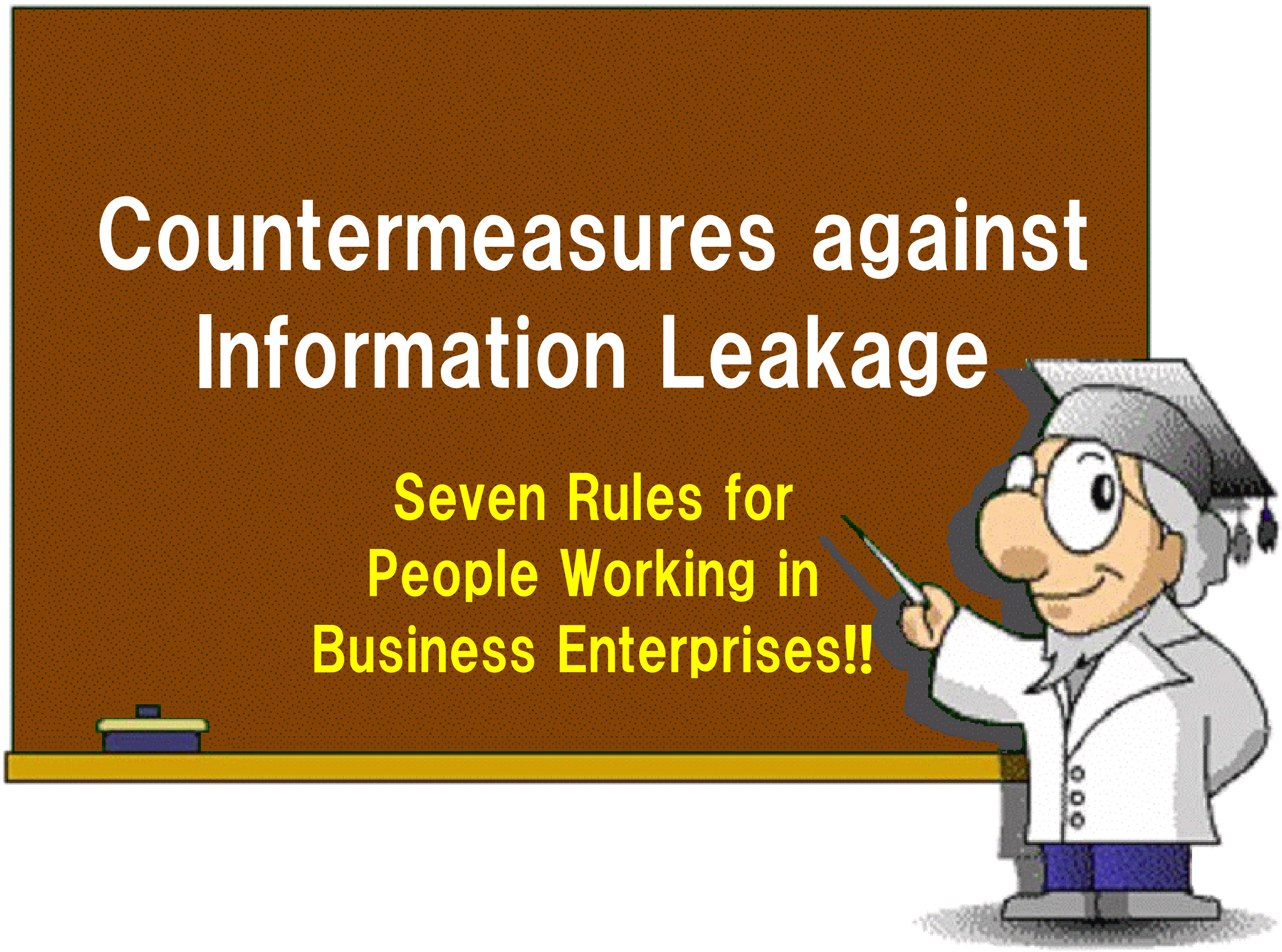
IPA Countemeasure Guide Series (5)



Countermeasures against Information Leakage

Seven Rules for People Working in Business Enterprises!!

Information-technology Promotion Agency
IT Security Center
http://www.ipa.go.jp/security/

July 1, 2014 Seventh Edition

This guide presents seven rules that should be followed by the people working in business enterprises to prevent information leakage.

To keep important information from being compromised, organizations need to establish their own security policy and follow it.

Note that you cannot prevent the leakage of important information (or data) belonging to your organization only by observing the rules presented in this guide.

However, the seven rules can serve as a guideline to keep yourself from accidentally leaking your organization's important information, while carrying out your work.

Seven Rules for People Working in Business Enterprises

(1) Do not take out your organization's IT resources (*1) without permission;

Don't take them out without permission

(2) Do not leave your organization's IT resources unattended without taking appropriate measures (*2);

Don't leave them unattended

(3) Do not easily dispose of your organization's IT resources without taking appropriate measures;

Don't easily dispose of them

(4) Do not bring in the office your personal devices (PC, electronic media), programs and data without permission;

Don't bring in personal devices

(5) Do not rent or transfer your assigned privilege (*3) to a third person without permission;

Don't rent your privilege

(6) Be careful not to let out business information obtained at work;

Don't let out business info.

(7) If you have accidentally leaked important information, report it first without making your own judgment.

Report it first

1. Do Not Take Out Your Organization's IT Resources without Permission

Taking out, without permission, your organization's PC, electromagnetic media or documents that contain business information, and bring them home to do some work: this should be strictly forbidden.

According to a survey conducted by Japan Network Security Association (JNSA), as for the causes of information leakage, "Lost/Misplacing" accounts for 29.2% and "Theft" for 19.0% (i.e., representing about half of all the cases). When taken out, IT resources might be involved in such incidents, and we cannot ignore this risk.

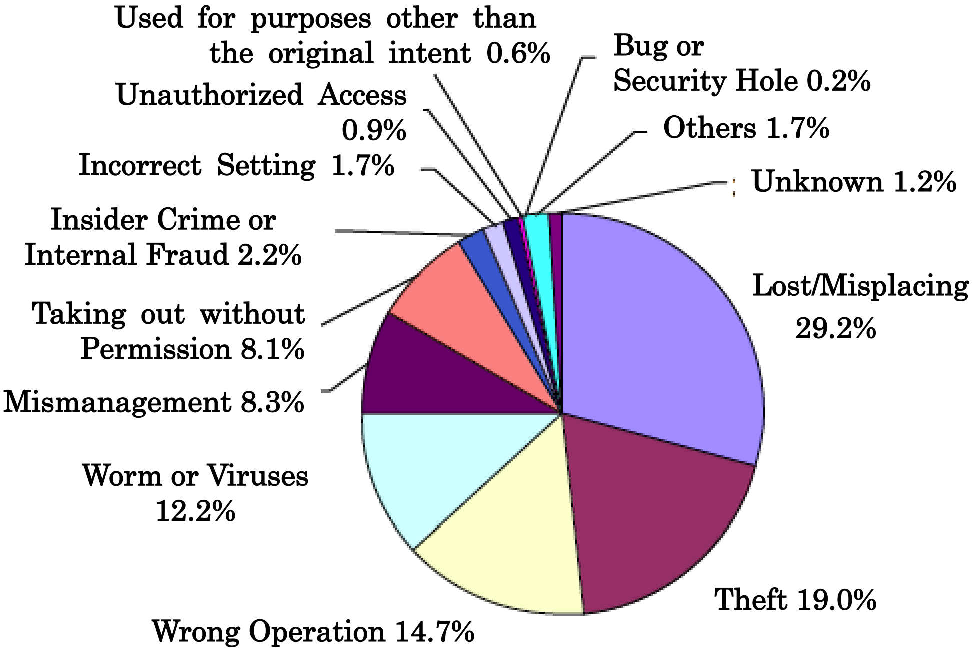


FIGURE 1: CAUSES OF PERSONAL INFORMATION LEAKAGE (YEAR 2006)
Extracted from a survey material by JNSA, posted on the Web below:
http://www.jnsa.org/result/2006/pol/insident/070720/

Furthermore, given that many organizations have reportedly suffered from information leakage due to "Lost/Misplacing" and "Theft", it is risky to allow employees to take out their organization's IT resources and use them unobserved by the management.

Even if you have permission to take out your organization's IT resources, it is your responsibility to keep them safe. If you think that there is a high risk of such resources being stolen or lost/misplaced, you should not carry them out.

Two principles that should be followed are as follows:
"Don't take out important information" and "Don't bring your work home with you."

According to the latest survey, the breakdown for the causes of personal information leakage was as follows:

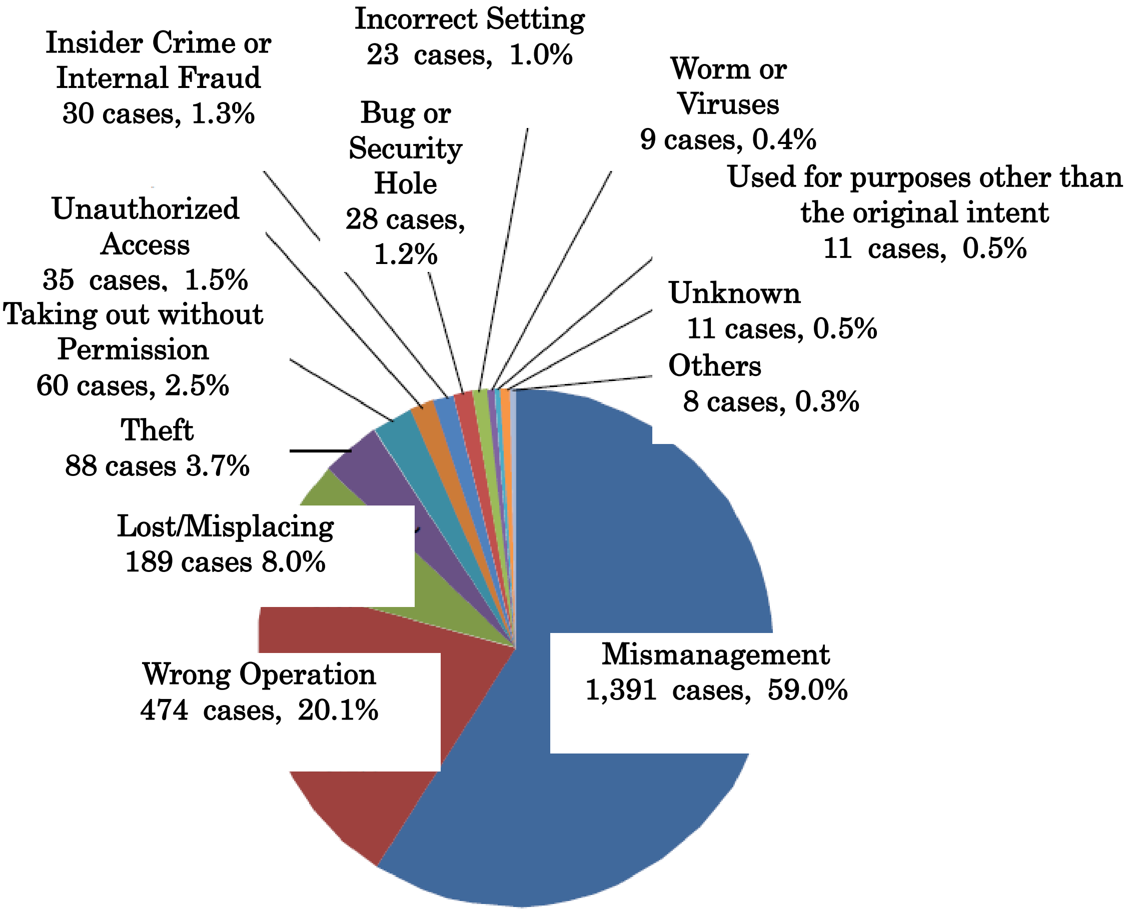


FIGURE 2: CAUSES OF PERSONAL INFORMATION LEAKAGE (YEAR 2012)
Extracted from a survey material by JNSA, posted on the Web below:
http://www.jnsa.org/seminar/nsf/2014/data/NSF2014_A3_ootani.pdf

Here, at the top for the causes is "Mismanagement". Said in one word "Mismanagement", it would be hard for you to grasp. According to JNSA's solution guide (http://www.jnsa.org/solguide/), this includes the cases below, all of which were due to the fact that, the organization's management guideline and procedure (management rule) were not strictly followed by its employees.

⚠ During the move to a new place, personal information went missing (e.g., erroneous disposal)

- ⚠ Confirmation of the delivery and receipt of personal information was insufficient, resulting in the loss of supposed-to-be-received personal information.
- ⚠ Information disclosure and management rules were not clarified, resulting in an accidental disclosure.

Nowadays, organizations have come to establish security policy and management procedure in handling IT resources. Despite this, problems often lie in the side of organizations that say: "We have management rule in place, but failed to have our employees observe it." This highlights the importance of providing security education to employees, and having employees follow information management procedure.

Even if you have permission to take out IT resources

The following actions should be restricted when taking out your organization's IT resources:

- **Using sensitive information on a PC that is not under your control (such as PCs at an Internet cafe);**
- **Needlessly (or defenselessly) connecting a taken-out PC to an external network;**
- **Using a taken-out PC for non-business purpose, or renting it to others.**

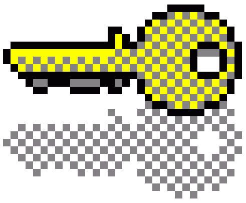
You need to exercise caution when using your organization's IT resources in an insecure environment.

When you take out your organization's PC for business purposes, you need to make proper settings and follow the defined usage.

We often hear that, a taken-out PC connected defenselessly (i.e., with no security control in place) to an external network (e.g., Wi-Fi in the city, a budget hotel's network) was infected with a virus; the PC was brought back to the office and connected to the organization's network; and the virus spread across the organization.

The cause of such problem is that, sufficient security controls are not in place, generally due to the lack of understanding about the difference between the protected organizational environment and an uncontrolled external environment. If the virus was Spyware, information/data stored would be compromised. For a taken-out PC, you need to implement adequate security controls.

When you take out business information/data for business purpose, it is recommended to **encrypt** them.



By doing so, even if a PC or electronic medium (e.g., FD, CD, DVD, HD, or USB memory) containing such important information/data is stolen or lost, you can deter information leakage.

For the same reason, when sending business information/data by email or as an attachment, apply encryption. By doing so, even if the email is sent to a wrong address or intercepted by someone else, such important information/data is protected from unauthorized disclosure.

To encrypt data, you can use specialized application software, which may require having a password for data-decryption. Note that, depending on the application, both the sender and receiver may be required to use the same application.

Applications such as Microsoft Word and Excel have a password protection feature for their documents and sheets/books (Refer to Section 9, "References".)

But remember this: encrypting data is not enough for protecting against information leakage. The purpose of encryption is to protect data itself, not to prevent information leakage.

When you take out your organization's IT resources, "Do not leave them unattended without taking appropriate measures" (which is described in the following section.)

2. Do Not Leave Your Organization's IT Resources Unattended Without Taking Appropriate Measures

Let's think about what should be restricted. Specific examples are:

- Leaving your seat or the office with important business documents left on your desk;
- Leaving printed documents on a remote printer;
- Leaving your PC unattended so anybody can use it (i.e., password-protection not applied);
- Leaving the office with your mobile computer left on your desk;
- Leaving electronic media or documents containing important information on your desk, instead of putting them in a lockable

cabinet;

- Leaving a personal message slip in a place where anybody can access.

You may think "You don't have to tell me these things!!" but these are important.

For example, we often hear that important documents, whose retention period is over and thus collected for disposal, are piled up on a passage instead of a secured room (because such room is not available), until a waste disposal contractor come and pick them up. This allows anybody walking through this passage to see the documents.

So, even if you watch out, unless everybody within your organization does, information leakage could still occur.

It is recommended to keep important business documents, electronic media, and mobile computers in a lockable cabinet when not in use.

When you leave your seat, let's lock your PC either by applying "computer lock", or making settings in advance for automatic activation of password-protected screen saver.

(Reference) - Utilizing "Computer Lock" Feature -

When you leave your PC, lock it so others cannot use it.

If you are using Windows OS, press:
"Ctrl" and "Alt" and "Delete" keys
(for "computer lock")
or
"Windows" key and "L" key

By doing so, you can restrict access to your PC by others.

This may be nothing to speak of, but it is a good manner to leave message slips turned down.

And take care not to expose your organization's IT resources in a place where unspecified number of people can access.

Even when you take out your organization's IT resources with permission of your boss, be careful not to:

- Leave a bag full of important materials on a train rack and fall asleep;
- Visit such places as bar and pachinko parlors, carrying a bag full of important materials.

These are risk-taking behaviors.

3. Do Not Easily Dispose of Your Organization's IT Resources without Taking Appropriate Measures

We often hear that, information was leaked from a PC once used in an organization and discarded without wiping its hard disk clean.

Similarly, we often hear that, business information was leaked from the electronic media or documents carelessly thrown out in a garbage box.

Nowadays, some companies offer a service of wiping hard disk clean. You can use such service, or establish and implement organization-specific procedures and technologies for the disposal of such materials. If your organization has no such rules, you may be the one to establish them.

It is out of the question to throw important documents and electronic media into a garbage can.

Are you sure you don't throw important documents in a garbage can?
機密
Confidential

As for important documents, it is recommended to shred or melt them under the supervision of your manager, or to have a specialized contractor do it.

As for electronic media (e.g., FD, CD, DVD), unless reusable, destroy it before throwing it away.

4. Do Not Bring in the Office Your Personal Devices (e.g., PC, Electronic Media), Programs and Data without Permission

Again, let's think about what should be restricted. Specific examples are:

- Bringing in your privately-owned PC and connecting it to your organization's network;
- Using irrelevant (i.e., unrelated to or unnecessary for your job) information/data while at work;
- Running an irrelevant, privately-owned program while at work;
- Downloading an irrelevant program (Freeware or Shareware) from the Internet;
- Accessing an irrelevant website using your organization's PC;
- Using your business e-mail address for non-business purposes;
- Bringing in an external storage device (e.g., USB thumb drive) and connecting it to your organization's PC.

■Risk of Bringing in Privately-Owned IT Devices

If a brought-in, privately-owned PC or external storage device (e.g., USB thumb drive) had already been infected with a virus, the infection might spread to other PCs and servers within the organization. If the virus was Spyware, **important business information might leak via the Internet**.

Recent situation

BYOD (Bring Your Own Device)

"Bring your own device" signifies that, employees do their job using their own device. But, self-seeking BYOD is very dangerous.

BYOD has both advantages (e.g., cost reduction, efficiency improvement) and disadvantages (e.g., the risk of information leakage increases when taken out), and it is tried in various fields.

Anyway, BYOD has momentum to change the future vision of information technology …

Current stance of organizations is: depending on circumstances, **"Organizations conduct checks and give permission if needed…"**

■Risk of Using Unauthorized Programs

A program downloaded from a website or brought in from outside could be Spyware. You should refrain from using programs irrelevant to your job.

If you think the program is really necessary for your job, check first its behavior in a secure environment, and then use it under the permission and management of the administrator.

■Risk of Using Unauthorized Services on the Internet

When an organization's important information is stored in an unauthorized network (online) storage service, or managed using a map service or information-sharing service, information leakage might occur due to improper settings or use.

While those services may help improve operational efficiency, users need to understand service mechanism as well as setting method, and use them with the permission of their manager.

A number of cases have been reported in which, users of such service forgot to make settings for what information is allowed/prohibited to be disclosed and to whom (i.e., did not know the presence of such settings and consequently, all the information registered was disclosed to everybody (by default setting)), resulting in information leakage. Recently, default settings for such scope in those services are securer than before, but still we need to watch out.

■Risk of Malicious Websites

Some malicious websites are designed to execute a malicious code if site visitors perform operations instructed.

Even if sufficient anti-virus/anti-spyware measures are taken in the environment, there are still viruses and spywares that cannot be detected by anti-virus software; so you should exercise cautions.

In particular, **there are spywares that target a specific organization or individual**, rather than targeting unspecified number of people; so you should refrain from accessing websites irrelevant to your job.

Nowadays, even a website relevant to your job might be defaced. In such case, you might be redirected to a malicious website against your will. So, be sure to implement the following measures:

- Keep the operating system and applications on your PC up-to-date, so that existing vulnerabilities are eliminated.
- Activate your antivirus software, so that known viruses are detected and cleaned, and that programs acting suspiciously are monitored.

■Risk of Information being Compromised due to Wrong Operations

There is a case where information is automatically saved on a PC or external media (e.g., USB thumb drive) without the user knowing. If the PC or external media is the one you brought from your home, you might bring it back home. In this case, important business information might be taken out from the office without permission, making it difficult to identify the source of compromise.

Furthermore, if you use your organization's email system for personal use, you might accidentally send important business information to a wrong address. Or you might also let out such information by carelessly posting messages on a blog site or a bulletin board.

You should refrain from performing those actions.

Information stored on the computer
コンピュータ内の情報
Information leaked!!
Non-business operation can cause information leakage.

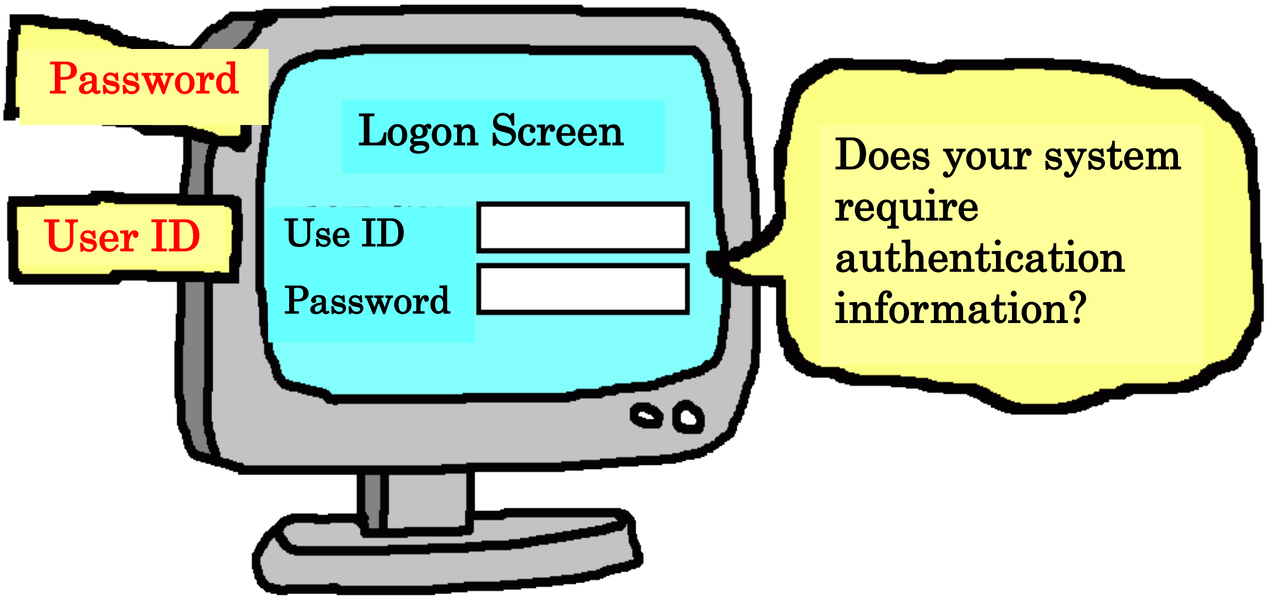
5. Do Not Rent or Transfer Your Assigned Privilege to a Third Person without Permission

Generally, an organization grants privileges to certain personnel based on their job and the team they belong to. This is what is called "Authority". However, renting or transferring this privilege to a third party should not happen in normal circumstances.

Similarly, rights to access business information and devices are given only to authorized personnel. In other words, access rights are assigned to each user ID and the IDs are protected by passwords or other authentication information.

Sharing or renting user IDs and passwords can cause a serious information security problem.

User ID and password are used to identify each user, so renting your User ID and password to a third person is a foolish conduct. For the same reason, **you should not write down your password on a slip and attach it on your PC's screen.**



Authority is always accompanied by responsibility. To carry out your responsibility, be careful not to take rash actions.

Unauthorized use of other persons' user ID and password is regarded as **masquerading (or impersonation)**, which violates **the Unauthorized Access Prohibition Law** (*4).

6. Be Careful Not to Let out Business Information Obtained at Work

In the first place, "Not letting out information obtained at work" is "confidentiality obligation", which is considered a general moral for people handling information (as a member of society).

As often-heard stories, don't you have images below?

- Confidentiality obligation related to medical treatment: Do not let out information about patients;
- Confidentiality obligation related to schools: Do not let out information about students;
- Confidentiality obligation related to the police: Do not let out investigation information;
- Confidentiality obligation related to court/trial: Do not let out information about persons involved;
- Confidentiality obligation related to worker dispatching: Do not let out information obtained at the dispatched company.

In this way, what to protect varies depending on the line of business (i.e., not limited to those listed above). Confidentiality obligation is imposed on other fields as well.

Generally at organizations, new employees are taught about confidentiality obligation in the first place. But if they are not reminded of, they tend to forget it in due course. Even a bit of off-guard might result in information leakage.

For example, while you have a chat with a compatible colleague, somebody may be listening and get the business information you chuck out. Well, I don't think there is a person who blabs business information to unknown people (if he or she remembers confidentiality obligation).

Shoulder Hacking is an act of looking into information over someone's shoulder, aiming at stealing it. Don't forget: **"You never know who is watching or listening."**

Again, let's think about what should be restricted. Specific examples are:

- At a bar, talking about your work contents in a loud voice, including ill feelings against your superiors;
- On a train, talking business over a mobile phone (it is a bad manner);
- Working with your PC on the Bullet train for a business trip (Permitted to take important information out?);
- Reviewing documents on a train home (Permitted to take important information out?);
- Working in a smoking area in a building where unspecified number of people can access;
- Posting business information on a blog site or electric bulletin board for the purpose of introducing yourself.

There are plenty of other examples, but the above-mentioned actions involve a high level of security risk. People harboring bad intentions can be anywhere. Allowing them to overhear or peep into even a small amount of information can lead to a serious information leakage. To avoid becoming the source of information leakage, refrain from the actions listed above.

Recently, we often hear the cases involving blogs and electric bulletin board (the one listed last in the specific examples above.)

Nowadays, an increasing number of people are using SNS (Social Networking Service), an interactive website on the Internet, to establish social network. So, anybody can easily become a sender of information. While some people transmit immoral information or bogus information to get attention of the other participants in the service, others post the information obtained at work (which should not be disclosed to external parties) to attract people, as if presenting their diary. Even if the person thinks that he perfectly camouflaged such information, when combined with other information on the Internet, it may lead to so much trouble to the organization he works for. To help people understand this story, IPA released some videos for security education and enlightenment, as shown below. If you are interested, feel free to visit:

Videos for Information Security Education and Enlightenment

http://www.ipa.go.jp/security/keihatsu/videos/ (in Japanese)

YouTube：IPA Channel

http://www.youtube.com/ipajp/

IPA 独立行政法人情報処理推進機構
技術本部 セキュリティセンター
映像で知る情報セキュリティ
ドラマやドキュメンタリーを通じて
最新の脅威と対策を学びましょう!
集合研修に
最適!
For Windows
定価：本体186円(税別)

The followings are examples of an attack called **Social Engineering**[*5]. This can also be used to compromise information.

- A phone call from outside, pretending to be a friend of an employee having a day off, asking his (or her) contact number or work contents;
- A phone call from a would-be system administrator, asking personnel's user IDs and passwords;
- A fake membership registration screen requesting users to enter the details of their work contents.

It is "Negligence" that allows information to be compromised, so daily attitude is very important.

Hello, I am the system administrator. There is a problem with the system, so we need to perform user registration again. Can I have your User ID and Password, please?

7. If You Have Accidentally Leaked Important Information, Report it First without Making Your Own Judgment

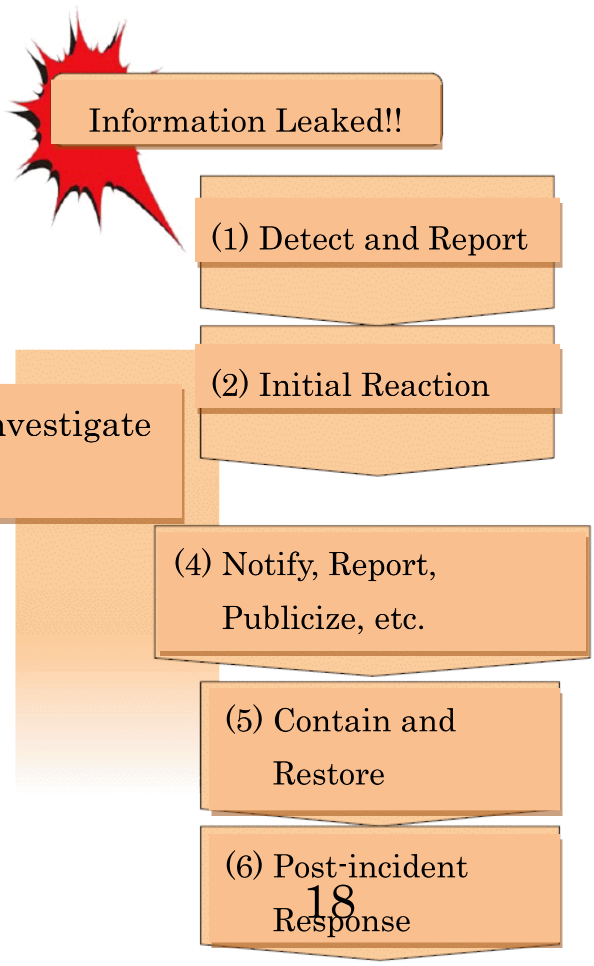
If you have accidentally leaked important information or discovered the leakage of such information, report it to your superior or the system administrator, rather than trying to solve it by yourself.

In the event of information leakage, you should not worry only about your company (organization). You need to minimize the damage to all the people affected, including those whose personal information leaked (e.g., individuals, clients, business partners, shareholders, parent companies, affiliate companies, employees.)

It is important to minimize damages incurred, based on your company's management policy and considering overall balance.

■ Points for Responding to Information Leakage
http://www.ipa.go.jp/security/awareness/johorouei/ (in Japanese)

Prompt responses help minimize problems.



8. Terminology

(*1) IT Resource

IT resources refer to business data (including programs) and equipment (such as PCs, electronic media, papers and documents) containing such data.

(*2) Without Taking Appropriate Measures

A state in which no security controls are implemented.

(*3) Privilege

Privileges are given to users so they can access resources. **Grunting Minimum-Required Privilege** is a basic point of security policy; it is important to grant privileges as in a narrow scope as possible.

(*4) Unauthorized Access Prohibition Law

A law to prohibit unauthorized access and relevant activities, which was passed by the Diet on August 6, 1999 and came into force on February 13, 2000, except for Article 6. And, Article 6 concerning assistance was also enacted on July 1, 2000, and the amended law was enforced on May 1, 2012.

For actual articles, visit the following website:

http://law.e-gov.go.jp/htmldata/H11/H11HO128.html (in Japanese)

The "Regulations on Assistance by Regional Public Safety Commissions for the Prevention of the Recurrence of Unauthorized Access", which was established by the National Public Safety Commission, can be found at:

http://www.npa.go.jp/cyber/legislation/kitei/enjyo_kitei.htm (in Japanese)

In addition, if a computer was caused to malfunction or data corrupted due to an unauthorized access, the person who performed the access would be charged with "Forcible Obstruction of Business".

(*5) Social Engineering

Method to illicitly obtain legitimate users' confidential information (such as their passwords) by exploiting their feeling and a loophole of the society, rather than using network or computer technologies.

Examples include: asking for a password using a clever turn of phrase; obtaining important information from rejected materials; masquerading as an employee and listening to or peeping into information.

This method is also called "social work", "social hacking", or "social cracking".

9. References

IPA Countermeasure Guides Series

http://www.ipa.go.jp/security/antivirus/shiori.html

- IPA Countermeasure Guide (1) Countermeasures on Computer Virus
- IPA Countermeasure Guide (2) Countermeasures on Spyware
- IPA Countermeasure Guide (3) Countermeasures on Bots
- IPA Countermeasure Guide (4) Countermeasures on Unauthorized Access
- IPA Countermeasure Guide (5) Countermeasures on Information Leakage
- IPA Countermeasure Guide (6)　Guide for <Avoidance of Risks> When You Use the Internet
- IPA Countermeasure Guide (7)　Guide for <Avoidance of Risks> When You Use Electronic Mails
- IPA Countermeasure Guide (8)　Security Measures Guide for Smartphone <Avoidance of Risks>
- IPA Countermeasure Guide (9)　Guide for First-Time Information Security Countermeasures
- IPA Countermeasure Guide (10)　Countermeasures against Targeted Attack Mail <Avoidance of Risks>

IPA®

Information-technology Promotion Agency
IT Security Center
2-28-8, Honkomagome, Bunkyo, Tokyo, 113-6591 Japan
(Bunkyo Green Court Center Office, 16th Floor)
URL http://www.ipa.go.jp/security/