Guidelines for the Prevention of Internal Improproprieties in Organizations

March 25, 2013
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
# Table of Contents

1. Background .......................................................................................................................... 2

2. Overview .................................................................................................................................. 4

   2-1. Composition of and Ways to Use these Guidelines ..................................................... 4

   2-2. The Importance of Constructing Systems for Internal Impropriety Countermeasures ................................................................................................. 5

   2-3. Systems for Internal Impropriety Countermeasures ..................................................... 6

3. Definition of Terms, and Related Laws ............................................................................. 8

   3-1. Terms .............................................................................................................................. 8

   3-2. Related Laws ................................................................................................................ 9

4. Model Management for Internal Improprieties ................................................................. 12

   4-1. Basic Policies (Responsibilities of the Top Manager and Governance) ................. 14

   4-2. Asset Management (Designation as Confidential, Designation of Access Privileges, Access Administration, etc.) ................................................................. 18

   4-3. Physical Management .................................................................................................... 26

   4-4. Technological and operational management .............................................................. 31

   4-5. Securing Evidence ......................................................................................................... 36

   4-6. Human Management .................................................................................................... 39

   4-7. Compliance ................................................................................................................... 42

   4-8. Workplace Environments ............................................................................................. 44

   4-9. Follow-up measures ..................................................................................................... 47

   4-10. Organizational management ..................................................................................... 49

Appendix I: Internal Impropriety Case Studies ................................................................. 51

Appendix II: Internal Impropriety Check Sheet ................................................................. 55

Appendix III: Q&A ................................................................................................................ 61

Appendix IV: Relationship with Other Guidelines, etc...................................................... 65

Appendix V: Examples of Basic Policies ............................................................................. 72
1. Background

Recently, information security incidents involving internal improprieties that threaten the very business of companies or other organizations have drawn attention. Typical examples include cases of employees or officers improperly selling customer data, resulting in large-scale leakages of personal information, and cases of employees improperly removing product information from a company when retiring resulting in the leakage of technical information. In addition to these there are cases involving employees who, acting without malice, take information home from the company without authorization in order to work at home, and then unintentionally leak the information from a home PC. Such information security incidents involving internal improprieties occur without fail every year which is being widely reported.

According to surveys by Japan Network Security Association (JNSA) which is a specified nonprofit corporation, one feature of incidents involving internal improprieties is that from 2005 to 2010 the number of incidents occurring due to internal crime or acts of internal impropriety made up only 1% of all the incidents involving leakage of personal data, but about 25% (a quarter) of all personal information leakages were the result of internal impropriety. As such, with the damage per incident greater than that from external attack, each occurrence inflicts a major impact on a business. Moreover, according to surveys by the Ministry of Economy, Trade and Industry, the vectors for leakage in companies experiencing leakage of trade secrets were reported as "leakage caused by departing (full-time) employees (50.3%)," "leakage caused by mistakes by active employees, etc. (26.9%)," and "leakage caused by current employees for motives of financial gain, etc. (10.9%)." As seen by this, leakages of trade information with value in maintaining competitiveness are almost entirely due to inside parties. For this reason, internal improprieties are viewed as one of the threats that organizations face, and must be addressed wholeheartedly by the top manager and management teams as a key management issue.

Incidents concerning internal improprieties tend to be handled within the organization for reasons including concerns over negative publicity or lack of coordination among parties concerned, and rarely become known outside the organization. As such, it is likely that in addition to those incidents that are disclosed in the media or in courts, there are also many incidents that are not brought to courts or which remain undisclosed cases of internal rule infractions. As sharing of information about internal improprieties among organizations is thus difficult, the status of such incidents in society is not well known, and it is difficult to consider the causes of and effective countermeasures for internal improprieties beyond the boundaries of the organization. As such consideration is not performed beyond the boundaries of the organization, at present each organization enacts countermeasures based on its own experiences. Moreover, interview surveys by the Information-technology Promotion Agency, Japan (hereafter "IPA") have revealed companies in which incidents have occurred for the reason that such risks were underestimated and no measure was enacted. Underestimation by companies like this is due to the lack of sharing of information about internal improprieties and awareness of such threats. In fact, believing that "internal improprieties won't happen in our company" or "our employees wouldn't commit improper actions," these companies have underestimated their risks. As such, when

---

1 "Survey Results on Information Security Incidents – Personal Information Leaks," JNSA
2 "Questionnaire Survey Concerning the State of Management of Trade Secrets," Survey Results (Definitive Version), Ministry of Economy, Trade and Industry
3 Report on Survey of Incidents Due to Improper Activity by Organization Insiders
countermeasures are considered and decided strictly within organizations, those organizations may fail to realize the need for countermeasures in the first place.

In the absence of internal impropriety countermeasures, the organization may fail to prevent incidents. Furthermore, incidents may go unnoticed until the damage spreads to the parties involved, while the inability to resolve incidents due to uncertainty over their causes can prove a hindrance to follow-up measures. Moreover, even if the perpetrators of the improper actions can be identified, there may be cases in which duty of care has been lax, rendering disciplinary action invalid or making prosecution difficult.

In order to help organizations prevent internal improprieties, IPA created "Guidelines for the Prevention of Internal Improprieties in Organizations" (hereafter "these Guidelines") and made it available to the public. The content of these Guidelines enables the preparation of effective internal impropriety countermeasures in companies (especially small- and medium-sized businesses) that have not yet thought about, or have not known how to address, internal impropriety countermeasures.
2. Overview

The chief aim of these Guidelines is the prevention of internal improprieties in organizations. Taking into account the actual occurrence of internal improprieties, these Guidelines also address early detection and prevention of the spread of damage following occurrences.

The targets for protection from internal improprieties are the information systems and information managed by organizations, for information recording media other than paper. However, the action of printing out information from information systems onto paper is also covered by these Guidelines.

2-1. Composition of and Ways to Use these Guidelines

These Guidelines are composed as described below, with a broad division into two parts: "Section 1: Background" and "Section 2: Overview" as the first half, and "Section 3: Definition of Terms, and Related Laws" and "Section 4: Model Management for Internal Improprieties" as the second half.

<table>
<thead>
<tr>
<th>Table 1 Composition and Assumed Readership of these Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Composition of these Guidelines</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Section 1: Background</td>
</tr>
<tr>
<td>Section 2: Overview</td>
</tr>
<tr>
<td>Section 3: Definition of Terms, and Related Laws</td>
</tr>
<tr>
<td>Section 4: Model Management for Internal Improprieties</td>
</tr>
<tr>
<td>Appendix I: Internal Impropriety Case Studies</td>
</tr>
<tr>
<td>Appendix II: Internal Impropriety Check Sheet</td>
</tr>
<tr>
<td>Appendix III: Q&amp;A</td>
</tr>
<tr>
<td>Appendix IV: Relationship with Other Guidelines, etc.</td>
</tr>
<tr>
<td>Appendix V: Examples of Basic Policies</td>
</tr>
</tbody>
</table>

*1: See "4-1. Basic Policies"

See Figure 1 regarding (1)-(4).

Section 1 and Section 2 show the positioning and the way of using these Guidelines, and is content aimed at all readers.

These sections assume persons implementing countermeasures and the top manager (or management team)*4 to be readers, and discuss the importance of preventing internal improprieties, as well as an overview and the usage of these Guidelines. As for threats posed by internal improprieties, see "Appendix I: Internal Impropriety Case Studies", and you will better understand the importance of countermeasures.

Section 4 offers content for the formulation of specific countermeasures by persons implementing countermeasures, who are charged with countermeasures by the top manager.

---

*4 Top manager differs by company scale, management policies, and company form; in these Guidelines, the term indicates the main director of the company.
manager (or management team). However, the top manager will also need to look over "Section 4, 4-1. Basic Policies" in order to understand his or her role in the organization. Persons charged with countermeasures should first assess the status of their organization's internal impropriety countermeasures by using the check sheet in Appendix II. To address items for which countermeasures are insufficient according to the results of the check sheet, consider specific countermeasures with reference to "4. Model Management for Internal Improprieties" and "Appendix III: Q&A." Figure 1 shows how to use these Guidelines depending on what to consider.

![Figure 1: How to use these Guidelines depending on what to consider](image)

2-2. The Importance of Constructing Systems for Internal Impropriety Countermeasures

In order to make use of these Guidelines to effectively and efficiently prevent internal improprieties, the top manager (or management team) must bear responsibility inside and outside the organization for internal impropriety countermeasures, and must be actively involved in promoting these. The involvement of top managers plays an important role in improving awareness concerning internal impropriety countermeasures in the organization, and in disseminating implementation measures.

In addition, organization-wide action is vital in the formulation and dissemination of specific implementation measures. As the content of internal impropriety prevention countermeasures extends to the work of multiple parties (or divisions) concerned, there must be cooperation with these parties concerned in the formulation of implementation measures. Given that the organization will formulate implementation measures concerning the protection of information assets, it can be assumed that persons/divisions in charge of information systems, office work, and personnel will be involved. As an example, when changes are made to work processes that handle information system, the information systems division or the division in charge carries out the task, while the division or persons in charge of
personnel provide education on the changes. In addition, check by the legal affairs division as to legal matters might also be necessary. In this way, in dissemination, education, etc. concerning implementation measures, organizations must communicate directions organization-wide so as to avoid oversight of countermeasures, and must create systems enabling the summarization of implementation status and assessment by the top manager.

2-3. Systems for Internal Impropriety Countermeasures

As mentioned in Section 2-2, systems for internal impropriety countermeasures involve various divisions within an organization, and the roles of “CEO” and “Supervising Manager” who supervise and mediate those divisions become important.

Internal impropriety countermeasures are closely related to the internal controls required by the Companies Act and the Financial Instruments and Exchange Act in terms of risk management and there are some overlaps between them in terms of systems. Hence, by using a framework of existing internal controls, organizations can effectively and efficiently construct internal impropriety countermeasures.

The below explains how to construct internal impropriety countermeasures based on an internal control framework.

Explanations are given from the viewpoint of the roles of “CEO”, “Supervising Manager” and “Divisions/persons in charge”.

2-3-1. CEO

In internal impropriety countermeasures, as in internal controls, organizations must establish the role of the CEO. Budgetary and personnel authority is necessary for internal impropriety countermeasures, as is the one who takes responsibility for implementing that authority. In these Guidelines, that role is given to the CEO. The CEO formulates basic policies for internal impropriety countermeasures, and determines these by resolution of the Board of Directors. In addition, the CEO understands the management of the company, and appoints a Supervising Manager whose role is to implement and promote specific measures.

2-3-2. Supervising Manager

Organizations shall establish a role for specifically promoting internal impropriety countermeasures. In these Guidelines, that role is given to the Supervising Manager. The Supervising Manager bears the role of mediating between business divisions and the top manager while also implementing and checking specific countermeasures for the whole organization. This mediator role is also given to an internal control committee, and so on in internal control. So, when an internal control committee, and so on exist within an organization, it may be advisable for a member of these to concurrently serve as the Supervising Manager to reduce the workload of constructing systems.

2-3-3. Appointment of the Supervising Manager

It is not necessary for all companies or organizations to establish an internal control committee and so on for the purpose of internal impropriety countermeasures. In the case of small-scale companies, systems relating to internal control are often insufficient, with no

---

5 Under the Companies Act, important rules concerning the construction of internal control systems and basic policies of systems, etc. are matters for deliberation by the Board of Directors (Companies Act, Article 348, item 3.iv; Article 362, item 4.vi; Article 416, item 1.i.e). Note that in these Guidelines, when no Board of Directors exists in a company, the explanation applies to matters decided by Director(s).

internal control committee and so on in place. Even in such a case, it is possible to prepare systems for internal impropriety countermeasures by newly appointing a Supervising Manager responsible for internal impropriety countermeasures.

Depending upon the scale and form of the company, the CISO\(^7\) or the top manager (CEO) may double as Supervising Manager. As an example, when the scale of a company is relatively small, the top manager has more of an organization-wide view than is possible in a large-scale company. As a result, the top manager can enact fast and effective countermeasures by directly undertaking internal impropriety countermeasures. In such a case, it may be possible for the top manager to concurrently serve as CEO and Supervising Manager, as well as to construct and prepare the systems. For details, see Q&A1:P62 and Appendix V: Examples of Basic Policies.

2-3-4. Systems for Participation and Cooperation by Related Divisions and Persons in Charge

The internal impropriety countermeasure initiatives addressed in these Guidelines are, within internal control, particularly concerned with overall internal control pertaining to IT. However, this does not mean that only information systems divisions with expert IT knowledge should participate. Internal impropriety countermeasures call for comprehensive countermeasures that involve multiple divisions – for example, preparation of workplace environments by the general affairs division, education and preparation of various internal rules by the personnel division. As such, active participation and cooperation by diverse divisions and persons in charge are necessary. Moreover, when the scale of these divisions is large, the responsible managers of the divisions noted below are also required to participate.

\(^7\) CISO, or Chief Information Security Officer, is appointed by management as the highest person responsible for information security, and bears responsibility for the overall information security of the company or organization. This document explains such a role in terms of the CISO.
3. Definition of Terms, and Related Laws

The definition of terms used in these Guidelines and an overview of related laws is described below.

3-1. Terms

(1) Organization
A corporation such as a company or a local government, or any other such body.

(2) Insiders
Any persons corresponding to officers, employees, contract employees, etc. (hereafter "officers and employees"), or ex-officers or ex-employees who fulfill either of the following:
- Persons having privileges to access the organization's information systems or information (e.g., networks, systems, or data), either directly or over a network
- Persons engaged in work that may allow physical access (excepting janitorial staff, security staff, etc.)

(3) Internal improprieties
Internal improprieties include not only illegal activities but also improper activities such as violations of internal rules concerning information security, which cannot be regarded as violations of laws. Acts of internal impropriety shall include the theft, removal from premises, leakage, deletion, sabotage, etc. of important information (customer lists, technical knowledge, etc.) or information assets (information systems, etc.). Actions by which insiders retired from organizations leak information that was gained while working in the organizations shall also be handled as internal improprieties.

(4) Systems for internal impropriety countermeasures
These are systems for the construction of internal impropriety countermeasures or for the consideration, review, etc. of specific measures. They include systems as shown earlier in Figure 2, and the roles shown below.

- CEO: The top manager who bears highest responsibility for decision-making concerning internal impropriety countermeasures, in accordance with laws and regulations such as the Companies Act, and in accordance with deliberation by the Board of Directors.
- Supervising Manager: The manager supervising the systems for internal impropriety countermeasures, appointed by the top manager in accordance with laws and regulations such as the Companies Act. The Supervising Manager creates, manages, and implements specific countermeasures across the organization based on the top manager's basic policies, and checks and reviews the status of countermeasures.
- Responsible manager of division: A person from a division appointed as the person responsible for that division. Under the direction of the Supervising Manager, responsible managers of divisions implement countermeasures in their divisions, and check and review the status of countermeasures.
3-2. Related Laws

An overview of laws related to these Guidelines is provided below. In order to comprehensively consider and take measures with respect to the related laws, etc. listed here, organizations must conduct said considerations together with persons in charge of the legal affairs division, as well as the personnel and general affairs divisions.

(1) **Act on the Protection of Personal Information**

This Act stipulates the obligations (safety management mechanisms, obligations to monitor employees and contractors, etc.) with which businesses that handle personal information must comply, in order to protect the rights and interests of individuals from the leakage or improper use of personal information. When a business violates this stipulation regarding obligations and handles personal information inappropriately, the competent minister having jurisdiction over the business may take measures including issuing suggestions and directions to the business. Failure to follow the directions may subject the business to penalties.
When important information must be protected as personal information

When organizations have the objective of protecting managed personal information from internal improprieties, they must comply with the rules for obligations concerning safety management mechanisms required by the Act on the Protection of Personal Information. For details, refer to the Personal Information Protection Guidelines for economic and industrial sectors (Article 2 of the Act; Articles 20-22; etc.).

(2) Unfair Competition Prevention Act

The Unfair Competition Prevention Act sets forth rules concerning the protection of trade secrets. With respect to the improper use or disclosure of trade secrets, it recognizes civil injunctions and applies criminal penalties in the case of highly illegal infringing conduct. However, in order to be recognized as a trade secret, information must be managed as confidential, and must be useful and not publicly known.

As these Guidelines show methods for handling important information, including trade secrets, they contain information beneficial for the protection of trade secrets.
When important information must be protected as trade secrets

When organizations have the objective of protecting expertise and other trade secrets from internal improprieties, they should refer to items including the "Directives for Management of Trade Secrets" presented on the website of the Ministry of Economy, Trade and Industry. Reference Material 1 of the "Directives for Management of Trade Secrets" offers the Trade Secret Management Check Sheet as a corporate self-diagnostic tool for fulfilling the manageability of confidentiality, one of the requirements for trade secrets. Its use enables assessment of the status of trade secret management within organizations.

(3) Labor Contract Act
This Act involves cases in which an employee commits internal improprieties such as leakage of information during the term of employment and, by violating the labor contract, is subject to dismissal, disciplinary action, claims for damages, etc. However, the efficacy of dismissal or other specific disciplinary action is to be determined based on the determination framework under labor laws. Moreover, in the event of damages to the company due to internal improprieties by an employee, said employee shall be subject to claims for damages based on default or improper activity under the labor contract.

(4) Act for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers
Although employees bear confidentiality obligations as part of their obligations under labor contracts, there is no labor contract between dispatched workers and the companies that temporarily hire them. As the hiring companies cannot directly place confidentiality obligations upon the dispatched workers, in order to have temporary workers maintain confidentiality, the companies must take into account the Act for Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers.

(5) Others
In addition to the above, legislation concerning improper activity by insiders includes the Penal Code (e.g., larceny, embezzlement, breach of trust, etc.), the Civil Code (contractual liability, tort liability, etc.), labor jurisprudence (violation of confidentiality obligations, non-competition obligations, etc.), and the Whistleblower Protection Act.
4. Model Management for Internal Impropriety countermeasures

This Section comprehensively presents countermeasures required from the following 10 standpoints in order to enact specific internal impropriety countermeasures within organizations.

4-1. Basic Policies
4-2. Asset Management
4-3. Physical Management
4-4. Technological management
4-5. Securing Evidence
4-6. Human Management
4-7. Compliance
4-8. Workplace Environment
4-9. Follow-up Measures
4-10. Organizational Management

Based on these 10 standpoints, 30 countermeasures are presented. However, as these are shown for hypothetical multiple internal improprieties, enacting all of the countermeasures may involve more countermeasures than is necessary when only a specific internal impropriety is targeted.

Following this, the flow of considerations based on the 30 countermeasure items is explained. In considering countermeasures, organizations must consider whether risks (i.e., impacts on business) can be allowed. As an example, if a given risk is allowed, it may not be necessary to enact all of the countermeasure items related to that risk. However, taking into account follow-up legal proceedings after an incident of internal improprieties, it would not be advisable to allow the risks under "4-2. Asset Management," "4-8. Human Management," and "4-7. Compliance." These items are necessary in order to show that fault lies not with the organization but with the perpetrators of the internal improprieties.

As shown in Figure 3, the countermeasures for the 30 items are composed of the following 3 points:
- "Countermeasure principles": Necessary countermeasures are shown in a box. These are also check sheet items. Be sure to gain an overview of countermeasures.
- "What risks are there?": Shows the risks when the countermeasures shown in "Countermeasure principles" are not taken. Be sure to grasp the necessity of those countermeasures.
- "Countermeasure points": Provides clues to drafting specific implementation measures against the above-mentioned risks.

---

8 These Guidelines summarize "countermeasure principles" and present them in Appendix III as a check sheet used for checking the status of internal impropriety countermeasures.
Figure 3  Structural overview of countermeasures

Per the following, consider specific countermeasures while reading the text from "Countermeasure principles" to "Countermeasure points." As some items may involve multiple parties (or divisions) concerned, these parties must participate. For the parties (or divisions) concerned for each item, see "Appendix II: Internal Impropriety Check Sheet"

(1) Read "Countermeasure principles" to gain an overview of countermeasures.
(2) Read "What risks are there?" to understand the risks when the countermeasures shown in "Countermeasure principles" are not taken. Consider the effects on business when the information security incidents under these risks occur. If the effects on business are small and a risk is deemed allowable, it may not be necessary to enact countermeasures.
(3) Read "Countermeasure points," and, taking costs, resources, etc. into account, draft specific implementation measures based on the effects on business of (2). "Appendix III: Q&A" and "Appendix IV: Relationship with Other Guidelines" are attached as a supplement to "Countermeasure points." Draft specific implementation measures with reference to these Appendices.
In "Countermeasure points," countermeasures that use the term "advisable" in their text assume the case in which organizations wish to strengthen the countermeasures.

It is advisable to periodically review the specific implementation measures drafted in (3), as the allowable risks in (2) may change along with societal background and scale of the company. Moreover, as these Guidelines can be expected to undergo revision in step with developments in the social background and in IT, it would be effective to time the above reviews to revisions to these Guidelines.
4-1. Basic Policies (Responsibilities of the Top Manager and Governance)

In preventing internal improprieties in the organization, the involvement of the top manager in promoting effective countermeasures throughout the organization is of extreme importance. Formulation of basic policies and construction of systematic management systems through the leadership of the top manager are also necessary. The top manager must view internal impropriety countermeasures as a management issue. In that event, it is important to undertake considerations as a component of risk management, from the standpoint of the confidentiality\(^9\), integrity\(^{10}\), and availability\(^{11}\) of information assets.

With the top manager taking the lead, it is possible to thoroughly promote awareness of and initiatives toward internal impropriety countermeasures within the organization, by constructing and operating systems and mechanisms for internal impropriety countermeasures. In the end, an organization doing so will be able to strengthen protection of personal information and internal control, as well as respond to legal requests toward the company.

\(^9\) I.e., enabling the use of information only by persons approved to access the information (e.g., not leaking information).
\(^{10}\) I.e., ensuring that information and information processing methods are accurate, and that no changes are made by persons without privileges (e.g., ensuring that information is not falsified).
\(^{11}\) I.e., enabling access to information and information systems whenever necessary, for users authorized to access the information (e.g., ensuring that system failure does not occur, making information and information systems unusable).
15

(1) Clarification of the Responsibilities of the Top Manager

Internal impropriety countermeasures are the responsibility of the top manager, who must formulate basic policies for the purpose of showing fundamental directions within and outside the organization, and must disseminate these to officers and employees.

■ What risks are there?

If "basic policies" are not formulated through the leadership of the top manager, the locus of responsibility within and outside the company will be unclear, and preparation of an effective management structure will be difficult. Moreover, "basic policies" also serve to communicate the intentions of the top manager with respect to prevention of internal improprieties. When these are not formulated, the intentions of the top manager will not be communicated to officers and employees, and dissemination of international impropriety countermeasures will be difficult.

■ Countermeasure points

The top manager must formulate the basic policies that form the general framework for internal impropriety countermeasures, and must set the direction for internal impropriety countermeasures. In order to make the countermeasures more effective, the top manager periodically reviews basic policies while monitoring and evaluating the implementation status of countermeasures.

1. The top manager sets the direction for internal impropriety countermeasures, and bears responsibility for these within and outside the organization through involvement in monitoring and evaluation.
2. With reference to these Guidelines, the top manager formulates basic policies.
3. The top manager determines the important information that the organization should protect.
4. The top manager checks internal impropriety countermeasures against the formulated basic policies, and disseminates the countermeasures to officers and employees through education, etc.
5. Based on the results of monitoring and evaluation, the top manager periodically reviews the basic policies.
6. The top manager discriminates between important information and other information. Furthermore, it is advisable for the top manager to divide important information into several categories, taking into account their degree of importance to the business.
7. The top manager regularly reviews the division and categorization of important information, as these may change along with societal background, changes in the business, etc.

---

12 Continuously assessing situations through periodic reporting
(2) Appointment of the Supervising Manager and Construction of Cross-Organization Systems

1. The top manager appoints the Supervising Manager and approves management systems and implementation measures, showing the organization as a whole that these are top manager-led initiatives. 2. Following the basic principles, the Supervising Manager must construct cross-organizational management systems. Moreover, the Supervising Manager must formulate implementation measures.

However, if the organization is one in which the top manager has a view of the entire organization and implements internal impropriety countermeasures on his or her own, it may not be necessary to construct management systems.

■ What risks are there?

If the top manager does not appoint a Supervising Manager or give approval to the countermeasures to be implemented, it will be difficult to allocate the necessary budget and personnel, which in turn makes the construction of effective management systems difficult. As the important information targeted by internal improprieties exists in diverse divisions in the organization, if cross-organizational management systems are not constructed, the organization may be unable to enact effective and efficient countermeasures or information management, or to establish them thoroughly. That latter failure heightens the risk of internal improprieties occurring.

■ Countermeasure points

The top manager takes the lead in constructing and operating systems for establishing internal impropriety countermeasures in the organization. Specifically, the organization is to establish and operate the following countermeasures.

1. A person with understanding of information security and management is to be appointed as Supervising Manager in order to achieve efficient and effective internal impropriety countermeasures that take the business into account.

2. The Supervising Manager reifies and documents cross-organizational management systems and the roles of the related divisions and thoroughly establishes those roles. Responsible divisions, taking the lead with the Supervising Manager, construct organization-wide implementation measures and implementation systems for internal impropriety countermeasures. See Figure 4 for an overview of the important information and roles for the hypothetical related organizations.

3. In constructing cross-organizational management systems, the Supervising Manager appoints responsible managers or persons in charge for each division, who then serve as management and operational staff.
Figure 4  Overview of important information and roles for hypothetical related organizations
4-2. Asset Management (Designation as Confidential, Designation of Access Privileges, Access Administration, etc.)

See Figure 5 for an overview of the flow for information asset listing or other handling and considerations.

- • • Content concerning 4-1. (1) of these Guidelines
- • • Content concerning 4-1. (2) of these Guidelines
- • • Content concerning 4-2-1. (3) of these Guidelines
- • • Content concerning 4-2-1. (4) of these Guidelines
- • • Content concerning 4-2-2. (5), (6), (7) of these Guidelines

Figure 5  Flow diagram for information (important information) handling and considerations
4-2-1. Designation as Confidential

(3) Information rating categories

Organizations or the division in charge must assess important information, assign it rating categories according to degree of importance, and based on those categories, set the scope (e.g., position, job category, etc.) of insiders able to handle the information.

What risks are there?

If important information such as customer lists or technical knowledge is not separated from other information, officers and employees will not know which information is important information that must be protected, and may leak information without knowing that it is important. Moreover, if important information is not assigned rating categories and managed appropriately according to category, countermeasures may prove insufficient or too costly. Organizations or the division in charge that do not perform this management may be unable to pursue the liability of employees committing improprieties. Moreover, doubt may be cast onto the management responsibility of the company or organization.

Countermeasure points

Organizations or the division in charge must establish the following in order to assess and appropriately manage important information.

1. Organizations or the division in charge are to establish handling for important information. When three or more degrees of importance have been assigned in the rating categorization, organizations or the division in charge are to establish handling for each degree of importance. Organizations or the division in charge are to periodically review the handling established for important information.

2. Organizations or the division in charge are to establish administrators for important information. As an example, organizations can set responsible manager of divisions, or persons in charge selected from responsible managers of divisions, as administrators. Large organizations are to establish an administrator for each division.
The application and labeling of rating categories

1. In order to restrict the scope of handling important information, creators of important information must select one of the ratings categories established in (3), and must have the selection confirmed by the administrator for important information.
2. Furthermore, some sort of indicator, such as a confidentiality mark, must be set on digital documents or digital data containing important information, to let insiders identify important information.

What risks are there?

If organizations do not set ranking categories for important information, the scope of handling for the information will not be set, and even officers and employees having no need to handle such information will have access to it, and the possibility of leakage will increase as the important information becomes known to more officers and employees. As the number of officers and employees knowing of the important information increases, the environment for detecting internal improprieties will worsen, the likelihood of occurrence will grow, and the perpetrators of internal improprieties will become difficult to identify after occurrence.

If organizations do not set an administrator for important information (e.g., the responsible manager of the division, etc.), appropriate management of important information will not be thoroughly established, and important information may leak due to information assets in PCs, etc. being lost or taken from the premises without authorization.

Moreover, if labels are not shown based on degree of importance, officers and employees may take information from the premises or leak it without knowing it is important information.

Countermeasure points

Organizations are to restrict the scope of handling important information, and are to set and operate the items below to make handling of the important information understood.

1. The scope of handling of important information is to be restricted to officers and employees with work-related need. In order to reduce the danger of improper use of important information, organizations are to set the scope of handling based on position, duties, role, scope of responsibility, form of employment, and so on.
2. Creators of important information must select one of the ratings categories established in (3), and must have the selection confirmed by the administrator for important information. In the same way, important information already created and stored must be assigned ranking categories.
3. A confidentiality mark (such as graphic data or a stamp, or a watermark with text, indicating confidentiality) making rating categories known to officers and employees must be attached to digital documents containing important information. For digital documents containing important information, along with the above confidentiality mark, it is advisable to designate and display a period of validity for the important information. The period of validity is to be reviewed periodically. When the period of validity has expired, the information is to be subjected to the established handling such as disposal.

Some tools allow such specification through file properties.
4. When deleting important information from the storage media of their PCs or other information devices, officers and employees must select an erasing method based on the degree of importance of that information and then perform deletion\textsuperscript{14}.

\textsuperscript{14} When officers and employees are away from work involving extremely important information, the information should be completely deleted from the storage media of their PCs or other information devices. Complete deletion covers levels from OS-level formatting to random data overwriting.
4-2-2. Designation of access rights

(5) User access management in information systems

1. To enable access to important information by only those users specified by the scope of handling (e.g., position, job category, etc.) set in (4), information systems division must operate information systems with procedures established for registration, change, deletion, and other settings concerning user IDs and access rights. 2. User IDs and access rights that have become unnecessary due to transfer or retirement must be deleted promptly.

■ What risks are there?

If information systems division do not set user IDs and access rights appropriately in information systems, officers and employees not intended to have access rights to important information may be granted access, and important information may be used improperly. Conversely, officers and employees needing to access important information to perform their work may not be granted access.

If information systems division do not delete user IDs that have become unnecessary due to transfer or retirement, these may be improperly used by current- and ex-officers and employees to access important information.

Information systems division that does not perform this management may be unable to pursue the liability of current- and ex-officers and employees committing improprieties. Moreover, doubt may be cast onto the management responsibility of the company or organization.

■ Countermeasure points

Information systems division is to take the countermeasures below in order to correctly set user IDs and access rights in information systems.

1. Information systems division is to establish and operate procedures such as approval procedures for the registration, change, and deletion of user IDs and access rights, and notification of completion of settings.

2. Information systems division is to set access rights to important information for user IDs in information systems, based on the scope of handling established in (4). If access rights based on the scope of handling established in (4) are not set, this is to be remedied by review of (4) or functional changes to the information system.

3. It is advisable to perform operation in conjunction with personnel procedures, etc. concerning personnel relocation, in order to prevent oversights in procedures for registration, change, and deletion of user IDs and access rights.

4. Information systems division is to periodically review requirements for access rights, to confirm that user IDs and access rights are being granted appropriately. As an example, it is advisable to perform reviews, etc. at the same time as personnel relocations.

5. Particularly for information systems storing important information, it is advisable to perform control and checks based on time, number of accesses, and other access conditions. For example, in the case of time, organizations are to check whether important information is being accessed at night, and in the case of number of accesses, organizations are to check whether important information is being downloaded in bulk. For example, in the case of time, organizations can prohibit access to such information at night, and in the case of number of accesses,
organizations can employ a mechanism in which superiors are notified when important information is downloaded in bulk.\textsuperscript{15}

\textsuperscript{15} When performing monitoring through notification etc., organizations need to check for the notifications received and take appropriate steps.
(6) Rights management for system administrators

When there are multiple system administrators, organizations or the division in charge must assign an appropriate scope of rights for each system administrator ID, and must enable system administrators to monitor each other.

■ What risks are there?

If organizations do not assign an appropriate scope of rights for each system administrator ID, improper registration or deletion of user IDs can occur, and business may be obstructed by improper deletion or improper use of important information caused by improper registration. Furthermore, when the assignment of scope of rights is not appropriate, as when rights are overly concentrated in a single administrator, there may be obstructions to business continuity, such as destruction of information systems or deletion of important information.

■ Countermeasure points

To prevent internal improprieties by system administrators, organizations or the division in charge are to assign an appropriate scope of rights for each system administrator ID, and are to confirm that these are operated properly, as follows.

1. When determining system administrators, organizations or the division in charge are to appoint persons with appropriateness to the position, including high consciousness of rules. It is advisable that multiple administrators be appointed, enabling mutual monitoring.

2. Rights should be distributed so as to not be concentrated in a single system administrator.

3. In order to enable mutual monitoring by system administrators, organizations or the division in charge are to create and keep task reports recording the content and time of tasks. Moreover, it is advisable that the content of task reports be confirmed by other system administrators.

4. System administrators do not use their special privileges when performing operations requiring no such privileges.

---

16 When only one person in the organization is in charge of the system administrator, the organization (or the division in charge) cannot avoid such risks through privilege distribution. In such a case, the organization can mitigate those risks by having personnel other than the system administrator check the history of information system management operations.

17 When multiple system administrators are put in place, not only can persons performing the work of information system configuration check the content of their work, but other system administrators can check whether the configuration work is implemented properly, allowing administrators to monitor each other. Work other than monitoring involving the presence of several persons can also be considered. Such work may use distribution and division of keys, etc.
(7) Identification and authentication of users in information systems

To identify users (insiders using information systems) and system administrators (insiders managing information systems) of information systems, organizations must perform authentication using individual passwords, IC cards, etc. for individual users and system administrators, without using shared IDs, shared passwords, shared IC cards, etc.

■ What risks are there?

When organizations use shared IDs, passwords, IC cards, etc. in information systems, in the event of internal improprieties the organizations become unable to identify which users accessed important information, making identification of the perpetrators of internal improprieties difficult. Moreover, when the identification of perpetrators of internal improprieties is difficult, an environment is created in which it is psychologically easy to take important information from the premises.

Organizations that do not perform this management may be unable to pursue the liability of the perpetrators of internal improprieties. Moreover, doubt may be cast onto the management responsibility of the company or organization.

■ Countermeasure points

In order to appropriately perform identification and authentication of users in information systems, organizations must prepare and operate rules for managing user IDs and system administrator IDs, as follows.

1. To identify users and system administrators, organizations are to assign a user ID or system administrator ID to each user or system administrator. In addition, user IDs and system administrator IDs are to be authenticated using passwords, etc.

2. In order to prevent improper use of a user's user ID by another user, organizations should establish administrative items concerning passwords and should have users follow these. Examples include not setting simple text strings as passwords, and periodically changing passwords.

3. Organizations are to prohibit the lending of IDs, passwords, IC cards, etc. to other users.
4-3. Physical Management

(8) Physical protection and entry/exit management

Organizations must establish boundaries that physically protect locations where important information is stored, handled, etc. from entry other than by authorized persons, by protecting important information and information systems with walls and entry/exit management measures.

■ What risks are there?

When unauthorized persons have physical access to equipment storing important information, or to PCs or other information devices that handle important information, those information devices may be destroyed and obstacles to work created, or the devices may be stolen and information leaked. Alternately, leakage or deletion of important information may occur through manipulation of these information devices.

In particular, destruction of storage devices or storage media for important information may leave the business inoperable. This risk necessitates thorough protections such as server rooms with strict entry/exit management.

■ Countermeasure points

As an example, organizations must clarify areas for storage or handling of important information per Figure 6, and must physically protect these to restrict the insiders, or the delivery persons and other outsiders, who are able to enter these areas.

1. Organizations are to establish physical areas calling for strengthened security, and are to prepare security rules that should be followed in accordance with the importance of the information assets managed in each area. As an example, authentication via IC card is to be performed upon entry into the server room.

2. Organizations are to determine the areas which can be entered and exited by insiders (i.e., officers and employees) and outsiders (e.g., delivery persons) and are to manage their entry/exit, so as to prevent important information from being improperly taken from their premises. As an example, organizations may restrict entry/exit to the shipping entrance for delivery personnel, the reception room for clients, and the entranceway and work floors for officers and employees. Access to server rooms are to be restricted to system administrators and other qualified personnel, and to require prior permission from the administrative staff (including the responsible manager).

3. In entry/exit management, it is necessary that organizations create records of entry and exit in order to prevent internal improprieties and to track perpetrators after occurrences. Moreover, taking "records to identify individuals" (such as facial photographs) of those entering or leaving the room is highly effective in preventing internal improprieties. In this case, the "records of entry and exit" and "records to identify individuals" are to be audited regularly or at random.

4. For physical areas allowing access to important information, organizations must also take into account unauthorized entry during unmanned hours. As an example, it is advisable to install automatic security systems and surveillance cameras. It is also advisable that records of security system operators performing the unlocking of buildings (time of initial entry) and locking (time of final exit) include "records to identify individuals" such as their facial photographs.

5. Organizations must also consider preparing environments for disconnecting equipment containing important information from networks as required.
Figure 6  Example of areas to be physically protected
(9) Asset management and physical protection of information devices and storage media

1. Organizations or the division in charge must manage and protect PCs, other information devices, and portable external storage media ¹⁸ to prevent theft, improper removal from the premises, etc.  2. In addition, when disposing of unneeded information devices or storage media, organizations or the division in charge must confirm that important information has been completely deleted.

■ What risks are there?

When organizations or the division in charge do not manage information devices and storage media, an environment is created that facilitates theft or improper removal of items from the premises, and theft or improper removal may go unnoticed. Moreover, if organizations or the division in charge do not physically protect information devices, they might be stolen and important information leaked.

In addition, if devices or storage media on which important information is stored or has not been completely deleted are disposed of, this important information may be leaked.

■ Countermeasure points

Organizations or the division in charge must stipulate measures required for information devices and storage media that handle important information that should be protected, and manage and protect information devices and storage media in the way that they are protected from theft, improper removal from the premises, or careless disposal.

1. In order to facilitate the detection of the loss or improper removal of information devices or the division in charge are to manage the installation locations and users of the devices via ledgers, etc., and are to periodically conduct inventory (i.e., checking of assets).

2. It is advisable that information devices be affixed to desks, etc., using security cables, etc. to prevent theft or improper removal from the premises. Moreover, mobile devices (laptop PCs, smart devices, etc.) and portable storage media (USB storage, etc.) are to be stored locked in shelves, desks, etc.

3. Information devices such as important information storage servers and access management servers are to be installed in a place such as a server room with strict entry/exit management, to prevent physical access by persons other than administrators.

4. When disposing of information devices and storage media, organizations or the division in charge are to completely delete important information from HDDs, USB storage, and other portable storage media so that restoration is not possible. Moreover, it is advisable that CD-ROMs, DVD-ROMs, HDDs, and other storage media be physically destroyed using a shredder, etc.

¹⁸ USB storage, portable HDD, etc.
Management and monitoring of the removal of information devices and storage media from the premises

When mobile devices (laptop PCs, smart devices, etc.) and portable storage media (USB storage, CD-ROMs, etc.) are taken from a physically protected location per (8), organizations or the division in charge must manage the approval and recording of the removal.\(^\text{19}\)

**What risks are there?**

If organizations or the division in charge do not have approval system in place for the removal of mobile devices and storage media from the premises, important information may be taken without authorization and may be leaked. Moreover, if organizations or the division in charge do not keep records of removal from the premises, investigation of any internal improprieties may be difficult.

**Countermeasure points**

In the management of removal of mobile devices and storage media from the premises, organizations or the division in charge must establish and operate the following items.

1. When removing mobile devices and storage media from the premises, the approval of division managers, etc. must be obtained.
2. When removing mobile devices and storage media from the premises, records of the information assets taken, the date, the person in charge, etc. must be stored and managed.

---

\(^{19}\) See (14) regarding the protection of important information stored in portable information devices and USB storage in the case those devices and storage are taken from a physically protected location per (8)
(11) Restrictions on bringing in and using personal information devices and storage media for work

Information systems division must restrict employees' bringing in and using personal mobile devices (laptop PCs, smart devices, etc.) and portable storage media (USB storage, etc.).

■ What risks are there?

When personal information devices and storage media are used for work, management of these by the organization becomes difficult. Information belonging to individuals and information belonging to organizations become handled together, increasing the risk of important information being leaked due to virus infection, erroneous operations, etc. Moreover, investigation of any internal improprieties may be difficult if owners of personal information devices and storage media do not comply with investigations of the personal items.

When personal information devices and storage media are brought into work floors or other areas that handle important information, important information may be stored on the personal information devices or storage media and taken from the premises. Moreover, in the case of information devices with cameras, important information may be photographed and taken from the premises.

■ Countermeasure points

In restrictions on bringing in and using personal information devices and storage media for work, information systems division must take into account the degree of importance of important information and the installation location, etc. of information systems. Specifically, information systems division is to establish and operate the following.

1. Information systems division is to consider whether to allow the use of personal information devices and storage media for work.
2. Information systems division allowing this must prepare the scope of work for which usage is allowed, as well as compliance items and other rules. If the scope of work for which usage is allowed is broad, information systems division should note that the important information handled will increase and management will become difficult. Moreover, it is advisable for information systems division to gain written consent on compliance items regarding use for work.
3. When personal information devices are allowed to access an organization's networks, it is advisable to restrict access to only authorized work systems and work services.
4. When information with a high degree of importance is handled on personal information devices, it is advisable that software, etc. allowing management of the important information on the personal information devices be installed as required, allowing organizations to manage the important information.
5. In server rooms where servers storing important information, servers for access management, etc. are installed, information systems division is to sharply restrict employees' bringing in or using personally-owned laptop PCs, tablets, smartphones, etc.
6. In areas where bringing in information devices is prohibited, it is advisable to provide warnings of this via posters, etc.
7. Information systems division is to restrict employees' bringing in personally-owned USB storage and other portable storage media. Only portable storage media provided by the company is to be used.
4-4. Technological and operational management

(12) Safety management for network usage

To prevent the leakage of important information from users’ PCs and other information devices in the use of organizations' networks, organizations must prepare safe network environments by restricting the use of file sharing software, social network services (SNS), external online storage, etc.

■ What risks are there?

If file-sharing software is installed on information devices, important information on the devices may be unintentionally leaked to the outside. Executing external files shared over file sharing software may result in malware infection and even spread infection to other information devices in the organization.

Moreover, if organizations allow the use of SNS, the use of external online storage, and posting to message boards, important information may be uploaded or posted and thereby leaked.

■ Countermeasure points

To prevent external leakage of important information from organizations’ networks, organizations must take measures concerning information devices

1. Organizations must not allow the installation and use of software not authorized by the organization (e.g., file sharing software) on the PCs and other information devices of officers and employees. Organizations are to decide what software is allowed. In the case of requests by users for certain software, organizations must decide whether to allow its use.

2. With regard to Web access, it is advisable to install contents filter, and to restrict access to SNS, upload services, message boards, etc.

3. With regard to e-mail, it is advisable to confirm that e-mail software is not configured to forward business e-mails to personal e-mail addresses. Moreover, to prevent mistaken e-mail transmissions which could lead to the leakage of information, it is advisable to install a mechanism that enables senders to recheck for their outbound e-mails, or a mail system that does not allow the transmission of unencrypted attachments.

4. To protect PCs and other information devices, organizations are to implement general security measures such as installing antivirus software and applying security patches.
(13) Transfer and Protection of Important Information

1. The transfer of important information to contractors or other parties concerned must be appropriately managed at all steps from transfer to disposal. Moreover, taking into account the possibility of mistaken transfer of important information to persons other than the intended parties during the transfer of important information via transmission over the Internet or via hand delivery of storage media, the important information must be protected using encryption or other means.

■ What risks are there?

In the transfer of important information by e-mail, storage media, etc., if important information is not prevented from being taken from the premises other than when necessary, insiders may improperly take the important information. Moreover, if the transferred important information is not protected, important information may be leaked due to mistaken transmission of e-mail or due to theft or loss of storage media.

■ Countermeasure points

Steps are to be managed as follows, from the transfer of important information to parties concerned, to the disposal of the important information by said parties.

1. With regard to the transfer of important information, organizations are to establish internal procedures and approval measures matched to the degree of importance, and are to make contractors and other parties concerned comply with these.

2. Organizations are to record transfers of important information to parties concerned.

3. Organizations are to use encryption in the transfer of important information to parties concerned, when using transmission over the Internet or hand delivery of storage media.

4. When important information has been disclosed to parties concerned, organizations are to obtain from the parties records concerning the disposal or deletion of the important information.

5. With regard to the arrangements above, organizations must require compliance not only from contractors but also from their subcontractors.20

---

20 With regard to the oversight of entrusted parties, Article 22 of the Act on the Protection of Personal Information stipulates, "When entrusting the handling of personal data in part or in entirety to another party, a business operator handling personal information must perform necessary and appropriate oversight of the entrusted parties, to ensure the safe management of the personal data for which handling was entrusted."
(14) Protection of Information Devices and Storage Media taken from the Premises

When mobile devices (laptop PCs, smartphones, etc.) and portable storage media (USB storage, CD-ROMs, etc.) that store important information are taken from a physically protected location per (8), the important information must be appropriately protected through technological measures.

■ What risks are there?

When information devices or storage media storing important information is taken from the premises without the implementation of technological measures such as encryption or password locking, the important information may be leaked in the event of theft or loss.

■ Countermeasure points

When mobile devices (laptop PCs, smartphones, etc.) and portable storage media (USB storage, etc.) that store important information are taken from an organization's premises, the organization must take appropriate measures.

1. When information devices are used, organizations are to configure them to perform authentication via user ID, password, etc. Moreover, it is advisable to set BIOS passwords, HDD passwords, etc. for laptop PCs. It is also advisable to install encryption software for protecting important information.

2. When sending and receiving important information by connecting to external networks, organizations are to encrypt important information.

---

21 When devices (e.g. smartphones, tablet PCs, etc.) other than the organization's standardized devices are among the information devices being able to access important information, organizations must implement the same level of security measures on those devices as those for the organization's standardized devices.
When performing work using important information outside of physically protection locations per (8), organizations must appropriately protect the important information, taking the surrounding environment, network environment, etc. into account.

■ What risks are there?

When work is done in a public place, important information may be leaked if viewed by surrounding persons. Moreover, if the organization's network is accessed via a public wired or wireless LAN and the communication is not protected, eavesdropping of the important information on the network may occur and the important information may be leaked.

■ Countermeasure points

In work involving important information outside of the organization, screens must be appropriately protected from unwanted viewing in the usage environment, and connections must be limited to approved network environments.

1. Care is to be taken against unwanted viewing of screens on trains, in cafes, etc. Moreover, it is advisable to protect screens from unwanted viewing by using privacy protection film, etc.

2. Organizations are to determine whether to allow connection to hotel wired or wireless LANs, public wireless LANs, and other networks shared by unknown users.

3. When accessing the organization's networks from an approved network environment, communication must be encrypted using a VPN, etc.

4. It is advisable to use tools or services allowing remote deletion of information on information devices in the event of the loss of information devices storing important information. Moreover, it is also advisable to use tools that delete important information when password lock authorization fails a set number of times.
Confirmations when Using Services Provided by Third Parties (Including Cloud Computing)

Before contracting and usage of services provided by a third party, organizations must confirm and agree with their service contents (security management measures, service level, provision of logs, etc.) and afterward must confirm that the third party is implementing services according to contract.

■ What risks are there?

If organizations do not determine which information may be handled via services provided by third parties and which may not, they may entrust sensitive, business-related information to the third parties, and should the leakage of such information occur, they may not be able to continue their operations.

When organizations use services provided by third parties without confirmation of their content and security management measures in place, important information may be leaked due to deficiencies in the third party's security management measures. Moreover, depending on the content of the agreement, damages caused by leakage of important information may not be compensated. Moreover, if organizations do not provide for the receipt of logs is in the agreement, investigation following the occurrence of internal improprieties may become difficult.

If organizations do not confirm that third parties are implementing services according to contract, they may be unable to prevent information leakages, etc. caused by deficiencies in the third parties.

■ Countermeasure points

In using services provided by third parties, organizations are to confirm in advance any matters necessary for the safe management of important information, and incorporate these into agreements. During use of services, organizations must confirm that services are being implemented according to contract. Specifically, organizations must confirm the content of services from the following standpoints, and must clarify the content of services or the content according to level.

1. Organizations must determine which information may be handled via services provided by third parties and which may not.
2. Organizations are to determine whether the security management measures of services provided by third parties are sufficient for the safe management of important information.
3. Organizations are to confirm whether the service level and management requirements of services provided by third parties are appropriate for business continuity.
4. Organizations must confirm whether logs will be provided in the event of internal improprieties.
4-5. Securing Evidence

(17) Recording and Storage of Logs and Trails in Information Systems

From the standpoints of early discovery of internal improprieties and the scope of the effects of follow-up measures, it is advisable to record and store logs and trails including the history of access to important information and users' operation history, and then securely preserve them.

■ What risks are there?

If information systems division does not record logs and trails, they will be unable to uncover the actions in logs and trails that are signs of improper activity, meaning that detection may be delayed and damage may be major when detected. Moreover, if information systems division does not preserve logs and trails, then in follow-up measures after incidents of internal improprieties, they will have difficulty identifying the causes of internal improprieties or investigating the trail of the perpetrators of the internal improprieties or the scope of effects. Moreover, if information systems division does not preserve logs and trails securely, grounds for punishment, etc. may not be recognized.

■ Countermeasure points

From the standpoints of early detection of internal improprieties and follow-up measures, information systems division is to record logs and trails and securely preserve them as follows.

1. Logs are to record histories of access to important information and the operation history of users (web access logs, histories of sending/receiving e-mails, etc.).
2. Trails are to record information other than that in the above logs, including date, user, operation terminal, content of operations, and content of transmissions, based on established policies.
3. Logs are to be reviewed on a regular basis. It is advisable to check for non-routine work performed by officers and employees, including access to a large number of files or to the files that are not relevant to their work. If the case has been confirmed, organizations are to strengthen monitoring or take other measures.
4. It is advisable to take users' privacy into account and obtain agreement from the labor union and other parties concerned as to collecting such logs and trails,
5. Information systems division is to decide the period of preservation for logs and trails, balancing risks and costs. From the standpoint of preventing internal improprieties, it is advisable that the period of preservation not be made known to insiders. In it is advisable that information systems division take measures to prevent falsification and unauthorized deletion, and allow access only by specified system administrators.

---

22 Records of events occurring in information systems and networks. In these Guidelines, "logs" are logs of activity taken on a system, and "trails" are collected according to policies determined for monitoring and auditing.

23 Information systems division must consider the period for storing logs from various standpoints, including the importance of the information to be logged, cost, business type, business form, etc. Relevant laws and regulations include, with respect to the preparation of rules for requesting the preservation of electromagnetic records of communication history under the partial revision to the Code of Criminal Procedure, include the following: "A public prosecutor, public prosecutor's assistant officer, or judicial police officer, when deeming seizure or seizure with demand for recording to be necessary, are to identify necessary items in electromagnetic records of communication histories recorded for business purposes, and may request in writing that these not be deleted for a period not to exceed 30 days (extensible to a period not to exceed 60 days in the case of particular need)."
Those checking for the logs and trails must obtain prior permission from system administrators such as responsible managers.
Information systems division is to record and store logs and trails of the access history and operation history of system administrators, and, along with logs and trails per (17), must have persons other than system administrators periodically perform checks of the content of logs and trails of system administrators.

■ What risks are there?

As system administrators bear considerable privileges, if persons other than system administrators do not check and monitor work reports by system administrators, it will be difficult to check the correctness and authenticity of tasks and to detect internal improprieties by system administrators.

■ Countermeasure points

Information system logs must log not only failures, but also normal administration and operation work. Specifically, information systems division is to establish the following, and record and protect work logs.

1. Information systems division is to record logs of work concerning information system configuration changes and operations, with the content of the work logs periodically checked by the supervisors of the information system administrators or by supervising administrators.24

2. When collection of logs and trails can not be performed in information systems, the work content of system administrators is to be documented, and is to be periodically checked by the supervisors of the information system administrators or by supervising administrators.

---

24 Companies and organizations which perform internal impropriety countermeasures and which have internal audit systems in place are to consider methods of checking and operating as audit items for internal audits.
4-6. Human Management

(19) Dissemination of Internal Impropriety Countermeasures through Education

1. Organizations must provide education for all the officers and employees, and must disseminate policies concerning the organization's internal impropriety countermeasures, procedures for handling important information, etc. It is advisable to repeat the education periodically. Moreover, organizations must review and update the content of the education, and disseminate the updated content to insiders.

■ What risks are there?

If organizations do not provide education for all the officers and employees, officers and employees may not take appropriate measures and internal improprieties may occur. Moreover, if organizations do not review the content of the education, measures toward new threats may not be taken, and internal improprieties may occur. Organizations that do not provide education may be unable to pursue the liability of persons committing internal improprieties. Moreover, doubt may be cast onto the management responsibility of the company or organization.

Note that, with respect to contractual parties to whom important information is presented, if organizations do not sufficiently inform the officers and employees directly handling said information of the fact of the important information and the handling of important information, information may be leaked by the contractual party.

■ Countermeasure points

In education, organizations must provide knowledge of important information and the handling of important information, must heighten officers' and employees' understanding and awareness of internal impropriety countermeasures, and must have them implement countermeasures.

1. Organizations are to provide education concerning matters to be followed by insiders, the background to these, and so on. It is advisable to repeat the education every year so its content is not forgotten.

2. As evidence of the education having been conducted, organizations are to record the fact that participants underwent the education and understood its content.

3. Organizations are to periodically review and update the content of the education, and disseminate the updated content.

4. It is advisable to conduct the education at appropriate levels and with appropriate content based on the privileges and duties of the participants, including position (managerial, non-managerial, etc.) and form of contract (employee, temporary worker, etc.). It is particularly advisable to provide education aimed at heightening consciousness of rules in system administrators.
To prevent the occurrence of important information leakage or other internal improprieties by ex-employees after the conclusion of employment, organizations should require said employees to submit written pledges of confidentiality as required.

■ What risks are there?

If organizations do not conclude confidentiality agreements (including written pledges) at the conclusion of employment, the officer or employee will leave the organization without recognizing the criticality of the important information they obtained during their work. In this case, the risk of such important information being disclosed by ex-officers and ex-employees increases. Furthermore, claims for damages caused by said disclosure will not be recognized. Organization may conclude no-compete obligation agreements (including written pledges) as required, but must be careful not to obstruct freedom of occupational choice.

■ Countermeasure points

At the conclusion of employment, it is advisable that organizations conclude confidentiality agreements and no-compete obligation agreements (including the submission of written pledges) with employees.

1. Confidentiality agreements must include descriptions which enable objective identification of the important information subject to confidentiality.

2. Any no-compete obligations must be of appropriate scope so as not to obstruct freedom of occupational choice.
(21) Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract

At the conclusion of employment or work contracts, organizations must require employees and contractors to return or completely delete all information assets that they were entrusted to handle. Moreover, organizations must delete information system user IDs and privileges granted to hires or contractors.

■ What risks are there?

If information assets (including important information) for which handling were entrusted are not returned or deleted, there is a risk of important information being leaked by ex-employees or ex-contractors. Moreover, if entry passes and loaned devices are not returned, or information system privileges are not deleted, improper entry into buildings, unauthorized intrusion into information systems via networks, and improper removal of information assets from the premises may occur.

■ Countermeasure points

Organizations must take the following measures at the conclusion of employment or contracts.

1. Written pledges or contracts must specify the return of information assets and the complete deletion of information assets from contractors' PCs, etc. at the conclusion of employment or contracts.
2. Organizations must confirm the return of all information assets for which handling was entrusted, and all entry passes.
3. Organizations must confirm the deletion of information system user IDs and privileges.
4. It is advisable to obtain conclusive evidence that all important information stored on contractors' PCs, etc. has been completely deleted.
5. As the removal of information and other internal improprieties occur more easily immediately prior to conclusion of employment, it is advisable to place PCs, etc. under the management of the system administration division, etc. for a set period prior to the conclusion of employment. (Examples: Restrictions on scope of access, restrictions on USB storage usage, etc.)
4-7. Compliance

(22) Preparation of Legal Proceedings

Organizations must take into account dismissal or other disciplinary actions for insiders committing internal improprieties, prepare rules of employment and other internal rules, and make provisions for official disciplinary proceedings.

■ What risks are there?

If disciplinary actions toward insiders committing internal improprieties are not incorporated into rules of employment or other internal rules, or if official disciplinary proceedings are not prepared, disciplinary actions may be rendered invalid by a claim of improper action from the insider.

■ Countermeasure points

When taking disciplinary action, it is necessary that items concerning disciplinary actions and confidentiality obligations be stipulated in internal rules.

1. Internal rules must note the internal improprieties (e.g., infringement of trade secrets, use of personal information for non-allowed purposes) that are subject to disciplinary action.
2. Internal rules must include descriptions which enable objective identification of important information for which confidentiality obligations hold.
3. Organizations must conduct dismissal and other disciplinary action within the framework of labor laws, based on internal rules that form the grounds for action.
4. In order to determine an appropriate disciplinary action, it is necessary to make the facts clear through a commission of inquiry, etc.
5. Organizations must make preparations for civil action and criminal prosecution legal proceedings.

See the following for examples of rules of employment and other detailed information.

○ Examples of rules of employment and examples of trade secret management rules
  "Trade Secret Management Guidelines, Reference Materials 2: Examples of Contracts (Ministry of Economy, Trade and Industry)"

○ Detailed Requirements of Related Laws and Regulations
  "Collected Requirements of Information Security-Related Laws and Regulations (Ministry of Economy, Trade and Industry), June 2009"
(23) Requests for Written Pledges

In order to make obligations to protect important information understood by officers and employees, organizations must request them to submit written pledges of confidentiality.

■ What risks are there?

If officers and employees do not submit written pledges, organizations will be unable to instill understanding and awareness of the obligations to protect important information. Moreover, in the event of dismissal or other disciplinary proceedings against officers and employees committing internal improprieties, disciplinary actions may be rendered invalid by a claim of improper action from the officers and employees.

■ Countermeasure points

Organizations must ensure that the important information covered in written pledges of confidentiality can be identified objectively. Moreover, organizations must request written pledges of confidentiality at periodic intervals so as to instill awareness of the protection of important information.

1. Written pledges of confidentiality must include descriptions which enable objective identification of the important information subject to confidentiality.
2. In order to make obligations to protect important information understood by officers and employees, it is advisable that organizations request written pledges of confidentiality at periodic intervals in addition to the time of joining the company, such as at the time of changes in work duties due to advancement, personal relocation, etc., or at the conclusion of projects.

See the following for examples of rules of written pledges of confidentiality and other detailed information.

○ Examples of written pledges of confidentiality


---

25 If organizations request the submission of written pledges of confidentiality from officers and employees at their retirement, they may not accede to the request.
4-8. Workplace Environments

(24) Preparation of Impartial Personnel Evaluations

It is advisable that personnel division provides impartial and objective personnel and performance evaluations. It is also advisable to provide opportunities to explain how evaluation is carried out in personnel and performance evaluations. Moreover, it is advisable to conduct personnel assignments and reassignments to prepare appropriate work environments, as required.

■ What risks are there?

When employees do not feel impartiality and objectivity in personnel evaluations and performance evaluations, discontent and dissatisfaction can degrade the workplace environment, which in turn may induce internal improprieties.

Moreover, if specific work is left in the hands of an individual without reassignment for long periods, important information may be handled only by the individual and improperly used. Moreover, if handling of the same type of important information becomes routine, awareness of the need for caution in handling the important information may lessen, heightening the likelihood of incidents occurring through careless mistakes or errors in operation.

■ Countermeasure points

The personnel division and persons in charge of personnel must take the lead in preparing evaluation systems for personnel evaluations and performance evaluations. Moreover, appropriate personnel assignments and relocation must be done.

1. It is important that personnel division impartially and objectively implement promotions, advancement, and organizational pay structure, while maintaining sufficient transparency. It is advisable that superiors or division heads provide explanations of the content of performance and other evaluations, as required.

2. As part of preparation for evaluation systems, it is advisable that organization encourage officers and employees to participate in education and training for skills and knowledge necessary for work.

3. When specific work is left in the hands of an individual without reassignment for long periods, it is advisable to consider personnel relocation to avoid such situation.
Promotion of Reasonable Work Environments and Communication

Organizations should promote environments that maintain good communication throughout the workplace, such as by preparing systems for promoting mutual work support and environments facilitating consultation, while also preparing suitable work environments through means such as normalization of workloads and working hours.

What risks are there?

If organizations do not prepare work environments with suitable workloads and working hours, specific officers/employees may be overloaded with work, and trying to reduce their workload and working hours, they may commit internal improprieties. Moreover, difficulties in executing work duties can heighten discontent in officers and employees and lead to internal improprieties. Moreover, when environments facilitating consultation or good communication are insufficient, work may continue under a situation of work-related worries or stress, and internal improprieties may occur.

Countermeasure points

In the preparation of workplace and work environments, the general affairs division and the persons in charge thereof must take the lead in normalizing workloads and working hours. In addition, they must prepare environments that facilitate consultation while considering trust relationships in the workplace, and at the same time, must promote support for work along with good communication with superiors and colleagues.

1. When workload is extremely high or working hours are long, including situations in which specific individuals cannot take time off or situations of overtime work, organizations must set appropriate scopes for workload and working hours.
2. Organizations must set work within a scope that is not harmful to physical or mental health, and must keep workplace environments safe and sanitary.
3. Superiors and division heads must discern the capabilities of staff members and subordinates and, to the extent possible, allot appropriate work content and workloads to these.
4. Superiors and division heads must consider systems and environments for providing as much support as possible to members and subordinates who require assistance with work and duties.
5. Organization must construct and maintain good teamwork among staff members, with staff members assisting each other with delays or problems on the job.
6. Organization must create and maintain an environment in which staff members engage in active exchange of information on the job and can also engage in consultations other than for work.
7. It is advisable that organizations promote work support and aid by persons.
8. In order to detect and rectify concerns over work or stress over personal relationships, it is advisable that organizations prepare environments that facilitate consultation not only with superiors but also with colleagues, and promote environments that maintain good communication throughout the workplace.
9. It is advisable that organizations create environments in the workplace that facilitate listening to problems. It is advisable to prepare environments in which when officers and employees find it hard to pour out their concern at the workplace (e.g. those related to their immediate superior), they can consult a consultation service outside their workplace that provides feedback to a big boss so that the situation is improved. To make consultants feel safe, organizations may handle concerns with anonymity depending on their content, with their feedback provided to a big boss.
it is advisable that organizations or the division in charge restrict independent work
that is conducted apart from other employees and disallows mutual monitoring.

■ What risks are there?

As independent work involves an environment in which the absence of other employees
disallows mutual monitoring, the likelihood of internal improprieties occurring is high. When
internal improprieties do occur, detection may be delayed and damage may spread. Moreover, when such independent work is performed, (24) proper preparation of impartial
personnel evaluations and (25) promotion of proper work environments and communication
may be degraded.

■ Countermeasure points

1. As independent work involves an environment in which the likelihood of internal
improprieties occurring is high, organizations need to check for the necessity of the
work etc. and prepare procedures to track the work. For each independent work, the
responsible manager etc. of the division concerned must check if the work really
needs to be done independently and pre-approve it. Check items for the
pre-approval are: the reason for "Why the work needs to be done in that period?"
eetc.; period/hours; and contents of the work. It is advisable to consider necessary
assistance to avoid such independent work.

2. Independent work involves the risk of internal improprieties by the individual, so
organizations need to perform after-the-fact check. Check items for the after-the-fact
check are: consistency between the pre-approved work contents and the actual work
contents; whether or not important information is handled during the independent
work; and contents of modification, etc.
4-9. Follow-up measures

(27) Preparation of Systems Required for Follow-up Measures

In order to identify the scope of the effects of internal improprieties, organizations must assess the concrete status of incidents and must implement measures to minimize damage and prevent the spread of effects. In addition, organizations must secure systems for cooperation with parties concerned inside and outside the organization, as required.

**What risks are there?**

Organizations that cannot identify the scope of the effects of internal improprieties may be unable to take prompt follow-up measures and may be unable to consider legal enforcement and other responses. Furthermore, when using third-party services (digital forensic analysis, incident response support, etc.) in the investigation or handling of internal improprieties, organizations that have not made provisions for the necessary information and means of communication may be unable to receive suitable support.

**Countermeasure points**

To construct systems required for follow-up measures, organizations must prepare the following content.

1. To minimize the damage caused by internal improprieties and prevent the spread of effects, organizations must determine in advance the required response procedures and reporting procedures. To assess the concrete situation surrounding internal improprieties and investigate the scope of effects, organizations must preserve verifiable evidence concerning "who did what and when.”

2. In responding to internal improprieties, organizations must cooperate with system administrators, persons in charge of incident response (including persons in charge of external incident response support), persons in charge of digital forensic analysis (including persons in charge of external support), attorneys, and internal auditors, and other third-party services. Moreover, when receiving services, it is advisable that organizations determine the content and methods of communication in advance, so as to enable prompt provision of necessary information.

3. Organizations must prepare systems for responding to cases that involve reporting requirements to the competent authorities.

4. Organizations having business continuity plan (BCP) and going to construct systems for internal impropriety countermeasures need to take into account the relationship with the BCP.

---

26 A series of scientific investigative methods and techniques for conducting preservation of evidence, investigation, and analysis of electromagnetic records, along with analysis and information collection concerning falsification, damage, etc. of electronic records, in response to legal disputes, legal action, and acts such as improper use of computer and networks or obstruction of service.

27 Follow-up response for the purpose of minimizing damage following information security incidents and accidents such as malicious attacks, viral infections, and theft of PCs.

28 See "Documents proving the consistency of evidence preservation (Chain of Custody)” of the Evidence Preservation Guidelines issued by the Institute of Digital Forensics.
Consideration of Punishment and Prevention of Recurrence

Organizations must consider the punishment to be applied to internal perpetrators of serious improprieties. Moreover, from the standpoint of preventing recurrence, while taking measures to prevent recurrence it is also advisable that organizations provide notification within the organization of cases involving internal improprieties.

■ What risks are there?

When organizations do not consider punishments for the perpetrators of internal improprieties, or do not take measures to prevent recurrence, similar internal improprieties may recur. Moreover, from the standpoint of preventing recurrence, when organizations do not perform internal notification and dissemination of cases involving internal improprieties, similar internal improprieties may recur.

■ Countermeasure points

To consider punishment for perpetrators of internal improprieties, and to consider the prevention of recurrence, organizations must prepare the following content.

1. To minimize the effects caused by internal improprieties, organizations must incorporate internal impropriety countermeasures into required response procedures, reporting procedures, and other business continuity management procedures. In order to consider punishments for perpetrators of internal improprieties, organizations must undertake consideration of legal action together with persons in charge of personnel, persons in charge of legal affairs, attorneys, etc., based on content established in the preparation of legal proceedings per (22) in these Guidelines.

2. Organizations must consider and implement measures to prevent the recurrence of internal improprieties.

3. It is advisable that organizations learn from the specific facts of incidents of internal improprieties, and, from the standpoint of preventing recurrence, provide notification of cases of internal improprieties within the organization, including the actions taken against the perpetrators.
4-10. Organizational management

(29) Preparation of Whistleblower Systems for Internal Improprieties

Organizations or the division in charge must prepare whistleblower systems for the occurrence of incidents suspected of involving internal improprieties. Organizations or the division in charge must establish multiple whistleblower contact points to allow reports by employees to parties concerned with internal impropriety countermeasures (Supervising Manager, etc.) other than their own divisions. Organizations or the division in charge must also secure anonymity for whistleblowers, as required. Organizations or the division in charge must also provide education on the specific usage and disseminate it.

■ What risks are there?

If organizations or the division in charge do not prepare whistleblower systems for the occurrence of incidents suspected of involving internal improprieties and do not provide education on the specific usage, internal whistleblowing will not function, response will be delayed, and signs of internal improprieties may be overlooked. Moreover, if organizations or the division in charge do not establish multiple whistleblower contact points for internal improprieties, then cover-ups may prevent information from reaching (i.e., being reported to) the Supervising Manager, etc. from divisions where the problems are thought to have occurred. Moreover, if organizations or the division in charge do not secure anonymity for whistleblowers, then due to the effects of surrounding human relations, etc., information thought to concern internal improprieties may not be obtained.

■ Countermeasure points

With regard to internal impropriety whistleblower systems, organizations or the division in charge must prepare content such as the following.

1. Reporting of internal improprieties must include the following information, etc. at a minimum: "Contact points (contact information and method)," "Targeted information or physical assets," "Time and situation of incident (e.g., improper use, destruction, etc.)," "How the incident became known," etc.

2. Organizations or the division in charge are to provide education on the above internal whistleblowing.

3. It is advisable for organizations or the division in charge to establish whistleblower contact points (including hotlines, etc.) in addition to the heads of the divisions to which employees belong.

4. In order to secure anonymity and prevent whistleblowers from suffering disadvantages from the act of reporting, organizations or the division in charge are to consider establishing anonymous post office boxes and suggestion boxes, or to consider the use of third-party organizations.
Implementing Checks Incorporating the Prevention of Internal Improprieties

Organizations must identify specific internal impropriety countermeasure items from the standpoint of preventing and deterring internal improprieties, and must conduct checks (including internal and other audits). Moreover, organizations must report the results of audits, following confirmation by the Supervising Manager, to the top manager (or management team), and must conduct reviews of countermeasures as required.

■ What risks are there?

(1) If organizations do not conduct periodic checks and audits, including the monitoring noted under Clarification of the Responsibilities of the Top Manager, the organizations may be unable to confirm the status of internal impropriety countermeasures or problem points in the organization, and may be unable to conduct and review effective measures.

■ Countermeasure points

In order to conduct checks and audits (including internal audits and external audits) incorporating the standpoints of prevention and deterrence of internal improprieties, organizations must consider the following items.

1. Organizations must make reference to items which are particularly advisable as internal impropriety countermeasures (measures in the underlined portions of these Guidelines and items thought to be related in cases of internal improprieties, etc.), must confirm the implementation status, preparation status, etc. of specific countermeasures, and must report to the top manager (or management team).

2. Organizations must check matters including whether differing management and handling are being applied to similar information, based on the work content of each division and dealings with parties concerned.

3. Organizations must confirm records concerning incidents thought to involve internal improprieties and related incidents, and must confirm that these are promptly reported following occurrence. Moreover, organizations must confirm whether any cases violate management procedures and handling methods for important information, and must confirm follow-up remedies, etc.
Appendix I: Internal Impropriety Case Studies

Case studies from interviews surveys and case study surveys from the "Survey of Incidents Due to Improper Activity by Organization Insiders" by the Information-technology Promotion Agency, Japan and from the committee for the creation of “Guidelines for the Prevention of Internal Improprieties in Organizations” are presented below.

<table>
<thead>
<tr>
<th>No</th>
<th>Overview</th>
<th>Items related to these Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A salesperson at a regional financial institution was embezzling funds from dormant accounts. Main cause: The salesperson was kept in a position without reassignment in order to maintain sales performance and no mutual monitoring was in place, which created an environment in which internal improprieties were difficult to detect</td>
<td>(24) Preparation of Impartial Personnel Evaluations (26) Management in Workplace Environments</td>
</tr>
<tr>
<td>2</td>
<td>A system administrator in a small company changed settings on the president's PC to forward e-mail sent to the president to the account of the system administrator, who then read the e-mail. Main cause: Only one person in the company was in charge of the system administrator, creating an environment in which internal improprieties were difficult to detect. Moreover, this employee may have had low consciousness of the rules required for system administrators.</td>
<td>(7) Administrator Access Management (19) Dissemination of Internal Impropriety Countermeasures through Education</td>
</tr>
<tr>
<td>3</td>
<td>A system administrator employee in a company taken confidential information from the premises with the intent of working at home, but performed work on a home PC with file-sharing software (Winny) installed, resulting in leakage of information. Main cause: Confidential information was taken from the premises without informing anyone. The employee may not have fully known the severity of punishment for working at home without permission and leaking confidential information.</td>
<td>(12) Safety Management for Network Usage (19) Dissemination of Internal Impropriety Countermeasures through Education</td>
</tr>
<tr>
<td>4</td>
<td>A laptop PC was lost while left for a long period on a piled-up desk. Subsequent investigation revealed that the laptop PC had been sold, with the perpetrator unknown. Main cause: Laptop PCs were not managed, and could be taken away by anyone entering the floor.</td>
<td>(9) Asset Management and Physical Protection of Information Devices and Storage Media</td>
</tr>
</tbody>
</table>
|   | An employee in a company took a CD-ROM containing confidential information from the premises, and sold the information. When taking confidential information from the information system, the employee had his subordinate create the CD-ROM containing the confidential information through official procedures, explaining to the subordinate that the action was part of work, and then engaged in cover-up.  
Main cause:  
Removal of CD-ROMs containing confidential information from the premises was not managed. | (9) Asset Management and Physical Protection of Information Devices and Storage Media |
|---|---|---|
| 6 | A developer in a company took development source code, etc. from the premises by uploading it to external online storage, out of belief that he owned the source code he developed and that the code would be useful in other projects.  
Main cause:  
The developer did not recognize that developed items belong to the company. Moreover, the company did not restrict the use of external online storage. | (12) Safety Management for Network Usage  
(19) Dissemination of Internal Impropriety Countermeasures through Education |
| 7 | A system administrator in a company repeatedly took confidential information from the premises and sold it. Each time, the employee escalated the severity of the act of removing confidential information from the premises.  
Main cause:  
The company was supposed to perform monitoring of system administrators' operations, but confidential information was repeatedly taken from the premises due to laxness on the part of the person in charge. Moreover, the privileges of system administrators were not distributed and may have been concentrated in a single person. | (6) Rights Management for System Administrators  
(18) Checking of System Administrators' Logs and Trails |
| 8 | A telecommuting employee in a company connected to the company's information systems from home via the Internet, and obtained and sold confidential information. As telecommuting makes work difficult to monitor, it more readily facilitates internal improprieties than does an office.  
Main cause:  
The company did not restrict access to its information systems and confidential information via the Internet by telecommuters, etc. Moreover, the company may not have been monitoring whether information other than that necessary for telecommuting was being accessed. | (15) Protection of Important Information in Work Outside of the Organization  
(17) Recording and Storage of Logs and Trails in Information Systems |
| 9 | Upon leaving a company, an employee downloaded a developed item and took it from the premises, with the intent of using it in a new place of employment.  
Main cause:  
There was a lack of awareness that developed items should not be taken from the premises and used at the new place of employment. Moreover, non-routine work performed by officers and employees such as access to a large number of files was not monitored and no measures were enacted. | (5) User access Management in Information Systems  
(17) Recording and Storage of Logs and Trails in Information Systems  
(20) Personnel Procedures for Conclusion of Employment |
<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>A salesperson in a company, leaving the company due to restructuring,</td>
<td>(21) Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract</td>
</tr>
<tr>
<td></td>
<td>changed a PC password without permission, and then claimed forgetfulness in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not providing notice of the changed password.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Main cause: Management rights for the PC were not placed with the company for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a set period prior to the conclusion of employment.</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>A number of employees in a division of a company, retiring at the same time</td>
<td>(20) Personnel Procedures for Conclusion of Employment</td>
</tr>
<tr>
<td></td>
<td>to form a new company, took customer data (a trade secret) from the premises</td>
<td>(21) Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract</td>
</tr>
<tr>
<td></td>
<td>for use in the new company.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Main cause: The employees had poor awareness of the fact that the act of</td>
<td>(23) Requests for Written Pledges</td>
</tr>
<tr>
<td></td>
<td>improperly removing trade secrets from the premises and using the information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>violates the Unfair Competition Prevention Act.</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>An employee of a contracted web site construction and operation company</td>
<td>(13) Transfer and Protection of Important Information</td>
</tr>
<tr>
<td></td>
<td>sold the customer data of a client company to a competitor, despite knowing</td>
<td>(16) Confirmations when Using Services Provided by Third Parties (Including Cloud Computing)</td>
</tr>
<tr>
<td></td>
<td>the impropriety of the act. The competitor used the customer data for its</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sales activities.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Main cause: The company may not have confirmed that the information security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>measures of the contracted web site construction and operating company were</td>
<td></td>
</tr>
<tr>
<td></td>
<td>sufficient.</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>An ex-employee of a company manufacturing and selling products used the</td>
<td>(21) Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract</td>
</tr>
<tr>
<td></td>
<td>company’s design drawings to manufacture and sell similar products at a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>competing company.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Main cause: The company did not properly handle the return of important</td>
<td></td>
</tr>
<tr>
<td></td>
<td>information upon departure of employees.</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Personal information handed over by a company to a maintenance contractor</td>
<td>(13) Transfer and Protection of Important Information</td>
</tr>
<tr>
<td></td>
<td>was copied and sold by a part-time worker in a subcontracting company.</td>
<td>(16) Confirmations when Using Services Provided by Third Parties (Including Cloud Computing)</td>
</tr>
<tr>
<td></td>
<td>Main cause: The company did not make the important information management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>systems of the contractor clear, and did not perform management extending to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>subcontractors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Case Description</td>
<td>Main Cause</td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>15</td>
<td>An ex-employee of a company used a remote access connection service for connecting to the company's network via the Internet, and taken confidential information from the company. Main cause: The ex-employee's account was not deleted from the remote access connection service.</td>
<td>(5) User Access Management in Information Systems</td>
</tr>
<tr>
<td>16</td>
<td>A teacher in an educational institution used USB storage to take grades and other student data from the premises. The student data was leaked when the USB storage was stolen. Main cause: The student data was not encrypted.</td>
<td>(15) Protection of Important Information in Work Outside of the Organization</td>
</tr>
<tr>
<td>17</td>
<td>In an educational institution environment allowing tacit permission for work usage of personal smartphones, an employee's personal smartphone was stolen and the personal information stored was leaked. Main cause: The institution did not set and operate an appropriate scope of usage, tacitly allowing work usage of personal smartphones.</td>
<td>(11) Restrictions on Bringing in and Using Personal Information Devices and Storage Media for Work</td>
</tr>
</tbody>
</table>
Appendix II: Internal Impropriety Check Sheet

The internal impropriety check sheet in this appendix is a summary of the countermeasures presented in Chapter 4 in these Guidelines.

* □: Key person in charge / implementing division\(^{29}\); [ ]: Divisions confirming support / implementation aid\(^{30}\)

<table>
<thead>
<tr>
<th>No</th>
<th>Content</th>
<th>Check items</th>
</tr>
</thead>
<tbody>
<tr>
<td>■Basic Policies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Has the top manager formulated basic policies and disseminated these to officers and employees, for the purpose of showing within and outside the organization that internal impropriety countermeasures are the responsibility of the top manager? (See Appendix IV for examples of basic policies.)</td>
<td>□: Top Manager(CEO)</td>
</tr>
<tr>
<td>2-1</td>
<td>Has the top manager appointed a Supervising Manager for internal impropriety countermeasures, and is the top manager conducting approvals for management systems and implementation measures? (However, if the organization is one in which the top manager has a view of the entire organization and implements internal impropriety countermeasures on his or her own, it may not be necessary to construct management systems.)</td>
<td>□: Top Manager(CEO)</td>
</tr>
<tr>
<td>2-2</td>
<td>Has the Supervising Manager constructed cross-organizational management systems in accordance with the basic principles, and formulated implementation measures?</td>
<td>□: Supervising Manager</td>
</tr>
</tbody>
</table>

---

\(^{29}\) A division which, from the standpoint of its work content, is deemed appropriate to implement that countermeasure item in the check sheet

\(^{30}\) Divisions with which key person in charge/implementing division should cooperate in establishing and implementing the countermeasure item.
<table>
<thead>
<tr>
<th>No</th>
<th>Content</th>
<th>Check items</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Immediate division</td>
</tr>
<tr>
<td>■Designation as Confidential</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Does the organization assess important information, assign it rating categories according to degree of importance, and set the scope of insiders allowed to handle the information?</td>
<td>□</td>
</tr>
<tr>
<td>4-1</td>
<td>Do creators of important information select an established rating category for the information, and obtain confirmation of the selection from superiors, etc.?</td>
<td>□</td>
</tr>
<tr>
<td>4-2</td>
<td>Are confidentiality marks, etc. understandable by insiders displayed on electronic documents containing important information?</td>
<td>□</td>
</tr>
<tr>
<td>■Designation of Access Rights</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-1</td>
<td>Do persons in charge of administering and operating information systems do so with procedures established for registration, change, deletion, and other settings concerning user IDs and access rights?</td>
<td>□</td>
</tr>
<tr>
<td>5-2</td>
<td>Do persons in charge of administering and operating information systems promptly delete user IDs and access rights that have become unnecessary due to transfer or retirement?</td>
<td>□</td>
</tr>
<tr>
<td>6</td>
<td>When there are multiple system administrators, does the organization assign an appropriate scope of rights for each system administrator ID and enable information system administrators to monitor each other? In addition, when only one person in the organization is in charge of the system administrator, does the organization monitor the administrator' operations through logs etc.?</td>
<td>□</td>
</tr>
<tr>
<td>7</td>
<td>Does the organization perform authentication using individual passwords, IC cards, etc. for individual users and system administrators, without using shared IDs, shared passwords shared IC cards, etc.?</td>
<td>[ ]</td>
</tr>
<tr>
<td>■Physical Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Does the organization physically protect locations where important information is stored, handled, etc. with walls and entry/exit management measures?</td>
<td>□</td>
</tr>
<tr>
<td>No</td>
<td>Content</td>
<td>Immediate division</td>
</tr>
<tr>
<td>----</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>9-1</td>
<td>Does the organization manage and protect information devices such as PCs and portable storage media such as USB storage to prevent theft, improper removal from the premises, etc.?</td>
<td>□</td>
</tr>
<tr>
<td>9-2</td>
<td>When disposing of information devices or storage media, does the organization confirm that important information has been completely deleted?</td>
<td>□</td>
</tr>
<tr>
<td>10</td>
<td>When mobile devices and portable storage media are taken from the premises, does the organization manage the approval, recording, etc. of the removal?</td>
<td>□</td>
</tr>
<tr>
<td>11</td>
<td>Does the organization restrict employees' bringing in and using personal mobile devices and storage media for work?</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

**Technological and Operational Management**

<table>
<thead>
<tr>
<th>No</th>
<th>Content</th>
<th>Immediate division</th>
<th>Information Systems Division</th>
<th>General Affairs Division</th>
<th>Personnel Division</th>
<th>Legal Affairs and Intellectual Property Divisions</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Does the organization restrict the use of file sharing software, SNS, external online storage, etc. on its networks, to prevent improper removal of important information?</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13-1</td>
<td>Does the organization manage the transfer of important information to contractors or other parties concerned, at all steps from transfer to disposal?</td>
<td>□</td>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13-2</td>
<td>Does the organization take into account the mistaken transfer of important information to persons other than the parties concerned via the Internet or otherwise outside the organization, and protect the important information using encryption, etc.?</td>
<td>□</td>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Does the organization limit the important information that can be used and handled outside the organization, and protect important information and information devices?</td>
<td>□</td>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Does the organization take into account the surrounding environment, network environment, etc. when performing work using important information outside the organization?</td>
<td>□</td>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Does the organization determine which information may be handled via services provided by third parties and which may not, confirm and agree on the services prior</td>
<td>□</td>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Content</td>
<td>Check items</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>---------</td>
<td>-------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Immediate division</td>
<td>Related divisions</td>
<td>Legal Affairs and Intellectual Property Divisions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Systems Division</td>
<td>General Affairs Division</td>
<td>Personnel Division</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Does the organization safely protect logs and trails for a fixed period, including the history of access to important information and users' operation history?</td>
<td>[ ]</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Does the organization not only record and store logs and trails of the access history, operation history, etc. of system administrators, but also have the content of these periodically checked by persons other than system administrators?</td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19-1</td>
<td>Does the organization provide education for all the officers and employees, and disseminate policies concerning the organization's internal impropriety countermeasures, procedures for handling important information, etc.?</td>
<td>□</td>
<td>[ ]</td>
<td>[ ]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19-2</td>
<td>Does the organization periodically repeat its education, and periodically review and update its content?</td>
<td>□</td>
<td>[ ]</td>
<td>[ ]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>At the conclusion of employment, does the organization require employees to submit written pledges imposing confidentiality obligations? (recommended)</td>
<td>□</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>At the conclusion of employment or work contracts, does the organization have employees and contractors return or completely delete all information assets which they were entrusted to handle, and does the organization delete their user IDs and privileges from information systems?</td>
<td>□</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Has the organization prepared rules of employment and other internal rules, and made provisions for official disciplinary proceedings?</td>
<td>□</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>In order to make obligations to protect important information understood by officers and employees, does the organization request them to submit written pledges of confidentiality etc.?</td>
<td>□</td>
<td>[ ]</td>
<td>[ ]</td>
<td>[ ]</td>
<td></td>
</tr>
</tbody>
</table>

■ Securing Evidence

■ Human Management

■ Compliance

■ Workplace Environments
<table>
<thead>
<tr>
<th>No</th>
<th>Content</th>
<th>Immediate division</th>
<th>Related divisions</th>
<th>Check items</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Information Systems Division</td>
<td>General Affairs Division</td>
<td>Personnel Division</td>
</tr>
<tr>
<td>24</td>
<td>Does the organization promote impartial and objective personnel and performance evaluations as well as provide opportunities to explain how evaluation is carried out in personnel and performance evaluations? (recommended)</td>
<td></td>
<td>[ ]</td>
<td>□</td>
</tr>
<tr>
<td>25</td>
<td>Does the organization as a whole promote environments that maintain good communication throughout the workplace, such as by preparing systems for promoting mutual work support and environments facilitating consultation, while also preparing suitable work environments through means such as normalization of workloads and working hours? (recommended)</td>
<td>□</td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>Does the organization restrict independent work apart from other employees in environments that disallow mutual monitoring, and has the organization set necessary procedures for prior approval for independent work? (recommended)</td>
<td>□</td>
<td>[ ]</td>
<td>[ ]</td>
</tr>
<tr>
<td></td>
<td><strong>Follow-up Measures</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>In order to identify the scope of the effects of internal improprieties, organizations must assess the concrete status of incidents and must implement measures to minimize damage and prevent the spread of effects. In addition, organizations must secure systems for cooperation with parties concerned inside and outside the organization, as required. Does the organization do so?</td>
<td>□</td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Has the organization considered punishment for perpetrators of international improprieties, and has the organization considered providing notification of cases of internal improprieties within the organization?</td>
<td>□</td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Organizational Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Has the organization prepared whistleblower systems for the occurrence of incidents suspected of involving internal improprieties, has it established multiple points of contact, and does it secure anonymity for whistleblowers, as required?</td>
<td>□</td>
<td>[ ]</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>Content</td>
<td>Check items</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Does the organization identify internal impropriety countermeasure items, conduct checks (including internal and other audits), report the checked results to the top manager, and conduct reviews of countermeasures, as required?</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related divisions</th>
<th>Immediate division</th>
<th>Information Systems Division</th>
<th>General Affairs Division</th>
<th>Personnel Division</th>
<th>Legal Affairs and Intellectual Property Divisions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>□</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[ ]
Appendix III: Q&A

Q&A for assisting countermeasures (1)

Q-1. The company does not know how basic policies should be formulated. (4-1 (1)) (4-1(2))

A-1. The basic policies shown in these Guidelines assume the use of existing basic information security policies. If necessary, items concerning internal impropriety countermeasures should be added. Below are minimum items for the organizations having no basic information security policy.

In their basic policies, companies should set the following 3 items at the minimum, from the standpoints of thoroughly conducting protection and management of important information within the company, and of external accountability.

1. The top manager shall recognize the need to conduct risk management as a management issue, and as a component of this, shall prevent internal improprieties and shall show the importance of protecting and managing important information.

2. Basic policies shall identify important information that should be protected and managed, and shall indicate the business importance of this important information. Important information is the information which has considerable effects on the business of the company or group. Examples include manufacturing and development information or sales information, including strategic information and undisclosed intellectual property. Shared information obtained from parties concerned that are obligated to perform management of confidentiality is also included.

3. Basic policies shall show implementation systems for the protection and management of important information, and while conducting reviews shall show that activities are ongoing. Implementation systems are to note systems that should be prepared in implementing internal impropriety countermeasures. The minimally responsible person must be indicated. Moreover, activities for improving countermeasures on an ongoing basis are to be shown.

For details, see the examples of basic policies in Appendix V.

The systems noted in basic policies assume a division into large-scale and small-scale companies, each with two types of systems. An overview of systems is described using the figure below.

In large-scale companies, a system with the top manager as the CEO and the CISO as the Supervising Manager (hypothetical example 1), and a system with the CISO as the CEO and the information systems division head as the Supervising Manager (hypothetical example 2), are assumed. In small-scale companies, a system with the top manager as the CEO and the CISO as the Supervising Manager (hypothetical example 3), and a system with the top manager as both CEO and Supervising Manager (hypothetical example 4), are assumed.
### Q&A for assisting countermeasures (2)

<table>
<thead>
<tr>
<th>Q-2. The company does not know how to categorize important information. (4-1 (1))</th>
<th>A-2. First, information can be divided into two according to whether it is subject to protection. Information subject to protection should be managed with the organization setting rules for its handling. In actual work, when there is a need to change handling according to differences in the degree of importance of information subject to protection, the number of categories for managing the information can be increased. However, as too many categories can complicate management, about four categories are advisable.</th>
</tr>
</thead>
</table>

### Q&A for assisting countermeasures (3)

<table>
<thead>
<tr>
<th>Q-3. The company does not know what sort of information comes under important information. (4-1 (1))</th>
<th>A-3. Important information varies according to the work content and the information handled by divisions. As an example, for the sales division this includes customer data and sales information restricted to parties concerned. In the case of the development division, important information may include developed item and specifications/design documents. In general, important information can be considered to be information that has an effect on the profits of the organization. However, the sharing of important information with parties concerned outside the organization is connected to profits in some cases, and varied handling and scopes of sharing can be imagined, depending on the work and status of the supervising divisions. Moreover, degree of importance varies with time for some information, with a high degree of importance until a certain period, after which the information becomes public knowledge.</th>
</tr>
</thead>
</table>

### Q&A for assisting countermeasures (4)

<table>
<thead>
<tr>
<th>Q-4. The company does not know how to set user-managed password rules that prevent the use of simple character strings. (4-2-2 (7))</th>
<th>A-4. A simple character string is password that is the same as the user ID, is a personal name or birthday, or is a keyboard array (such as &quot;123456&quot; or &quot;QWERTYU&quot;). To avoid users setting such simple character strings as passwords, organizations should set rules such as eight or more characters, with a mixture of upper-case and lower-case letters.</th>
</tr>
</thead>
</table>
Q&A for assisting countermeasures (5)

<table>
<thead>
<tr>
<th>Q-5. The company does not know how it should strengthen security for physical divisions that handle important information. (4-3 (8))</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-5. Organizations should restrict the persons who can enter physical divisions (company grounds, buildings, rooms, etc.) that handle important information, and should be able to identify targeted persons. Organizations should also record workplace or room entry/exit, and should appropriately manage and regularly and irregularly check the records. It is advisable to install equipment for automatically recording those histories, but when the installation or placement of such equipment is difficult, organizations should record workplace or room entry/exit history on their own, and then appropriately manage and regularly and irregularly check the records. It is important that the workplace or room entry/exit history not be viewable by other persons entering or existing. With regard to IC cards which are used to enter or lock the physical divisions that handle important information, organizations must consider items such as the following.</td>
</tr>
<tr>
<td>(1) Operation and management of keys and IC cards</td>
</tr>
<tr>
<td>• Organizations are to prohibit the loaning of keys and IC cards among officers and employees and keep records of the loaning and return of keys and IC cards under the confirmation of the responsible manager (the person in charge of the physical divisions).</td>
</tr>
<tr>
<td>• For &quot;dimple keys&quot; and cards etc., organizations are to use keys and IC cards that are hard to duplicate.</td>
</tr>
<tr>
<td>• When keys and IC cards have become unnecessary due to transfer, retirement, etc., organizations are to make sure that the keys and IC cards are returned.</td>
</tr>
<tr>
<td>• Organizations are to establish procedures (i.e., create manuals) for the loss of keys and IC cards, along with measures that can be taken immediately to invalidate lost keys and IC cards.</td>
</tr>
<tr>
<td>• Organizations are to carry out regular and irregular (i.e., surprise) checks of key/IC card possession, targeting persons to whom keys and IC cards are lent.</td>
</tr>
<tr>
<td>• Spare keys are not to be stored together with information identifying the keys' place of use.</td>
</tr>
<tr>
<td>• Information identifying the place of use of a spare key with a given key number is to be handled as important information.</td>
</tr>
<tr>
<td>(2) Confirmation of entry/exit history</td>
</tr>
<tr>
<td>• Organizations are to carry out regular and irregular checks of entry/exit records (including camera images) and make sure that the key operators (the owners of the IC cards) and those who actually entered and left the physical division are identical.</td>
</tr>
<tr>
<td>• Organizations are to carry out regular and irregular checks of entry information and exit information that are obtained through entry/exit management, so that they can detect unnatural points.</td>
</tr>
<tr>
<td>(3) Others</td>
</tr>
<tr>
<td>• Organizations are to use cameras, etc. to monitor activities within physical divisions handling important information, and are to communicate the fact of the monitoring.</td>
</tr>
<tr>
<td>• Organizations are to consider installing automatic security systems etc. so that an intrusion through an intentionally-unlocked window etc. is detected.</td>
</tr>
<tr>
<td>• Organizations are to establish rules for special exemptions, including emergency entry or entry by the people not supposed to enter (e.g., top managers, persons with special privilege).</td>
</tr>
</tbody>
</table>

Q&A for assisting countermeasures (6)

<table>
<thead>
<tr>
<th>Q-6. The company does not know how to set procedures for the handling (transfer) of important information. (4-4 (13))</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-6. Procedures for the handling (transfer) of important information, if via a network, differ depending on whether e-mail or online storage is used. As an example, if an organization uses e-mail and assumes the sending of important information as</td>
</tr>
</tbody>
</table>
attachments, the organization should establish rules such as always attaching important information in encrypted format, and using telephones or other measures other than e-mail for the decryption password.

If the organization uses online storage, it must consider whether to limit the use of online storage to only that arranged by the organization. In that case, the organization is to establish rules such as the period during which download is possible, and the transfer of passwords when downloading. Moreover, when the organization uses an Internet-based online storage service, assuming that the service does not allow download by anyone, the organization is to establish rules such as always encrypting important information to be uploaded, and never sending the download destination and password in the same e-mail message.

Q&A for assisting countermeasures (7)

Q-7. The company does not know what content to include in education. (4-6 (19))

A-7. In education, organizations should include content that heightens understanding and awareness concerning internal impropriety countermeasures, such as the following.

1. Describe specific case studies of the effects on the company or organization caused by internal improprieties.
2. Describe matters that should be followed concerning categories and management methods of important information indicated in operation regulations. Examples include rules to prevent faxes, printouts, and other documents recording confidential information from being left unattended for a long time, and reporting procedures in the event of detection of internal improprieties.
3. Describe disciplinary actions in the event of discovery of internal improprieties, based on company regulations and other internal rules. As an example, it is effective to describe the content of disciplinary actions for internal improprieties based on specific cases.
4. Explain that countermeasures are being implemented, while indicating management methods for important information. As an example, with regard to the content of countermeasures, it is effective to explain that monitoring, etc. of e-mail archives, etc. is being conducted.
5. To deepen understanding of internal impropriety countermeasures, it is advisable to explain related laws and regulations (the Unfair Competition Prevention Act, the Personal Information Protection Act, etc.) that form the background to operation regulations.

Q&A for assisting countermeasures (8)

Q-8. What sort of information assets are there for which handling is entrusted, and what sort of privileges are granted? (4-6 (21))

A-8. Information assets for which handling is entrusted include the following information and hardware.

1. Important information
   - Customer data (including information not generally disclosed, such as information concerning purchasing and sales)
   - Information concerning the creation of program source code, design drawings, etc.
   - Information concerning information systems (information system configuration information, etc.)
   - Information concerning undisclosed intellectual property (i.e., patents) held by the company

2. Hardware
   - PCs (including laptop PCs), smartphones loaned by the company, CD-ROMs, DVD-ROMs, USB storage, etc.

3. Privileges granted
   - Entry passes
   - User IDs (and associated passwords)
   - Storage repository (safes, wagons, cabinets, etc.) keys
Appendix IV: Relationship with Other Guidelines, etc.

(1) JIS Q 27001 Supplementary Notes A

These Guidelines indicate measures for organizations to take in protecting information assets from internal improprieties. Information security management aims to maintain the confidentiality, integrity, and availability of information assets that should be protected by the organization, and contains many related items from the standpoint of protecting information assets. As such, for the reference of persons reading these Guidelines from the standpoint of information security management, the management measures of JIS Q 27001 Supplementary Notes A, which relate to the management measures of these Guidelines, are shown below. Note that as for "Workplace Environments" in these Guidelines, there are no corresponding JIS Q 27001 management measures.

<table>
<thead>
<tr>
<th>Major item</th>
<th>Item name</th>
<th>JIS Q 27001 Supplementary Notes A Related Items</th>
</tr>
</thead>
</table>
| Basic Policies                | (1) Clarification of the Responsibilities of the Top Manager              | A.5.1 Information security policy  
A.6.1 Internal organization  
A.6.2 External parties     |
|                               | (2) Appointment of the Supervising Manager and Construction of Cross-Organization Systems | A.5.1 Information security policy  
A.6.1 Internal organization  
A.6.2 External parties     |
| Designation as Confidential   | (3) Information Rating Categories                                         | A.7.1 Asset management  
A.7.2 Information classification  
A.11.1 Business requirement for access control |
| (4) The Application and Labeling of Rating Categories |                                                                            | A.7.1 Asset management  
A.7.2 Information classification  
A.11.1 Business requirement for access control |
| Asset Management              | (5) User Access Management in Information Systems                          | A.7.1 Asset management  
A.7.2 Information classification  
A.8.3 Termination or change employment  
A.11.1 Business requirements for access control  
A.11.2 User access management  
A.11.3 User responsibilities |
| Designation of access rights  | (6) Rights Management for System Administrators                            | A.7.1 Asset management  
A.7.2 Information classification  
A.11.2 User access management  
A.11.3 User responsibility     |
|                               | (7) Identification and Authentication of Users in Information Systems      | A.7.1 Asset management  
A.7.2 Information classification  
A.11.2 User access management  
A.11.3 Users responsibilities |
| Physical Management           | (8) Physical Protection and Entry/Exit Management                         | A.9.1 Secure areas  
A.10.1 Operation procedures and responsibilities  
A.11.3 User responsibilities |
|                               | (9) Asset management and physical protection of information devices and storage media | A.9.2 Equipment Security |
|                               | (10) Management and Monitoring of the Removal of Information Devices and Storage Media from the Premises | A.9.2 Equipment Security  
A.10.1 Operation procedures and responsibilities  
A.10.7 Media handling  
A.10.8 Exchange of information |
<table>
<thead>
<tr>
<th>Major Item</th>
<th>Item name</th>
<th>JIS Q 27001 Supplementary Notes A Related Items</th>
</tr>
</thead>
</table>
| (11) Restrictions on Bringing in and using Personal Information Devices and Storage Media for Work | | A.9.2 Equipment security  
A.10.1 Operation procedures and responsibilities  
A.10.4 Protection against malicious and mobile code  
A.10.7 Media handling  
A.10.8 Exchange of information |
<table>
<thead>
<tr>
<th>Major Item</th>
<th>Item name</th>
<th>JIS Q 27001 Supplementary Notes A Related Items</th>
</tr>
</thead>
</table>
| Technological and Operational Management       | (12) Safety Management for Network Usage                                   | A.10.1 Operation procedures and responsibilities  
A.10.4 Protection against malicious and mobile code  
A.10.6 Network security management  
A.11.4 Network access control  
A.12 Information systems acquisition, development, and maintenance |
|                                                | (13) Transfer and Protection of Important Information                     | A.10.7 Media handling  
A.10.8 Exchange of information  
A.12.3 Cryptographic controls |
|                                                | (14) Protection of Information Devices and Storage Media taken from the Premises | A.11.5 Operating system access control  
A.11.6 Application and information access control  
A.11.7 Mobile computing and Teleworking  
A.12.3 Cryptographic controls |
|                                                | (15) Protection of Important Information in Work Outside of the Organization | A.10.4 Protection against malicious and mobile code  
A.10.7 Media handling  
A.11.5 Operating system access control  
A.11.6 Application and information access control  
A.11.7 Mobile computing and Teleworking  
A.12.3 Cryptographic controls |
|                                                | (16) Confirmations when Using Services Provided by Third Parties (Including Cloud Computing) | A.6.2 External parties  
A.10.2 Third party service delivery management  
A.11.6 Application and information access control  
A.10.8 Exchange of information |
| Securing Evidence                              | (17) Recording and Storage of Logs and Trails in Information Systems      | A.10.10 Monitoring |
|                                                | (18) Checking of System Administrators' Logs and Trails                   | A.10.10 Monitoring |
| Human Management                               | (19) Dissemination of Internal Impropriety Countermeasures through Education | A.8.1 Prior to employment  
A.8.2 During employment  
A.8.3 Termination or change of employment  
A.15.1 Compliance with legal requirements |
|                                                | (20) Personnel Procedures for Conclusion of Employment                    | A.8.2 During employment  
A.8.3 Termination or change of employment  
A.15.1 Compliance with legal requirements |
|                                                | (21) Return of Information Assets Due to Conclusion of Employment or Conclusion of Contract | A.8.2 During employment  
A.8.3 Termination or change of employment  
A.15.1 Compliance with legal requirements |
| Compliance                                     | (22) Preparation of Legal Proceedings                                     | A.8.1 Prior to employment  
A.8.2 During of employment  
A.8.3 Termination or change of employment  
A.15.1 Compliance with legal requirements |
|                                                | (23) Requests for Written Pledges                                         | A.6.1 Internal organization  
A.8.1 Prior to employment  
A.8.2 During of employment  
A.8.3 Termination or change of employment  
A.15.1 Compliance with legal requirements |
<table>
<thead>
<tr>
<th>Major Item</th>
<th>Item name</th>
<th>JIS Q 27001 Supplementary Notes A Related Items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workplace Environments</td>
<td>(24) Preparation of Impartial Personnel Evaluations</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>(25) Promotion of Reasonable Work Environments and Communication</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>(26) Management in Workplace Environments</td>
<td>-</td>
</tr>
<tr>
<td>Major Item</td>
<td>Item name</td>
<td>JIS Q 27001 Supplementary Notes A Related Items</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Organizational management</td>
<td>(29) Preparation of Whistleblower Systems for Internal Improprieties</td>
<td>A.13.1 Reporting information security events and weaknesses, A.13.2 Management of information security incidents and improvements</td>
</tr>
<tr>
<td></td>
<td>(30) Implementing Checks Incorporating the Prevention of Internal Improprieties</td>
<td>A.10.10 Monitoring</td>
</tr>
</tbody>
</table>
(2) Directives for Management of Trade Secrets

The Directives for Management of Trade Secrets introduce advisable management methods for securing protection for information, primarily as trade secrets under the Unfair Competition Prevention Act. These Guidelines also cover management methods that are adapted to most recent changes in circumstances and are not covered by the Directives for Management of Trade Secrets, and which should provide helpful reference. When referring to these Guidelines, freely refer to the “Points of Countermeasures” items below that concern the management of trade secrets. However, as these Guidelines contain portions that indicate advanced countermeasures, from the standpoint of the Directives for Management of Trade Secrets it is not necessary to respond to all of the countermeasures.

<table>
<thead>
<tr>
<th>Major item</th>
<th>Item name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-2-2 Designation of access rights</td>
<td>(5) User Access Management in Information Systems</td>
</tr>
<tr>
<td></td>
<td>(6) Rights Management for System Administrators</td>
</tr>
<tr>
<td></td>
<td>(7) Identification and Authentication of Users in Information Systems</td>
</tr>
<tr>
<td>4-3 Physical Management</td>
<td>(8) Physical Protection and Entry/Exit Management</td>
</tr>
<tr>
<td></td>
<td>(9) Asset Management and Physical Protection of Information Devices and Storage Media</td>
</tr>
<tr>
<td></td>
<td>(10) Management and Monitoring of the Removal of Information Devices and Storage Media from the Premises</td>
</tr>
<tr>
<td></td>
<td>(11) Restrictions on Bringing in and Using Personal Information Devices and Storage Media for Work</td>
</tr>
<tr>
<td>4-4 Technological and Operational Management</td>
<td>(12) Safety Management for Network Usage</td>
</tr>
<tr>
<td></td>
<td>(13) Transfer and Protection of Important Information</td>
</tr>
<tr>
<td></td>
<td>(14) Protection of Information Devices and Storage Media taken from the Premises</td>
</tr>
<tr>
<td></td>
<td>(15) Protection of Important Information in Work Outside of the Organization</td>
</tr>
<tr>
<td></td>
<td>(16) Confirmations when Using Services Provided by Third Parties (Including Cloud Computing)</td>
</tr>
<tr>
<td>4-5 Securing Evidence</td>
<td>(17) Recording and Storage of Logs and Trails in Information Systems</td>
</tr>
<tr>
<td></td>
<td>(18) Checking of System Administrators' Logs and Trails</td>
</tr>
</tbody>
</table>

Moreover, the following items should provide helpful reference from the standpoint of preventing the leakage of trade secrets by insiders. Refer to them as necessary.

<table>
<thead>
<tr>
<th>Major item</th>
<th>Item name</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-8 Workplace Environments</td>
<td>(24) Preparation of Impartial Personnel Evaluations</td>
</tr>
<tr>
<td></td>
<td>(25) Promotion of Reasonable Work Environments and Communication</td>
</tr>
<tr>
<td></td>
<td>(26) Management in Workplace Environments</td>
</tr>
<tr>
<td>4-9 Follow-up Measures</td>
<td>(27) Preparation of Systems Required for Follow-up Measures</td>
</tr>
<tr>
<td></td>
<td>(28) Consideration of Punishment and Prevention of Recurrence</td>
</tr>
<tr>
<td>4-10 Organizational Management</td>
<td>(29) Preparation of Whistleblower Systems for Internal Improprieties</td>
</tr>
<tr>
<td></td>
<td>(30) Implementing Checks Incorporating the Prevention of Internal Improprieties</td>
</tr>
</tbody>
</table>
(3) The Guidelines for Economic and Industrial Sectors Concerning the Act on the Protection of Personal Information

The Guidelines for Economic and Industrial Sectors Concerning the Act on the Protection of Personal Information indicate necessary and appropriate safety management methods required by the Act on the Protection of Personal Information. With regard to the improper removal of personal information from the premises by employees, the "Workplace Environments" section from these Guidelines offers items not found in the Guidelines for Economic and Industrial Sectors Concerning the Act on the Protection of Personal Information. Referring to "Points for Countermeasures" under "Workplace Environments" should be of aid in strengthening measures against the improper removal of personal information from the premises.
Appendix V: Examples of Basic Policies

Examples of basic policies are indicated below. Add to and modify these for use as required.

Examples of Basic Policies

1. Significance of internal impropriety countermeasures
   These basic policies (hereinafter "these Policies") are hereby established for the purpose of protecting important information and information systems handled by ○○○ (e.g. IPA) (hereinafter "the Organization") from threats by internal improprieties, and for the purpose of establishing necessary items for safely making use of these items in business. From here out the Organization will consider internal impropriety countermeasures an important issue for management, and will undertake these.

2. Protection of important information
   These Policies designate ○○○, △△△, and □□□ (e.g. customer data) as important information to be protected by the Organization.
   • ○○○ is ....
   • △△△ is ....
   • □□□ is ....
   • (Example: To protect the advantages of products with respect to competitors, development information must not be leaked from important manufacturing contractors.)
   The Organization will take measures appropriate to work situations with respect to this important information. The implementation of these measures will be disseminated within the Organization.

3. Implementation Systems
   The Organization sets forth roles and responsibilities in order to establish systems of organizational countermeasures for internal improprieties.
   • CEO···○○○ (e.g. president or other management team representative)
     The CEO conducting decision-making concerning internal impropriety countermeasures.
   • Supervising Manager···□□□ (e.g. president or other management team representative)
     The person responsible for deciding important matters concerning internal impropriety countermeasures, conducting checks and reviews of countermeasure status, and conducting checks of countermeasures and status when internal improprieties occur.
   * Note: ○○○ and □□□ may be identical.

3-1. Monitoring by the CEO
   The CEO sets policies for internal impropriety countermeasures, and receives and evaluates periodic reports on those policies from the Supervising Manager on an ongoing basis. The CEO also reviews implementation systems and policies as necessary.

3-2. Countermeasure implementation and reporting by the Supervising Manager
   The Supervising Manager drafts specific measures based on the CEO's policies, and periodically reports to the CEO on implementation status.

4. Review of basic policies
   In order to maintain effective and efficient internal impropriety countermeasures, these Policies are to be periodically reviewed and revised as necessary.