Confidential

For DEC General DM Service Department

Information Security Handbook

1. Basics

Version1.3

Introduction

The Information Security Handbook consists of two parts, "1. Basics" and "2. DM Services". This manual is "1. Basics".

This volume describes the basic information security rules that employees should follow.

Please understand what you should be aware of when doing business and the rules for handling information and check whether you can comply with the rules by comparing with your daily work and behavior.

* Services provided by DX Headquarters, DA Headquarters, and ECX Headquarters are collectively referred to as "DM services".

Information Security Handbook: 1. Basic structure

● Before getting to work

Concepts to be aware of and rules to be followed before starting work

● Under business

Rules to be followed during business response

● Before leaving the facility

Rules to follow before leaving work and after leaving work

This volume describes the basic rules of transcosmos.

Even if the operation differs depending on the organization / business office to which you belong

There are, so please check the rules of the workplace to which you belong.

Before Getting to Work

Management Philosophy/Service Mind

It is the basic management philosophy and service mind of transcosmos. Please always keep this content in mind when carrying out your work.

Basic Management Philosophy

The magnitude of customer satisfaction.
It ’s the value of our existence.
The growth of each person.
Create its size and future.

Service Mind

- **We thank our customers and**
  Let's provide services that exceed customer expectations.
- **We value communication and**
  Let's work on improving the service as a team.
- **We protect your information and assets,**
  Become a trusted partner.

Importance of Information Security

Transcosmos mainly handles outsourcing business that operates on behalf of client companies and handles a lot of information such as personal information of client companies and confidential information.
Since this information is handled based on the trust of the client company, it must be handled appropriately so that troubles such as information leakage and loss do not occur.

Main Impacts of Information Security Problems

Impact on client companies

- When personal information is leaked
  - Loss of social credibility, deterioration of corporate image
  - Compensation for individuals who have leaked information
- When information is leaked to a competitor
  - Loss of business opportunity
- If data is lost
  - Business interruption / stagnation

Impact on us

- Loss of trust from client companies
- Termination / reduction of applicable business and other client companies
- Man-hours and costs for handling, compensation for damages to client companies
- Impact on management

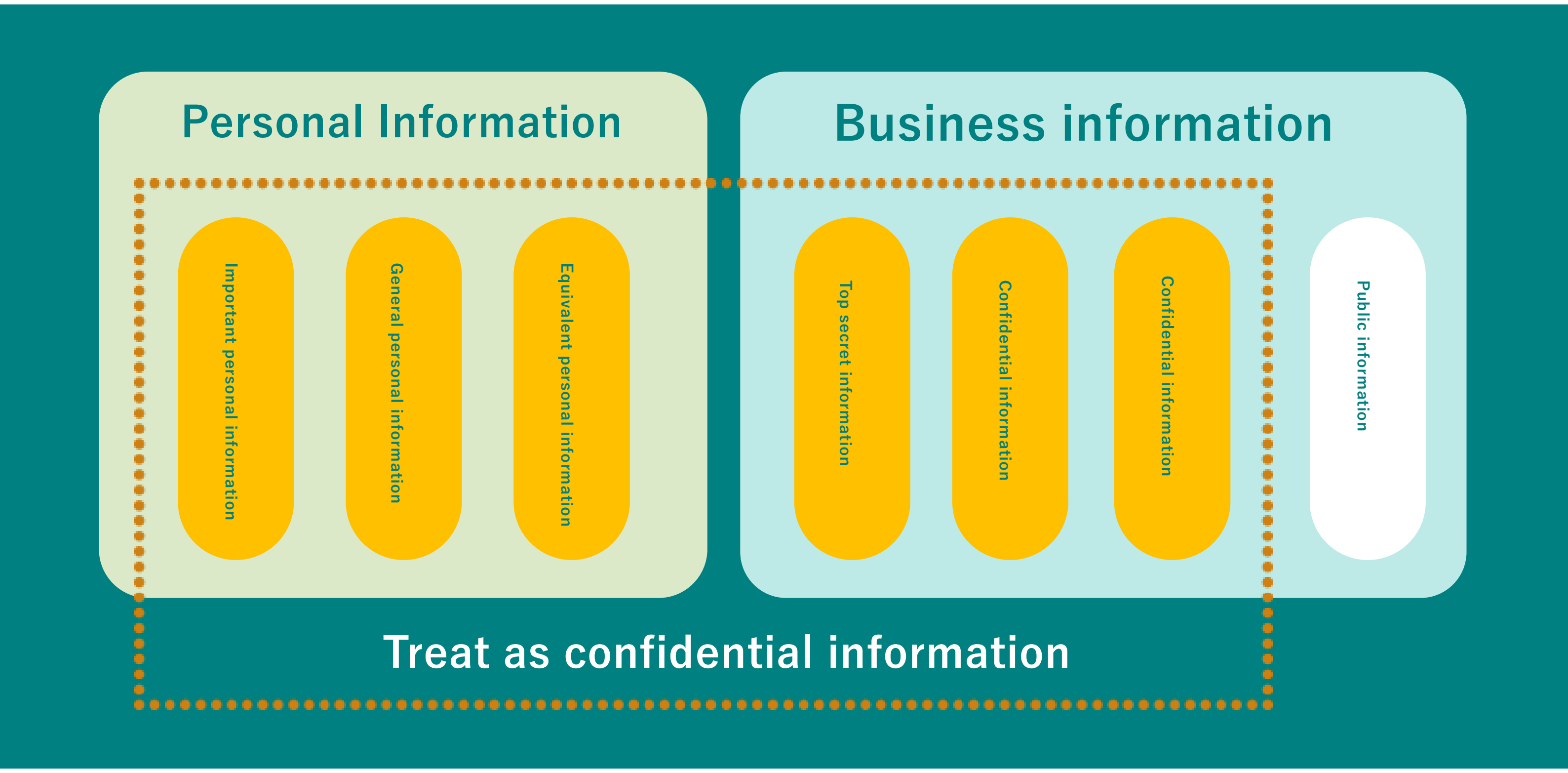
Impact on employee parties (in case of intentional or serious rule violation)

- Disciplinary action
- Compensation for damages
- Possibility of punishment

Types of Information to Protect

Organize the information handled in business and understand the information to be protected and the handling.

※Information classification in our information asset survey



Personal Information

We define personal information as follows.

“Personal information means information concerning an individual that falls under any of the following categories.

①Information that can identify a specific individual by name, date of birth, or other description contained in the information.

②Items containing personal identification codes.”

"Important personal information" defined by our company

- Personal information that has a risk of damaging the human rights of individuals or suffering financial loss of individuals in the event of information leakage.

(Information that requires special handling among personal information).

Important Personal Information

- **Personal information requiring consideration, sensitive information (sensitive information)**
  - Racial, creed, social status, medical history, criminal history, facts of being harmed by a crime, and other matters that require special consideration in handling so as not to cause unfair discrimination, prejudice, or other disadvantages to the person.
  - Matters concerning workers' right to organize, collective bargaining and other acts of collective action
  - Participation in collective demonstrations, exercise of right to petition and other matters concerning the exercise of political rights
  - Matters related to health care or sex life
- **Settlement-related information**
  - Credit number, expiration date, etc.
  - Approval website ID / PW
- **Biometric information**
  - Biometric information such as fingerprints and irises
- **My number (specific personal information)**
  - Individual number (my number)
- **Personal information about students, children and toddlers**
  - Personal information about students, children and toddlers

Examples of Personal Information

- Name of person
- Information regarding date of birth, contact information (address, residence, telephone number, email address), position or affiliation with the company, combined with the person's name
- Information recorded by security/surveillance cameras and other video information that can be used to identify the person in question
- Photographs and audio recordings of calls (content) that can be used to identify the person in question
- Content of business card
- Information on the emergency contact list created within the department
- Sent and received emails (email address information that can identify specific individuals, information in emails, and attached materials)
- Employment management information (employment information from resumes and CVs, various HR application procedural documents of employees, my number, health checkup forms, stress check results, and interview guidance results, etc.)
- Information publicly available in official gazettes, telephone directories, staff records, etc. ⇒Name of the person, etc.

- Questionnaire or website inquiry information that can identify a specific individual
- Membership information registered by purchasers in the mail-order business
- Forms (membership registration cards, call lists, etc.), data files, databases, etc. that contain personal information entrusted to us as part of out outsourced services

Business Information

Business information is classified according to the degree of confidentiality, and other than public information, it is necessary to protect and manage it as confidential information with information security.

"Confidential Information" defined by our company

- Undisclosed or pre-publication decision facts, occurrence facts, financial information, and other important facts regarding the operation, business or property of listed companies that significantly affect investors' investment decisions.
- Important facts about subsidiaries
- Minutes and materials containing this information
- Contracts and agreements with other companies with high confidentiality

"Confidential Information" defined by our company

- Various design documents, know-how on business operations, customer list, supplier list, various manuals, guidelines, training materials, proposals, quotations, contracts, minutes, intranet information with restricted access rights as confidential information and system etc.
- Contracts and agreements with other companies
- Trouble reports, information security design documents, network configuration diagrams, ISMS records (access logs, implementation records, etc.), etc.

"Confidential Information" defined by our company

- Information other than "confidential information" and "confidential information" that is not permitted to be disclosed outside the company.
- Information that can be disclosed and provided only within the company

➤ Public Information

- ◆ Information that is open to the public through catalogs, pamphlets, web publications, etc., regardless of whether it is from our company or other companies.

⚠ CAUTION ⚠

Personal information is also protected by the "Personal Information Protection Law", and businesses that handle personal information must properly acquire, use, and manage it.

Confidentiality Compliance

Basic Rule

- Information and information equipment of the company and client companies should be used only for business purposes, not for purposes outside the scope of business or for private use.
- Confidential information of the company and client companies is not handled by personal information equipment.

  ※ In addition to saving to personal computers (personal computers), storage media, mobile phones, smartphones, etc., it also includes forwarding to personal information devices using e-mail, the Internet, etc.
- Confidential information obtained during business and internal information of client companies will not be disclosed to anyone other than those related to the relevant business.
- The names of client companies outsourced by the Company will not be disclosed outside the company (excluding those disclosed in pamphlets, websites, etc. with the consent of the client companies).
- We will comply with the confidentiality obligation of confidential matters even if we leave the relevant business due to transfer or retirement.

⚠ CAUTION ⚠

- **Information leakage due to unauthorized use of information or serious rule violations is subject to disciplinary action.**
- **In addition, damages may be claimed against individuals.**
- **Confidentiality of personal information and business information must be maintained even after leaving the relevant business.**

Entering and Leaving the Facility

Basic Rule

- ● Enter and leave the room according to the method determined by the facility.
- ● When entering and exiting with a security card, each person should not hold the card and piggyback (enter / exit following the previous person).
- ● In the work area, always wear your admission card (or ID) so that others can see it.
- ● Do not enter areas that are not related to your business.
- ● Do not allow unauthorized persons to enter the room without the permission of their superior.
- ● Do not lend your admission card / security card to others.
  Also, do not use other people's things.
  - ➤ If you forget it, report it to your superior and follow the response decided by the facility.
- ● If you enter or leave the room on a holiday / holiday or outside the designated working hours, notify your superior by the day before (however, if there is an urgent need, the notification on the day will be accepted with the consent of your superior).

⚠ CAUTION ⚠

In order to maintain the security in the facility, entry and exit rules are set in each facility, and entry and exit should be done according to the rules of each facility.

Admission Card/Security Card Management

Basic Rule

● You are responsible for managing the loaned admission card / security card so that it will not be lost or stolen.

Basic rules for admission card / security card management

- When commuting, do not put it in your clothing pocket to prevent it from falling
- To prevent it from falling or being stolen, use a bag with a closed mouth or store it in the inner pocket of the bag to prevent it from falling easily.
- Do not put it in the same place as items that are frequently taken in and out of the bag (regular, wallet, mobile phone, etc.).
- Do not take it outside on days when there is no work
- If the card case is damaged, immediately repair or offer replacement.
- Keep your bag away from your body after drinking alcohol

● If it is lost or stolen, immediately report it to your superior and request a card entry suspension procedure.

● If it is no longer needed due to transfer or retirement, it will be returned promptly.

⚠ CAUTION ⚠

Loss of admission card / security card is the most common information security problem.

Be aware that it is an important loan from the client company / company and be

Restrictions on Bringing Personal Belongings to the MCM Center

Precautions when visiting the MCM Center operated by DCC

● Every base has restrictions on bringing in personal belongings, and it is necessary to follow the rules for each base. In particular, the MCM Center handles high-security level information, and restrictions on bringing in personal belongings are strict.

Personal items that are prohibited from being brought in

- Information devices with recording functions such as PCs, mobile phones, smartphones, tablets, smart watches, USB memory, memory cards, portable audio players, cameras, recording devices, etc.
- Paper such as notebooks, notepads, schedule books, etc.

※Excludes items that are permitted by the company to be used for business purposes.

Operation with or without lockers in the facility

Facilities where lockers are installed

Store items other than those permitted to be brought in in a locker and do not bring them into the business area.

Facilities without lockers

Check and comply with the rules regarding the storage of prohibited items and personal belongings at the business establishment.

⚠ CAUTION ⚠

In principle, items that can store and copy data cannot be brought into the business area.

Since the rules for prohibited items differ depending on the facility, please check in advance if you are unsure.1

Case Study ①

The fun drinking party turned into a big trouble

We held a drinking party to deepen communication in the workplace, where we had a great time talking about our daily work.

However, Mr. A, who drank too much on the day, fell asleep on the return train and lost the bag containing the rented security card.

In addition, a general person who was at the drinking party contacted the head office of the client company and received a complaint when he heard information that only the insiders of the business office could know.

Three months later, the business of the relevant office has ended.

⚠ What kind of problem is there?

● Talking about business outside the company

Since we and our client companies have a non-disclosure agreement, information leakage is a breach of confidentiality and may be a reason for termination of the contract.

● I lost my bag with my admission card / security card

When drinking alcohol, the possibility of troubles increases, so please drink alcohol in a modest manner as a member of society.。

In addition, the following damages are possible and may lead to serious troubles.

- Occurrence of destruction / theft due to illegal intrusion by "spoofing"
- Occurrence of secondary damage due to leakage of confidential information and personal information
- Loss of credit from client companies (insufficient management ability)

Under Business

Organize your desk

Basic Rule

- Keep things tidy and tidy on and around your desk.
- Work while organizing unnecessary documents so that documents are not mixed on the desk.
- Do not leave empty containers for garbage and drinks but clean them up frequently.
- When leaving the seat, the document being processed should be laid down on a desk or stored in a designated place such as a cabinet.
- Cables connected to the PC should be wired so that they will not be caught on the body and the PC will be knocked down or dropped.

⚠ CAUTION ⚠

- **If documents and unnecessary items are scattered on the desk, the risk of loss or mis-disposal increases, so always keep an environment in order.**
- **Some facilities do not allow you to bring in uncapped beverages. Follow the rules of the facility.**

Use of business PC

Basic Rule

● I do not use my business PC privately.

Banned cases

- Connect your personal mobile phone, smartphone, mobile audio, etc. to the USB port to charge.
- Connect headphones or earphones to watch audio / video data that is not related to business.

● Do not access or search for non-business-related information.

Banned cases

- Search yourself, your family, acquaintances, celebrities, etc. in the client company's database.
- Access data that is not relevant to your business

● Do not tamper with or erase data or leave false records.

● Do not install software that is not necessary for your business.

● When installing the software, use it if you can carefully check and comply with the license agreement.

● Do not leave PC vulnerabilities by updating Windows Update and software used in a timely manner.

⚠ CAUTION ⚠

● **Illegal copying or unauthorized use of software is a violation of the law and may require a large amount of compensation from the software manufacturer in addition to legal punishment.**

Management and use of login ID and password

Basic Rule

- Do not give or lend the login ID / password given to an individual to others. Also, do not use another person's ID.
- Do not write your login ID / password on a piece of paper and stick it on a conspicuous place (business terminal, desk, etc.).
- When you leave your seat, lock the screen of your PC screen even for a short time.

※Screen lock: Ctrl + Alt + Del / Windows + L keys

Basic rules for setting login password

- Set with 8 characters or more
- Includes 3 or more types of uppercase letters, lowercase letters, numbers, and symbols
- Change at least once every 3 months
- Simple things, things that are easy to guess from others (avoid serial numbers, your name, etc.).

※If the above setting is difficult due to the convenience of the system to be used, the setting should be as close as possible to this.

⚠ CAUTION ⚠

Manage the given ID so that it will not be used by others.

If used improperly, the person who used the ID may also be suspected.

Use of the Internet

Basic Rule

- It will be used within the scope of business purposes and will not be used privately.
- Do not access or use various services such as community sites, web mail, and Internet servers on the Internet for private purposes.
- Do not download non-business data or install software from the Internet.
- When secondary use of data on the Internet (articles, photos, videos, maps, illustrations, music, etc.), copyright is not infringed.
  - Check the terms of use and use within the specified conditions

⚠ CAUTION ⚠

- **Internet usage is constantly monitored with access records.**
  Use the Internet properly.
- **There is a risk of virus infection by using software and data on the Internet**
- **Infection with a virus can cause information leakage and system troubles.**
  Therefore, do not access sites or download data that are not related to your business.

Use of E-mail ①

Basic Rule

- Do not use for any purpose other than business purposes.
- Do not send data to private e-mail addresses, personal computers or mobile phones, or to destinations not related to business.
  - Email monitoring is operated by the department manager
- Do not give your business email address to anyone unrelated to your business.
- Data encryption, security passwords, etc. are set for attachments containing personal information and confidential information of client companies.
  - Do not write the password in the text of the email attached to the file but create a new email and tell the recipient.

Precautions for using Gmail

When composing an email, the email destination candidates are automatically displayed, but unrelated and unintended recipients are often displayed, and if you select them carelessly, you will have trouble sending emails incorrectly.

Problem

Currently, it is not possible to stop the automatic display of email destination candidates.

Measures

① Since the ones registered in "Contacts" are displayed as destination candidates, narrow down the registered contents of "Contacts" to the minimum necessary and delete the ones that are not used frequently.

② The initial setting of Gmail is that when you send an email to a destination that is not registered in "Contacts", the destination is automatically registered in "Contacts".

● When sending an email, reconfirm the following items before sending.

- Is the destination (internal / external) correct, and does it contain extra destinations?
- Is the content sent to the destination correct from other content?
- Is it correct in the attached file, or is it attached extra?

● Do not open multiple windows at once and edit outgoing mail, as it is very easy to make mistakes.
E-mail mis-sending troubles occur repeatedly due to the same cause.

⚠ CAUTION ⚠

● E-mail mis-sending will cause information leakage troubles, so be sure to check the address and contents before sending.

● In addition to the above, some organizations and business establishments are making efforts to prevent erroneous email transmission. Follow each set procedure / rule.

Use of e-mail ②

Attachment automatic encryption exemption rule

- You can send the file unencrypted by adding "[no-zip]" to the end of the subject, but it is best to avoid it as much as possible.
- However, the approval of the superior is required to use [no-zip] transmission.
  - Recognize that [no-zip] transmission is a very high-risk operation in which the contents of the attached file are transmitted to the other party as it is if the email is sent incorrectly.
  - We do not recommend the operation of sending with [no-zip] unless there is a serious reason such as the encrypted zip file cannot be used at the destination.
  - Even if you are concerned that it will take time and effort at the destination, first explain and persuade the risk of information leakage and the magnitude of the impact when sending incorrectly. As a result, the worst situation can be avoided for both the other party and our company.

Rule

- Use [no-zip] after obtaining the approval of your superior before sending.
- If it is difficult to obtain the prior approval of the superior for all cases in consideration of 24-hour operation and the response when the superior is absent, in what case in advance according to the actual situation of the work [Please discuss with your superior whether to use [no-zip] and obtain approval (please obtain approval again when your superior changes).

Use of e-mail ③

Recommended rules when using the mailing list

- When creating ML with us
  - The ML name must meet the following conditions
    - Being able to clearly distinguish between internal use and external use (including external destinations)
    - When using a project, the "client company name" and "project name" can be easily identified.
  - Two ML managers select those who can perform management work
    - If there is a person who has retired or has been transferred, promptly delete it from the ML distribution destination.
    - If the ML delivery destination changes (addition / deletion), the ML delivery destination will be shared with those registered in the ML.
      (To keep track of who ML users will be delivered to).
  - If you stop using ML due to the end of a project, you need to take prompt measures so that it will not be delivered even if the user sends it by mistake.
    - When there is no prospect of ML reuse
      ➔ Delete ML
    - When there is a possibility of ML reuse
      ➔ Delete all ML delivery destination registrants and empty

- When using ML created by another company
  - Be especially careful when checking before delivery, as it will have a large effect when an email is sent incorrectly.
  - If possible, it is also necessary to inquire about the delivery destination and confirm that the senior officers of the other party are not included.
    (Whether or not there are delivery destinations that require attention).

- When registering both ML created by our company and ML created by other companies in the contact information, use a notation name that is easy to identify.
  - "Internal use" and "external use" can be easily distinguished
  - "Client company name" and "project name" can be easily identified

- When sending business report materials etc. as a file attachment using external use ML for clients
  - The naming rule for attachments is defined as follows
    - Enter the "client company name" and "project name" so that the first part of the name matches the notation name of the ML registered in the contact.
  - At the time of confirmation before sending, confirm that the name of the destination and the name of the attached file match.
    - Check judgment method is simple and confirmation accuracy is improved
    - You can check the destination and attached files at the same time
      - If the names don't match, it's often wrong to set either the destination or the attachment.

Use of commercial equipment

Basic Rule

- Lock the screen if you leave your seat while using your PC (To prevent unauthorized PC operation and prevent others from seeing confidential information).
- Do not use commercial equipment such as telephones, fax machines, printers, and copiers for private use.
- If you want to put it on hold while you are on the phone, set it to "Hold" so that you cannot hear this conversation while it is on hold.
- When using a printer or copier, collect printed matter promptly.
- Remove the faxed paper immediately.
- When sending a fax, reconfirm that the documents and destinations (fax number, speed dial, etc.) to be sent are correct immediately before sending.

⚠ CAUTION ⚠

Information transfer

Basic Rule

- When personal information or confidential information is exchanged with a client company, it is exchanged by a method agreed in advance by both parties.
- When personal information is delivered, a record of receipt / delivery is kept.
- For data containing confidential information, take measures against information leakage such as data encryption and security password setting.
- When sending documents or data containing confidential information, use registered mail or home delivery, etc., and send it by a method that keeps a delivery record.
- When carrying confidential information, in principle, go straight to the destination.
- When using the online storage service, obtain approval from the "online service usage application" before using it (see page 28).
- Information obtained from outside the company should be used after confirming that it is not infected with malicious programs.
- We will release the software created by us after confirming that it is not infected with malicious programs.

⚠ CAUTION ⚠

When confidential information is exchanged with a client company or an external company,

Disposal/return of information

Basic Rule

- Documents and memos containing personal information and business information should not be discarded as general garbage but should be disposed of according to the rules set by the business establishment.

Actions

- Shredder
- Put in confidential document collection box

- Do not use the paper with personal information / business information as the backing paper.
- In case of transfer or retirement, all lent items will be returned.

⚠ CAUTION ⚠

Even if the memo records the response of the client company and the contents of the meeting, if personal information and business contents are described, there is a risk of information leakage trouble, so do not mix it with general garbage and throw it away.

Taking out business information

Basic Rule

- Personal information / business information and information devices (notebook PCs, storage media, etc.) should not be taken out of the business area.

  ※Business manuals, training materials, notebooks with information related to business, memos, etc. are also applicable.

- If it is unavoidable to take it out of the work area due to the necessity of work, obtain the permission of the superior in advance.
- Observe the following when carrying documents and data including business information and notebook PCs.

Actions

- Do not browse in public places (restaurants, transportation, etc.)
- Do not let go in vehicles such as trains, buses, and taxis

  (Do not place on a rack, floor, or next sheet).
- Do not leave in a parked car
- Don't drink on the way home
- Turn off your laptop

⚠ CAUTION ⚠

- **Taking out information without permission is a serious violation of the rules and is subject to disciplinary action. Be sure to get the approval of your superior.**
- **If you take confidential information outside the company, be aware that the risk of**

Use of online services ①

Basic Rule

- Online services refer to all systems that are accessed via external networks, including the Internet (including Webmail not provided by the company).
- In principle, the use of online services is prohibited by company-wide rules, but if you have no choice but to use online services due to business reasons, you will be permitted to use them after approval by prior application.
- Online services are classified into the following three types and are based on the use of TCI-designated services.
  - TCI Designated Services (with pre-confirmed security specifications and a proven track record of use)
  - TCI Specially Designated Services (among TCI designated services, many have been used)
  - Client-designated Services (online services specified by the client company)
  - Undesignated Services (online services that do not fall under the above categories)
    - When the business requirements are not met by the TCI designated service and the requirements are met by using other services
- When using online services not designated by TCI
  - The use of online services involves the risk of information leakage, but when applying for the use of services not designated by TCI, the application / user department evaluates the risk of information leakage and designs the operation to ensure the risk before operation. It means that it has declared that it will operate as designed without the risk of information leakage.
  - If you cannot operate properly according to the operation design due to the system or other reasons, you should not apply for use.

Use of online service ②

Online service risk assessment perspective

Online service provider

- How is the creditworthiness of the service provider itself?
  - Domestic / overseas companies, servers are domestic / overseas
  - Management scale, years after establishment, capital affiliate / parent company
  - Is there a risk of bankruptcy (risk of information leakage after bankruptcy)?
- How is the performance and quality of the services provided?
  - How many years and how many services have been provided
- Are information security measures and security operation measures taken?
  - Are you prepared for an external attack?
  - How about measures against information leakage for insiders and operational quality?
- Did you confirm the terms of service?
  - Are there any concerns about information leaks, failures, cancellations, etc.
- About saved data
  - Whether the data is surely erased at the time of cancellation or does not remain on the backup medium (risk of information leakage after cancellation).

Service usage environment

- Is it possible to specify a global IP address or limit the usage environment with the terminal used?

  (Can unspecified access be blocked).
- Is it possible to encrypt data communication on the Internet line?

  (Do not be intercepted during communication).

User authentication

- Is it possible to perform authentication that is difficult to be spoofed by a third party?
  - Password policy (character type, number of characters, reuse)
  - Password change policy (first time, period)
  - Two-step verification

Service usage permission settings

- Is it possible to reduce the risk by preventing users from using unnecessary functions or functions that may be abused?
  - Is it possible to narrow down to only the necessary functions by setting the user's authority?
  - Is it possible to set a small group when sharing information between users?

Service operation management

- Is it possible to minimize the impact of problem events, such as being able to accurately grasp the unauthorized use of users and conducting detailed investigations when problem events occur?
  - Is there a function to notify the administrator when the user exceeds the specified number of times, capacity, period, time, etc. or when the service provision is abnormal?
  - Account lock (exceeded authentication failure, expiration date)
  - User's service usage history (how detailed it can be recorded, information retention period).
  - Is there a function to report usage status at regular intervals (monthly)?
  - Is it possible to extract unused users for a certain period of time?

Toward the introduction and operation of online services

- After conducting a risk assessment of the candidate online service, necessary risk countermeasures will be considered and operation design will be performed, but if the load on the operation staff increases, the operation risk will also increase, so introduction is recommended. I will not.
- Since online services are operated side by side with risks, it is important to be able to continue operations that avoid risks appropriately by designing operations that combine both online services and operations by operation personnel.
- It is necessary to design the operation, evaluate the actual operation, and then consider whether or not to introduce the online service.

Trouble Report

Basic Rule

● In the event of a trouble or accident, or if you discover a situation that may lead to trouble, immediately report it to your superior.

Examples to report

- Trouble related to information security
  - Incorrect transmission of information, information leakage, loss / loss / damage of information, etc.
- Business trouble
  - Work mistake
  - Complaints from client companies or consumers
  - System failure
  - Lost or damaged loan from client company
- Trouble related to compliance
  - Unauthorized use of information, falsification of data, violation of laws and regulations, etc.

※ **In addition to the above, if an event of concern occurs, we will promptly report it.**

Case Study ②

Mr. B who was very busy that day

Mr. B, who is involved in the ordering business, sends the order data of the day to the mailing list of the client company by e-mail every day. Before sending order data by e-mail, it was a rule to always confirm the address and attached contents at the fingertips.

However, I was very busy from the morning on that day, and due to my daily routine, I neglected to confirm before sending and sent it to a mailing list that had nothing to do with it.

⚠ What's the problem?

● Incorrect transmission of wrong address will result in information leakage

Incorrect transmission by e-mail or fax will immediately result in information leakage, and if personal information is included, information will be collected from the incorrect destination, response to the person who was the target of the information leakage, apology to the client company, and outside the company. Many man-hours such as notification will be required.

You may also be liable for damages.

● Violate the rules

To prevent business mistakes, business establishments prepare work procedure manuals and information handling rules. Performing work that ignores the rules set due to daily habituation and busy work increases the risk of work mistakes, information leaks, information loss, and inaccurate information recording.

Before leaving the facility

Behavior before leaving the company

Basic Rule

- Documents and equipment should be stored and stored in the designated place.
  - At business establishments that collect documents and memos in the process of processing, submit them according to a set procedure without individual management.
- When leaving the office, turn off the power of the business terminal and display.
  - Unless there is a method specified separately at the business establishment
- The notebook PC should be stored in a drawer or cabinet and locked.
- Clean up the area around your seat on the desk, check if personal information / business information (printed matter, etc.) remains, and if so, store it in a drawer or cabinet and lock it.

⚠ CAUTION ⚠

- **Since employees in other areas and outside contractors may enter at night, manage personal information and business information so that they cannot be accessed in unmanned business areas.**

When you leave the facility

Basic Rule

● Do not talk about business content outside the business area.。

  ➤ Including elevators and break rooms in the facility

● Do not have business conversations with others on the way to work or after returning home.

● Do not write on the Internet community site *, etc. so that you can guess the business content or business content.

※SNS, blogs, bulletin boards, chats, etc.

！ CAUTION ！

Conversations related to business outside the business area may lead to information leakage in unexpected places.

Be especially careful in places where you can relax easily.

Employees of client companies may be stationed in our center and use break rooms and shared spaces, so be careful about conversations and actions.

Case Study ③

Information disclosure that should have been done in good faith

Mr. D, who is involved in the support business of a home appliance maker, saw a user's complaint about the product he supports on the Internet community site and said, "It is improved with the new product that will be announced soon." I wrote a comment and recommended the purchase of a new product.

The site was on fire among users who saw this information, and manufacturers were repeatedly requested to replace it with new products.

⚠ What kind of problem is there?

● Corresponds to information leakage

Private information obtained during business should not be posted on the Internet community site. Of course, talking to people who are not related to work, such as family members and close acquaintances, is also prohibited.

● There is a risk of information spreading on the Internet

Currently, various information can be easily transmitted on the Internet community site.

Information transmitted on Internet community sites spreads all over the world in a blink of an eye and is almost impossible to undo.

● There is a risk of claiming damages

If the client company suffers damage due to postponement of product launch or impact on stock price, we may be required to compensate for the damage. The amount is very high and can be a threat to business management.

Case Study ④

Mr. A who works hard at home

Mr. A, who is enthusiastic about his work, brings his USB memory to the workplace to improve his business knowledge, copies the business materials on the network, takes them home, and studies well on his home computer.

Mr. A has a good track record and was a reliable person.

⚠ What's the problem?

● Corresponds to information leakage

Taking out information / data in the business area without permission is an information leak and may be a big problem depending on the content of the data.

● Corresponds to a rule violation

It corresponds to a rule violation such as bringing personal information equipment into the business area, taking out information without permission, and storing data in personal information equipment. The act of taking out business data without permission is subject to punishment under internal rules, and the parties may end their business immediately at the workplace of the client company.

● There is a risk of secondary information leakage

If information is leaked due to the loss of the USB memory, or if your home computer is infected with a virus, business data may spread on the Internet.

Work Remotely

Information Leakage Risk

Basic Rule

- Working from home requires proper security measures and awareness because the security level is lower and the risk of information leakage is higher than in the offices of companies that are controlled to enter and leave the room.
- Do not show PC screens during work or paper materials for work to family members or acquaintances.
- Do not talk when asked about business content or client company information.
- If you are using paper materials at home, store them in a company bag so that they cannot be seen by your family or acquaintances when you leave your desk.
- Do not use your personal computer or information equipment to do business

If a family member or acquaintance posts unpublished information of a client company on SNS or talks to a third party and leaks the information, it may lead to serious trouble. Be careful not to get your family and acquaintances into trouble.

⚠ CAUTION ⚠

Even when working from home, if business documents and unnecessary items are scattered on the work desk, the risk of loss or mis-disposal increases due to mixing with personal belongings, so always maintain an organized environment.

Cyber Security Risk

Basic Rule

- Cyber security risks in the Internet environment are the same at work and at home. The network in the company is managed by the Management Information Infrastructure Department, etc., but at home you have to maintain and manage the network security environment yourself.
- Here, the minimum contents that must be dealt with are described.
- Windows Update for business PCs and software updates will be carried out in a timely manner.
- Security measures when using Wi-Fi
  - When connecting to Wi-Fi, use the security protection of WPA2 to connect.
    (Please note that old Wi-Fi routers may relate to the dangerous old standards "WEP" and "WPA".)
  - Wi-Fi routers also need to be vulnerable, so update the firmware to the latest version before using it.
  - Do not use free Wi-Fi.

  (In principle, using a PC outside of work or home is prohibited)

⚠ CAUTION ⚠

If you are using an old standard Wi-Fi router, replace it with a new Wi-Fi router, or connect to your PC with a LAN cable (wired) instead

Labor Issues

Basic Rule

Management of business hours

- When working from home, work and private use tend to coexist, and long working hours and overtime work may occur. Therefore, work and private use should be consciously separated.
- Overtime work is done with the approval of the superior in accordance with the rules within the department.

Communication challenges

- When working from home, it is not possible to have face-to-face or extension telephone conversations, which may cause various communication-related issues.
- In many cases, it is a problem that includes business people, superiors, other departments and customers, and it is difficult for individuals to solve these problems.
- Start by organizing the issues, consult with business people, superiors, and colleagues, share the issues, and do not hold them alone.

Stress challenges

- Prolonged work from home may cause various stresses such as work-related issues, changes in life rhythm, work environment, family issues, and anxiety about the future.
- These stresses are felt by many people, not just you, and it is difficult to improve even if you have them alone, and you may be able to reduce the stress by talking to someone. We encourage you to talk to your colleagues, superiors, family, and acquaintances.

Remote harassment (telework harassment)

- Remote harassment has become a problem due to the increase in telecommuting, so please be aware of the following.
  - Harassment and bullying such as entering an individual's private area more than necessary, making negative or intimidating words and actions, and sexually saying and acting, triggered by camera images and sound from a microphone at a web

conference, etc.

  - Force constant connection to web conferencing for behavior monitoring only
  - Extortion such as online drinking party

- If remote harassment occurs, find someone who can speak and consult with them, or consult with a company-wide consultation desk.

● Efforts for mutual assistance

- In an environment where people tend to work from home, which tends to be lonely, how the organization or team works on mutual assistance, especially when dealing with business issues, communication, stress, mental issues, etc., results in productivity and service quality. Is thought to affect.
- Each person is required to consciously work on mutual aid.

※What is mutual aid:

By helping each other in the community around us, we try to solve each other's problems.