takasago Secrecy

Request for information leakage countermeasures

7 rules

The environment surrounding information security is changing in various aspects, and threats and issues are also changing.
Individuals have to do the following for information security.
Gain the necessary information security knowledge, Raise your awareness of information management,
Thoroughly implement information security measures.

1 Internal use only

Do not take out “information assets(*)” without permission. (* documents, data, etc.)
When bring out information assets, keep them in a bag etc. and always with you.
Electronic data must be encrypted, set passwords, etc.

- When bring out information assets, keep them in a bag etc. and do not leave them out of sight.
- If you participate in the drinking party, do not take information assets out even if you have permission.
- Set the password when sharing information by email or OneDrive, etc.

2 Do not leave information assets easily

Do not leave important documents or electronic media when leaving a desk or returning home.

- When leaving a desk, turn over the documents, store them on the cabinet, and password lock the PCs.
- Documents and mobile PCs are stored in desks or lockable cabinets, when returning home or all concerned are absent for a long time.

3 Do not disposing of information assets easily.

Do not dispose of information in an available state.
Take action to make information easily unavailable, if disposing information assets.
The removable media must be processed, such as crushing.

- When disposing a document, its shredder or request a specialized company to dissolve.
- When data erasure on a devices, request a specialized company or use dedicated software.
- The removable media is destroyed before disposal.

4 Unauthorized devices is prohibited for business use.

Do not use devices(*) other than the authorized devices for work.
*PC, Smart phone, removable media
When using devices other than authorized devices, take necessary measures before using them.

- Make the necessary security settings.
- The precautions when using are the same as for company devices.

5 Do not lend or borrow a user ID/ password.

Do not lend the ID (authority)/password assigned to the individual to others.

- Do not lend the ID / password to others.
- Do not ask for other's ID / password.

6 Do not disclose company internal information.

Do not disclose confidential business information acquired without permission.

- Do not disclose the information of the business to third parties who are not related to the business.
- Even manufacturers or business contractors with whom confidentiality agreements have been concluded will not provide information that is unnecessary for requesting and outsourcing.
- Do not post business information to public places such as SNS. (Includes thoughts & feelings on business)
- When using a smartphone or the like, disable the function for automatically linking information to SNS or the like.

7 Discuss / Report

- Do not make your own judgment but first discuss/report, if you do not know how to handle information or have an information incident.

Reference Information Security Management Office (Email : information_security_office@tte-net.com)
高砂熱学工業株式会社
Takasago Thermal Engineering Co., Ltd.
(2021.1)

takasago Secrecy

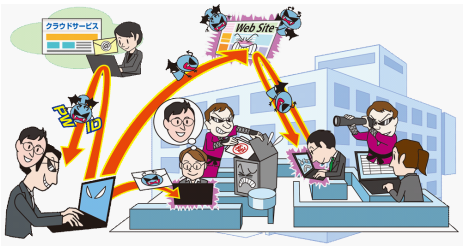
Point to notice for threats and countermeasures

Information security measures are becoming more diverse and complex due to changes in lifestyle and awareness of personal information.
We have to collect information on the latest security threats through newspapers and news reports.

Confidential Information Theft by Advanced Persistent Threat

Hackers send virus mail to a specific company and remotely control a computer infected with a virus.
And they steal organization's confidential information.

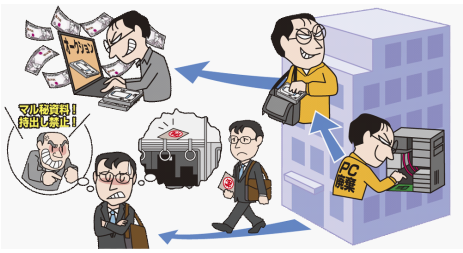
⇒Don't open suspicious email attachments.
⇒Don't visiting malicious websites.



Information Leakage by Internal Fraudulent Acts

Information leakage caused by an employee illegally taking out information, misusing it, or losing it..

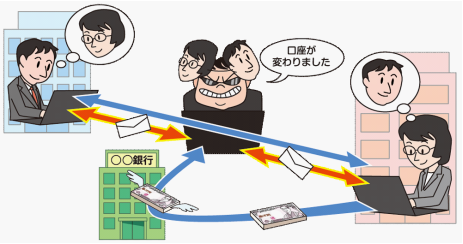
⇒Observe the rules of information management.
⇒Make appropriate access settings for important information.



Pecuniary damage by Business E-mail Compromise

Manipulate emails and trick organization's financial staff into sending it to the attacker's bank account.

⇒Be careful of fake bank transfers and remittance requests.
⇒If you feel that it is unnatural, check it in a way other than email.



Attacks Exploiting Supply Chain Weaknesses

Outsourcing partners with weak security measures are targeted as a foothold of attacks.

⇒Thorough information management and outsourcing management.
⇒Choose a trusted outsourcing partner.

Supply Chain :
It refers to a series of flows from procurement to sales. And then includes external organizations that have outsourced specific operations.

Financial Loss by Ransomware

The virus that encrypts files stored on computers etc. and make them unavailable.
And it requires money to recover files.

⇒Don't open suspicious email attachments.
⇒Make backups regularly.
⇒Fix vulnerabilities in OS and software.

To conclude

The most important thing is the security awareness of each employee. We always have to trying to take security measures as a member of the information society.

Source : Created based on “10 Major Security Threats” by IPA*.
*Information-technology Promotion Agency, Japan
https://www.ipa.go.jp/security/vuln/10threats2020.html

Reference Information Security Management Office（Email : information_security_office@tte-net.com）

高砂熱学工業株式会社
Takasago Thermal Engineering Co., Ltd.

(2021.1)