Technical Protection Measures for Personal Information in Each Processing Phase in the Korean Public Sector

Mina Shim[1], Seungjo Baek[1], Taehyoung Park[1], Jeongseon Seol[2] and Jongin Lim[1]
[1] Graduate School of Information Management and Security, Korea University
Anam-dong, Seongbuk-gu, Seoul 136-713 - Korea
[e-mail: {mnshim, nomadvirus, mosto2004, jilim}@korea.ac.kr]
[2] Korea Telecommunications Operators Association
44-9 Samsung-dong, Gangnam-gu, Seoul 135-090 - Korea
[e-mail: 12jss@ktoa.or.kr]
*Corresponding author: Jongin Lim

Received August 16, 2009; revised September 23, 2009; accepted October 10, 2009;
published October 30, 2009

Abstract

Personal information (hereinafter referred to as “PI”) infringement has recently emerged as a serious social problem in Korea. PI infringement in the public and private sector is common. There were 182,666 cases of PI in 2,624 public organizations during the last three years. Online infringement cases have increased. PI leakage causes moral and economic damage and is an impediment to public confidence in public organizations seeking to manage e-government and maintain open and aboveboard administration. Thus, it is an important matter. Most cases of PI leakage result from unsatisfactory management of security, errors in home page design and insufficient system protection management. Protection management, such as encryption or management of access logs should be reinforced urgently. However, it is difficult to comprehend the scope of practical technology management satisfied legislation and regulations. Substantial protective countermeasures, such as access control, certification, log management and encryption need to be established. It is hard to deal with the massive leakage of PI and its security management. Therefore, in this study, we analyzed the conditions for the technical protection measures during the processing phase of PI. In addition, we classified the standard control items of protective measures suited to public circumstances. Therefore, this study provides a standard and checklist by which staff in public organizations can protect PI via technical management activities appropriate to laws and ordinances. In addition, this can lead to more detailed and clearer instructions on how to carry out technical protection measures and to evaluate the current status.

Keywords: Personal information protection, PET, PIA, information security management

DOI: 10.3837/tiis.2009.05.008

1. Introduction

1.1 Research Background

Personal information infringement has recently emerged as a serious social problem in Korea. It is a constant problem both in the private and public sector. The extent of the damage is extremely large. There have been many cases of infringements in the public sector, such as leakage and exposure of PI through web sites, unauthorized perusal, and leakage due to careless public servants. There were 182,666 incidents of PI leakage in 2,624 public institutions from the latter half of 2006 to the first half of 2008, based on parliamentary inspection of the administration conducted in 2008. Online infringement cases are constantly increasing [1]. Leakage of PI causes psychological and economic damage to data subjects. At the same time, it acts as a key obstacle to e-government and a government information sharing system seeking administrative transparency and public confidence and thus it is important to address the problem. In particular, the fact that government offices share PI, amounting to 64 million via CDs in Korea is evidence of the huge impact of careless PI management. Most of the incidents involving leakage or exposure of PI are caused by insufficient security management, design errors in web sites, inadequate system protection measures, and excessive perusal of PI. Strengthening protection measures, such as encryption, access controls, and log management, are extremely important. However, since there are many views on what the scope of legal protection should be, as well as declarative regulations, without stating detailed technical measures it is not easy for those in charge of protecting PI to decide the scope of technical protection measures that must be complied with. It is difficult to have a clear understanding of the standard of compulsory obligations, such as access control, authentication, log management, and encryption, as well as the scope of possibilities. Most Korean public servants charged with managing PI are facing this kind of difficulty. They demand the development of standards and checklists for more detailed and clearer instructions on how to carry out technical protection measures and to evaluate the current status.

1.2 Research Method

Several characteristics distinguish Korea’s public sector from that of other countries. These characteristics demand more diverse and more specific measures for technical protection of PI processed in the public institutions of Korea. As a prime example, the level of implementation of e-government in Korea is higher than any other country. The government has implemented various online administrative services to build a service-oriented government that can be accessed to the general public, anywhere and anytime. It is striving to unify its administrative service systems [2]. Many public institutions have of late been processing PI online via various means, such as the Web, to carry out tasks and provide public services. The scope and amount of information sharing amongst agencies through the government information sharing system is expanding. One task faced at this point in time is to prepare for the implementation of such information sharing. The responsibility of those in charge of protection of PI is to establish administrative, physical, and technological protection plans required by national policies and laws. They must then perform appropriate protection measures. Therefore, "technical protection measures and checklists" for carrying out appropriate protection measures were developed along with a list of questions in this research. In particular, the appropriate scope and protection measures of technical protection regulations required by

Korean laws were categorized into protection items and specific requirements. Each of the protection items and specific requirements were developed in the form of appropriate questions. These provided a list of questions addressing technical protection measures.

Additionally, PI protection technologies that can currently be utilized were broken into separate elements and linked with each of the protection items presented in order to improve the level of understanding on protection activities. This enables the establishment of more practical protection plans and their implementation.

2. Analysis of Personal Information Protection Laws and Regulations for Public Institutions in Korea

2.1 The Current Status of the Personal Information Protection Policy

In Korea, in response to the recent surge of PI infringement incidents, systematic plans including "measures to strengthen the protection of PI by public institutions" and "development of a mid- and long-term road map", to protect PI in both private and public sectors, were announced. Work being conducted on a policy to strengthen the protection of PI, or necessary conditions, which are centered on the public sector, enable us to understand the overall technical protection measure requirements that the public sector is demanding, before considering relevant laws and guidelines. Pertinent policies over the past two or three years have strongly recommended inspection of PI leakage via web sites and introduction of a countermeasure system, and call for a PI management system that operates both before and after an incident.

"Measures to strengthen protection of PI at public institutions", a policy announced in September, 2007, presented technical requirements to strengthen protection of PI in public institutions, under the name of "technical countermeasures and strengthening of the infrastructure". It strongly recommended: constant monitoring of public institution web sites and consulting, use of a method that replaces the use of resident registration numbers online, filtering programs, PI filtering programs and secure servers. It strongly recommended the introduction and use of techniques for web sites of public institutions, such as PI exposure checks, agent-based automatic countermeasure systems, and integrated ID management systems. It calls for these PI protection technologies as part of PI protection activities. A "Level Measurement index for the protection of PI at public institutions", which was developed at the same time, is an objective standard for improving the level of protection of PI at public institutions and for the promotion pertinent work performance at institutions. The technical protection measure measurement index and items included in the "technical security" and "physical security" at the level of "laying out the groundwork" demands various technical protection measures and the necessary technologies. They included: management and logging of technical access control of the PI processing system (system access privilege management and monitoring); management of assessment of vulnerabilities; management of encrypted communication; and management of encryption. "Development of a mid- and long-term road map for protection of PI at public institutions", announced in December, 2007, is composed of a total of five areas and 24 specific tasks. In particular, a task to advance PI protection technologies in the "advancing technology" area is included. It specifically refers to establishment of an inspection system for protection technology for the public sector, regular assessment of the level of PI protection technologies by collaboration between government and non-government bodies, and a support system to advance PI protection technologies. These require: PI leak checking and analysis, web site monitoring, operation and management of inspection system before and after the leak of PI, and the necessary technologies. Such recent technical PI protection policies of public institutions can be confirmed based on their detailed legal grounds by analyzing Korean laws, regulations and guidelines.

2.2 Legal Requirements for Personal Information Protection for Public Institutions in Korean Laws and Regulations

2.2.1 Provisions for Technical Protection Measures at Each Phase of Processing Personal Information in Related Laws and Regulations

Laws and regulations on PI protection in Korea are broadly classified based on public and private perspectives: protection of PI that is included in the records that the government manages; and protection of consumer information. The requirements of technical measures to protect PI include general technical measures and specific technical measures based on the characteristics of the public sector. Therefore, we analyzed these laws, regulations, guidelines and manuals and the technical protection requirements derived from them. Other related guidelines and manuals were analyzed and technical protection requirements were discovered [3]. Clauses and key factors required by laws and regulations and guidelines based on each processing phase are included in **Appendix 1** and **Appendix 2**.

Table 1. The Legislation, Guidelines and Manuals Related to the Government Record and Customers' Viewpoint

Item		Name
Laws and Regulations	**Public Sector**	A. Laws/execution ordinance/enforcement regulations related to protection of personal information at public institutions B. E-government laws/execution ordinance C. Resident registration law/execution ordinance D. Vehicle management law/execution ordinance E. Statistics Law F. National Public Service Law
	Private Sector	G. Act on Promotion of Information and Communication Network Utilization and information Protection, etc. H. Use and Protection of Credit Information Act I. Act on Real Name Financial Transactions and Guarantee of Secrecy
Guidelines and Manuals		K. Personal information protection guidelines (Korea Communications Commission notice issue 2008-2) L. Technical and managerial protection measure standards for personal information (Korea Communications Commission notice issue 2008-3) M. Personal information management work manual for public institutions N. Installation and operation guidelines for CCTV at public institutions for protection of information O. CCTV management guidelines at public institutions P. Biometric information protection guidelines Q. CCTV personal image data protection guidelines R. RFID privacy protection guidelines S. Administrative institution information system access privilege management regulations T. Guidelines for evaluation of effects of personal information at private institutions U. Basic guidelines for personal information protection at public institutions

Clauses that require technical protection measures at each processing phase of PI in Korea in the public sector were chosen from the laws, regulations and guidelines analyzed. The four phases for processing PI are: collection, storage and retention, use and provision and destruction. The current phase is determined by the general life cycle. The legal grounds of technical protection measures required by each processing phase were separately organized into particular requirements linked to PI protection technologies. They were used as a basis to develop technical protection standards and checklists.

The four notable types of technical measures to protect PI are: encryption, access control, privilege management, and authentication. Specific requirements for encryption include: encryption to prevent alteration, leak, and illegal use of PI; encryption for secure storage and transmission of PI; RFID; encryption for PI in collection, storage, and provision phase, which involves new technologies such as RFID, biometric information, and CCTV video information; encryption to prevent alteration and forgery, etc, of access records regarding PI. Specific requirements for access control include: backup and data isolation, programs, etc, which have PI recorded on them; implementing firewalls; installing and operating access control devices, such as intrusion prevention systems; storage of access logs about PI; and checking access logs and saving logs to confirm access records and supervision. Specific requirements for privilege management include: assigning and managing privileges for access control; access control for third parties, such as maintenance companies and outsourcing companies. Finally, specific requirements for authentication include: use of public certificates and administrative e-signed certificates; use of more secure authentication methods, such as two-factor authentication. These are the most representative ones, but various other detailed measures are included. The most noteworthy protection measures of the four types are extremely important, especially as prerequisite items for public institutions. They are at the heart of the development of protection standards and checklists as research findings. The analysis process is detailed in Section 2.2.2.

2.2.2 Implications of Technical Measures for Protecting Personal Information in Each Processing Phase

Specific technical protection measures for each phase of processing PI, which were found through analysis of relevant laws and regulations, serve as important directions in finding specific requirements of protection standards. The most important parts of the protection measures are: clauses that align with the "principle of collection limitation, purpose specification, security safeguards, etc.", which are prescribed as declarative/compulsory in key principles and guidelines of PI protection, such as the eight principles from “the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” and for the most part are reflected in Korean laws and regulations. However, there is no need to link all requisites with possible techniques - only when technical measures are best. Therefore, this study was conducted with managerial/physical protection requirements excluded from technical protection measures in each processing phase.

- **Technical Protection Measures in Personal Information Collection Phase**

The most emphasized regulations in the collection phase are "minimization of PI collection" and "notification and acquisition of consent". These are the most important requirements to prevent or minimize infringement of PI. However, these two requirements are currently being enforced by managerial and procedural approaches rather than technical measures. That is, when collection occurs by entering PI online, unless there is a technical program in place that checks whether the PI entered is relevant to the scope of the service being provided, the realization will inevitably be difficult. However, for notification or obtaining consent, since the specifics can be shown on the computer screen by a program, etc, they may fall under the category of technical measures. However, notification or obtaining consent via screen output is a technique that falls under the operation and management of PI policy; thus, they were excluded from the technical protection measures category. Notification or obtaining consent is excluded, not only in the collection phase, but in other phases as well.

Therefore, the major items that fall under technical protection measures, among the laws and regulations required in the collection phases, are as follows: secure authentication of user identity; control when entering PI; safety of PI transmitted during collection. In particular, PI collected via public services must have secure identification of the user as a prerequisite. In consideration of the seriousness of illegal usage of resident registration numbers, alternatives to using resident registration numbers, authentication by e-signing, and protection of resident registration number for the purpose of confirming real names must be included. In addition, control of personal image data and biometric information is included, when CCTV, RFID or biometrics are used.

Mandatory protection measures in the PI collection phase generally focus on managerial obligations of administrative agencies. Therefore, technical protection measures that are clearly required are simply stated as "measures for securing safety against alteration/leakage or illegal use", "appropriateness of measures that secure safety of PI"[1] and "measures against infringement of PI of persons that transmitted electronic documents"[2], without dealing with specifics. Some guidebooks/manuals, require technical protection measures, such as "whether to encrypt when collecting biometric information"[3] and "establishment of protection measures such as encryption when online transactions or civil appeal applications, etc, are unavoidable"[4], but they stop at encryption of PI.

- **Technical Protection Measures in Personal Information Storage and Retention Phase**

In the PI storage and retention phase, not only managerial protection measures but also physical/technical protection measures are required. Physical protection measures include establishment of protection areas according to "protection work regulations" and study of crime prevention in computing labs. These and other representative measures are excluded from technical protection standards. Protection measures to prevent against leakage of documents are needed for the output data with PI, along with managerial/physical protection measures.[5] Also, it is prescribed that data, programs, etc, with PI should be stored in separate storage devices and kept in an isolated facility.[6] Along with this, regulations on technical protection measures in the retention phase are extremely specific compared to the collection phase. According to the regulations, every measure, such as construction of a closed network and installation of a firewall for the protection of back-up systems should be considered.[7] In addition, the handling of collected PI is more clearly defined,[8] and "installation/operation of access control systems, such as intrusion prevention systems" and "measures against prevention of alteration/forgery of access logs", are regulated. Also, it is compulsory for telecommunication providers to have technical protection measures, such as installation/operation of access control systems, [9] "store access logs and regularly confirm/supervise", and "back up access logs in separate storage devices so that they don't get altered/forged". Encryption PI of users is made as a rule.[10]

Technical protection measures in PI storage and retention include: encryption of PI file and DB encryption, secure management of backup files and databases, access control of stored PI and logging and secure management of log files.

[1] "Act on the Protection of Personal Information Maintained by Public Agencies" article 9, clause 2, " Enforcement Decree " article 5, clause 6

[2] " Enforcement Decree of e-government Act" article 6, clause 3

[3] "Handbook of biometric information protection guidelines" checklist 4.1

[4] "Manual of management tasks related to personal information for public agencies" III. 1-1

[5] "Enforcement Regulations of Act on the Protection of Personal Information Maintained by Public Agencies " article 4 clause 1, article 4 clause 2, article 5 clause 2

[6] "Enforcement Decree of the Resident Registration Act" article 10

[7] "Resident Registration Act " article 28 clause 2, " Enforcement Decree" article 46 clause 4

[8] "Act on Promotion of Information and Communications Network Utilization and Information Protection, etc." article 28 clause 1

[9] "Gudelines of personal information protection(Korean Communications Commission(KCC) notice issue 2008-2)" article 17

[10] "Technical, managerial protection measure standards for personal information (KCC notice issue 2008-3)" article 4, issue 20083)"

- **Technical Protection Measures in Personal Information Usage and Provision Phase**

In the PI usage and provision phase, "purpose specification, use limitation, security safeguards" principles from the eight principles of the OECD guideline are especially stressed, with respect to relevant public institutions using and providing PI. "Act on Promotion of Information and Communications Network Utilization and Information Protection, etc" contains clearly-stated provisions pertaining to handling and protection of PI that is accessed or transmitted for usage or provision, and clearly states the following items: "access control systems"; "measures for preventing alteration/forgery of log files"; protection measures using encryption techniques, etc, that allow secure transport of PI"; and "measures against infringement using computer viruses such as installation/operation of anti-virus programs." The regulations given by the Korean Communications Commission for service providers state that protection measures that allow secure transmission of PI on networks using methods such as measures against computer viruses and encryption algorithms, should be made compulsory under this category.[11]

Generally, most of the usage and provision of PI in public institutions is conducted through a government information sharing system that uses the national administration network. Therefore, government employees are required to use government certificates through GPKI (Government PKI).[12] When transmitting government information or electronic documents that contain PI, confirmation of identification by electronic means, such as public key certificates or government certificates, should be used. However, in execution ordinances, etc, it is defined as a "government certificate and transmission method that uses a secure method that corresponds to this", so it can be said that an ambiguity exists with respect to consistency of technical protection measures.[13] In addition, related to access privilege management, authentication methods with enhanced security, such as "security tokens, smart cards, one-time passwords (OTP), biometrics", can be used along with government certificates (GPKI). Use of various methods such as ID/password in confirming the identity of a civil petitioner is made compulsory,[14] where necessary. In addition, in regards to access by employees of maintenance companies or outsourcing companies, technical protection measures are being taken through measures such as, "setting up of access period, examination of appropriateness of allowing access privileges, separation of internal network from accessible network, setting up of minimum access privileges."

That is, regulations for the usage and provision phase emphasize procedures to obtain consent from the data subject, as well as on managerial protection measures about usage and provision, while stressing technical protection measures for authentication, transmission, and access privileges. Therefore, the following need to be included as key technical protection measures: secure authentication when using and providing PI; anti-virus technology in PI processing terminals; web or C/S screen control; network access control; separation of administration network or encrypted transmission for secure online transmission; and examination of PI leakage and isolation.

- **Technical Protection Measures in Personal Information Destruction Phase**

[11] " Gudelines of personal information protection (KCC notice issue 2008-2)" aticle 17

[12] " E-government Act" article 18, clause 1, " Enforcement Decree " article 18, "administrative institution information system access privilege management regulations" article 4, "personal information management work manual for public institutions" Ⅱ. 3-4. general management work 3. management in processing stage, etc

[13] "E-government Act" article 18, clause 1, " Enforcement Decree" article 18

[14] "Administrative institution information system access privilege management regulation" article 8 clause 2, article 9 clause 1

Regulations on protection measures in the PI destruction phase fundamentally focus on managerial protection measures. They are characterized by "requirements for destruction of PI and notification of destruction of PI." Technical protection measures in this regard are only mentioned briefly, with no specific techniques stated. Examining the main content, when retention of PI becomes unnecessary after meeting the retention objective, the PI must be destroyed, and that fact needs to be notified on the web site. In addition, PI must be destroyed using a method that makes recovery impossible, and that fact needs to be notified within one month. With regards to telecommunication providers, PI needs to be destroyed when one or more of the following conditions is met: accomplishment of the objective for collecting and using PI; ending of the terms of usage; and closing of the business.[15] Also, with regards to information about official candidates, when they demand it, their PI must be destroyed.[16] In many cases, regulations on the preservation time or the need for preservation are inconsistent, for peculiarities related to requirements for destruction of PI stated by the law, as they conform to other laws.

In other related guidelines, biometric information must be made unrecoverable and destroyed, when one or more of the following is met: accomplishment of the objective of usage; termination of usage; revocation of consent; unnecessary retention. The fact that destruction occurs needs to be notified to the data subject.[17] In addition, according to the regulations, photos of an individual's personal image with the expired retention term need to be immediately erased,[18] and photos of an individual's personal image data, collected by image data processing devices need to be destroyed within 30 days of collection.[19] Furthermore, when the objectives of data collection have been accomplished, service providers need to shred/incinerate PI in paper form and erase unrecoverable electronic PI. As well, if consent for collection and usage is revoked, they need to take adequate technical measures, such as destroying PI, and need to notify data subjects that their PI has been destroyed.[20]

In addition, provisions say that the destruction of PI after it has been destroyed using an unrecoverable method must be confirmed; for printed material this involves disposal (shredding or incinerating) of PI after directly taking measures to destroy it.[21] They emphasize managerial protection measures, but also technical protection measures, such as unrecoverable destruction.

3. Personal Information Protection Technologies by Public Institutions for Each Processing Phase

The aim of the present thesis is to adjust PI protection technologies designed for different PI characteristics and for each phase in the life cycle, which are already known by previous research, to align with PI protection technologies demanded in the network environment in the public sector, according to the technical protection measures found by analysis of relevant

[15] "Act on Promotion of Information and Communications Network Utilization and Information Protection, etc." article 29

[16] "State Public Officials Act" article 19 no 3 clause 2

[17] "Guidelines of biometric information protection" article 9 clause 1, article 9 clause 2

[18] "Installation/operation guidelines for CCTV at public agencies for protection of personal information" article 13

[19] "Guidelines of CCTV personal image information protection" article 16 clause 1

[20] "Guidelines of personal information protection (KCC notice issue 2008-2)" article 19 clause 1, article 19 clause 2 issue 1, article 19 clause 2 issue 2, article 20 clause 1, article 20 clause 2

[21] "Personal information management work manual at public institutions" III. management work by processing stage 4. management in the destruction stage

laws. This is to confirm the operating environment of PI protection technologies in detail when checking the management conditions, by utilizing checklists of protection standards, to be presented in Chapter 4 by each public institution. In addition, it is to support the adoption of PI protection technologies and improvement activities. Also, the detailed technical analysis is crucial to developing appropriate technical protection measures and items and assessing the appropriateness of the measures. PI characteristic-specific technologies such as Abedelmounaam were examined in order to classify PI protection technologies into elements according to each processing phase. The subdivision method that improves upon Abedelmounaam, developed by Gi-Hyo Nam et al., was used.

3.1 Personal Information Protection Technologies Based on the Personal Information Characteristics and the Life Cycle Phase

The Abedelmounaam (2003) classification is the most widely used classification of privacy protection technologies. It categorizes internet privacy technologies into technical-based and law-based [4]. Gi-hyo Nam et al. improved on these technologies to overcome their limitations of not including various new technologies, in 2006 and 2009. This work broadly classified PI protection technologies into operational and policy/managerial technologies based on their characteristics [5]. Operational technologies refer to protection technologies used to prevent a range of privacy infringements that may occur during the phases where PI is transmitted/received and provided, and include the following: prevention technologies against PI infringement (privacy filtering technologies); technologies that check current infringement factors (privacy scanning); secure communication to guard against infringement (communication with PI protection); and storage technologies (storage technologies for protection of PI). Policy/managerial technologies refer to technologies that allow service providers to effectively describe PI protection policies, for ease of understanding by users, as well as allowing operation of services based on the PI protection policies. Here, PI protection policy technologies and PI protection policy management technologies are included. This classification classes PI protection technologies according to their objectives and characteristics. A specific technology is linked to the protection technology factors for each processing phase, since it is the most fundamental and common-used classification system.

Table 2. Protection Technology for Life Cycle of PI

Personal Information Protection Technology Type			Life Cycle			
			Collection	Storage & Retention	Usage & Provision	Destruction
Administration Technology	Privacy Filtering Technology	Network Filtering		√		
		PI Disclosure Protection		√		
		Privacy Infringement Prevention			√	
	Privacy Scanning Technology	PI Disclosure Testing		√		
		PI Retrieval		√		
		Privacy Vulnerability Testing		√		
	PI Transfer Technology	PI Concealment	√			
		PI Encryption	√		√	
		PI Authentication	√	√	√	√
	PI Storage Technology	Secure OS based DB		√		
		DB Encryption		√		
		DB Monitoring		√		
Policy/ Management Technology	Privacy Policy Technology	XML based Privacy Policy	√	√	√	√
		HTML based Privacy Policy	√	√	√	√
	PI Management Technology	Privacy Policy Management	√	√	√	√
		PI Management	√	√		√

According to the PI management model research (2006) by Korea Information Security

Agency, PI protection technologies can generally be applied according to each phase of the life cycle. If consideration is made on how specific technologies examined in PI protection technologies by characteristics are linked based on the security requirements of each phase of the life cycle, they can be expressed as technologies that correspond to technical protection measure requirements analyzed through pertinent laws. That is, PI protection technologies protect PI from infringement risks that may occur during each PI processing phase. They are summarized as technologies that protect the rights of data subjects [6][7].

3.2 Personal Information Protection Technologies for Each Processing Phase

The general public services aim to provide more safe and convenient services using new technologies. Such protection requirements in pertinent PI protection laws make clear statements about protection measures when specific technologies not intended for a typical PI processing system are used in the PI collection and usage phases. As a chief example, when CCTV, RFID, and biometrics are used, requirements are stated for special PI protection technologies to protect personal image information, biometric information, etc. Therefore, classification of technologies is needed in this regard as well.

Table 3. Personal Information Protection Technology for Specific Processing Areas

	Personal Information Protection Technology
CCTV Technology	**Privacy Masking, Camera Operation Control, Personal Image Information Encryption, Network Isolation Technology**
RFID Technology	**Tag Function Control Technology** (Kill Tag, Sleep/ Wake Tag), **Physical Approach** (Shield the Tag(Faraday Cage), Active Jamming, Blocker Tag, Proxying Approach), **Cryptographic Approach** (Minimalist Cryptography, Re-Encryption, Silent Tree Walking, NTT Forward Secure)
Biometrics Technology	**Biometric Information Management Technology**(Changeable Biometrics), **SmartCard based Biometric Information Protection** (Sensor on Card, Store on Card, Match on Card), **Biometric Information DB Isolation Technology, Biometric Information Modification/Fabrication Detection Technology** (Challenge/Response Protocol, Watermarking)

- **CCTV Personal Information Protection Technologies**[22]

When CCTV or web cameras are installed on the outer wall of a building, etc, surrounding apartments or residences may be filmed depending on the area shot and the camera angle. This infringes personal privacy. Faces of individuals risk exposure when CCTVs are installed by the roadside. Therefore, technologies against infringement of this kind are required to protect privacy and to protect individuals from video exposure.

- **RFID Personal Information Protection Technologies**

Identification information of objects are stored in extremely small tags and attached to the objects in RFID technologies. Information on the items of interest and the surrounding environment are wirelessly transmitted to the reader that has an attached antenna linking it to a network, where the information is processed. It is a non-contact, automatic-identification technology. RFID technology has the advantage that it can be used in diverse domains such as logistics, transportation and automobiles. However, adverse side effects, such as privacy infringement are coming to the fore as access to user information becomes easier. The general vulnerabilities of RFID technologies to privacy concerns include: information leakage (data security); personal tracking (location privacy); and omnidirectional privacy (forward privacy). Therefore, a PI protection technology classification is correspondingly necessary [8].

- **Biometric Personal Information Protection Technologies**

Biometric information is PI that cannot be replaced or erased. When unique biometric

[22] http://www.privacyinternational.org/issues/cctv/_index.html

information (face, fingerprints, iris, etc) is illegally leaked, there is no means available to check the source, use another set of biometric data, or prevent the use of leaked information. This can seriously infringe individual privacy. That is, biometric information, owing to its invariability, cannot be changed as is the case for a password or a PIN. If stored biometric information for user authentication is illegally used by others, there may be serious consequences. Therefore, PI protection technologies that can prevent PI infringement risks due to leaking biometric information are extremely important [9].

3.3 Personal Information Protection Technologies for Each Processing Phase at Public Institutions

PI protection technologies necessary in the public environment in Korea were examined from multiple viewpoints with reference to related research. A table of the PI protection technologies, necessary at each processing phase of PI at public institutions, was organized [10][11]. Effort was made to include every processing phase, section and countermeasure technologies, from the collection phase of PI to the destruction phase. This ranged from public servant PCs to PI DBs, and to special types of PI processing technologies, such as CCTV and RFID. Telecommunication service networks are classified broadly into six sections from the aspect of PI management. This aids understanding of the technologies required for each section of the service network that each of the public institutions operates according to protection standards. There are seven sections to cover the service environment of public institutions in Korea: 1) civil affairs PC section for security of users that use the service; 2) public servant PC section for security of internal users within the service organization, including those in charge of services; 3) transmission section for security in the process of transmitting PI, based on requests for services and their provision; 4) web/application section for security of services on the web; 5) DB section for security in storage or retention of service information; 6) offline section for security in tasks that are performed off-line; 7) other section (common section) for security of operation and management involving policies.[23] If the content of **Table 4** is understood, together with the legal requirements dealt with previously, those in charge of PI protection that conduct protection measures will be able to effectively implement countermeasures against risks that may occur during each processing phase, in each section, and for each processing technology. A more detailed description of specific technologies is omitted in this thesis as it is not one of the main subjects.

Table 4. Protection Technology for Personal Information Life Cycle in the Korean Public Sectors

Phase	Area	Personal Information Protection Technology
Collection Phase	**[1]Civil Affairs Office Public PC Area**	**Privacy Monitoring/Filtering Technology** **Privacy Authentication Technology** (Alternative Technology for Resident Registration Number - Internet Personal Identification Number Technology (i-PIN/G-PIN(Government i-PIN)) **Privacy Management Technology** (Privacy Policy Negotiation Technology (P3P)) **Privacy Infringement Protection Technology** (Adblocker, Spyware Filter, Spam Blocking Technology, Keyboard Security Technology)
	[2]Public Service Personnel PC Area	**Authentication Technology** **Privacy Infringement Protection Technology** (Adblocker, Spyware Filter, Spam Blocking Technology, Keyboard Security Technology)
	[3]Network Area	**Network Encryption** (Secure Server, Web Session Encryption) **Data Concealment Technology** (Client/Server Anonymization Technology)
	[4]Web/	**XML based Privacy Policy Notification Technology** (P3P)

[23] Found from investigation of actual conditions of management of personal information processing systems, which was conducted as part of "a study on a plan for technical protection measures for personal information by the processing phase ", conducted in December, 2008, by the Administrative Safety Department

Phase	Area	Personal Information Protection Technology
	Application Area	**HTML based Privacy Policy Notification Technology**
	CCTV Tech.	**Privacy Masking, Camera Operation Control Technology, Personal Image Information Encryption Technology**
	RFID Tech.	**Tag Function Control Technology** (Kill Tag, Sleep/ Wake Tag) **Physical Technology**(Tag Shielding Technology(Faraday Cage), Active Jamming, Blocker Tag, Proxying Approach) **Cryptographic Technology** (Minimalist Cryptography, Re-Encryption, Silent Tree Walking, NTT Forward Secure)
	Biometrics Tech.	**Biometric Information Management Technology**(Changeable Biometrics) **SmartCard based Biometric Information Security** (Sensor on Card)
Storage and Retention Phase	[2]	**Internet Access & Usage Control Technology**
	[3]	**Privacy Filtering Technology** (Intrusion Protection System, Intrusion Detection System, Intrusion Prevention System, Application Firewall) **Contents Monitoring Technology** **Data Leakage Protection(DLP) Technology**
	[4]	**PI Disclosure Protection Technology, Privacy Scanning Technology, Privacy Vulnerability Testing Technology, Privacy Vulnerability Testing Technology**
	[5]DB Area	**DB Security** (SecureOS based DB, DB Encryption, DB Access Control), Backup Technology
	Biometrics Tech.	**Biometric Information DB Isolation Technology**
Usage and Provision Phase	[1]	**Digital Rights Management, Watermarking**
	[2]	**User Authentication Technology** (GPKI(Government PKI), Biometric Authentication Technology, Dual Authentication Technology) **Digital Rights Management, Watermarking** **Remote Access Control Technology**(Server Based Computing, Remote Access Control System, GVPN(Government VPN)) **Identity & Access Management** (ID Management, Role/Entitlement Management, SOD(Segregation of Duties), IP/MAC Control Technology (One Person per Computer Technology), Password Management Technology) **PI Electronic Approval System**
	[3]	**Network Encryption Technology**
	[5]	**Privacy Logging System** (ID Auditing, Security Information and Event Management, Log Management Technology)
	[6]Offline Area	**Offline Media Control Technology** (Secure USB, CD Security Technology, Notebook /PDA Security Technology, Printed Paper Control Technology)
	Biometrics Tech.	**Biometric Information Modification/Fabrication Detection Technology** (Challenge/Response Protocol, Watermarking) **SmartCard based Biometric Information Security** (Store on Card, Match on Card)
Destruction Phase	[1], [2], [4], [5]	**PI File/Disk Eraser**
Others	[3]	**Network Dualization Technology**
	[7]Others	**Information Life Cycle Management, PIA aiding Technology**
	CCTV Tech.	**Network Isolation Technology**

As we have seen in **Table 2**, cryptography is an essential and critical technical measure for PI protection. It is mainly used in protection technologies for personal data encryption and user authentication. So, it is important that we use a strong cryptographic algorithm such as 256bit-AES for strengthening personal data protection. The strength and efficiency of cryptographic algorithm is crucial to the level of personal data protection. In the Korean public sectors, Cryptographic technologies are essential to protect PI. They are used in many areas and technologies such as network encryption, DB encryption and GVPN. Especially, for governmental usage, the public sectors must use cryptographic technologies meeting the requirements of the Korean Cryptographic Module Validation Program (KCMVP)[24][12]. And they cannot use a PI protection solution including a cryptographic module without a KCMVP certificate.

[24] The Korea Cryptographic Module Validation Program (KCMVP) is system that verifies the safety and implementation conformance of cipher products used for protection of critical intelligence that is not classified esoterically among mutually shared data in an information network system of a nation or public institution.

4. Technical Protection Standards for Personal Information Protection at Public Institutions

Based on the analysis of related laws and technical analysis, standard technical protection measures and checklists for protection of PI necessary at public institutions in Korea, are presented as the main findings of this research study. As mentioned in the above analysis, the implications based on legal analysis were considered and common/selective requirements were re-classified by breaking PI protection requirements into separate elements; protection standards and checklists were presented, linking them to the required technologies for each of the diverse PI processing phases. Although not dealt with in this thesis, for the present research, various public institutions were sampled to determine their actual conditions. The results were reflected in the protection requirements, after analyzing the risk factors for each of the seven PI processing sections, as indicated in Chapter 4.

In addition, in Korean law, some requirements were omitted based on the legal objectives or they differed according to the laws, causing some to point to the inconsistencies. Measures to address this involved analyzing the requirements found in the guidelines or manuals of related institutions, so that the shortcomings were not reflected in the protection standards. In selecting standard protection measures, common protection measures were devised. Technical measures that rated low in importance were bundled as an inclusive management item. If protection measures were only required for a few items, if they had a high level of importance and were urgent, they were classified into a separate item, to be selected as necessary. It is expected that the protection standards (items and checklists) developed in this manner will be adequate for use as technical measures that all public institutions must abide by. Consequently, improvements in effectiveness and management standards are expected.

4.1 Technical Protection Measures and Specific Requirements

After the analysis of related laws, guidelines, etc. given in Section 2.2.1, control items for the technical protection measures for each phase were grouped into the collection phase (5 items), storage and management phase (5 items), usage and provision phase (14 items), and destruction phase (1 item). Although the entire process of grouping cannot be described, development of practical protection standards necessary for every public service were found by devising requirements that require technical measures rather than managerial ones. In particular, specific technical types based on the processing phase, for the section, for the particular processing technologies, understood from previous research, were considered. However, only technical protection measures that can be used in practice, which were found by investigation of the actual conditions of operation and management of PI protection technologies at public institutions, were selected. In addition, technologies that are used in only some public institutions, such as CCTV, RFID, and biometric recognition technologies, were bundled as a special type, for selective usage. Technologies that have not been realized in legislation, but have been validated as being technically effective, were stated as specific required technologies in the protection measure checklist. Technologies that have not been validated for their effectiveness and abstract technologies were excluded.

Protection measures for the "usage and provision" phase are more numerous with respect to processing of PI compared to other phases. As explained in the analysis results, it is deemed that this is due to the many diverse departments and organizations whose aim has been to improve the administration efficiency under the framework of an e-government and government information sharing system. Individuals, information flows, and methods involved in the flow of PI are diverse. Consequently, there is considerable risk of misuse/abuse and exposure/leakage of PI arising from the sharing of PI between the central government and affiliated public institutions that have diverse physical systems and operate under diverse objectives. Therefore, various technical protection measures for prevention of information privacy violations and countermeasures against this are necessary.

Table 5. Applications in each class

Phase	Control Items	Detailed Conditions	Q&A	
Collection Phase	1.1Confirmation of Authenticity in Collecting PI	1.1.1 Alternative method of resident registration(ID) number	1	5
		1.1.2 Encryption of ID number	1	
		1.1.3 Supporting e-signature	1	
		1.1.4 Protection of ID number for confirming authenticity	2	
	1.2 Controlling insertion of PI in collecting information	1.2.1 Prevention of hacking the keyboard	1	2
		1.2.2 Inserting a replaced PI	1	
	1.3 Safety in sending the collected PI	1.3.1 Encryption of session in the web environment	1	2
		1.3.2 Encryption of C/S environment	1	
	1.4 Control of collecting personal video information	1.4.1 Control of CCTV video information	4(1)	4
	1.5 Control of collecting specific PI	1.5.1 Control of RFID tag information	1	3
		1.5.2 Control of bio information collection	2	
Usage and Provision Phase	2.1 Blocking PI file from access to the storing device physically	2.1.1 Control of access to the PI storage device physically	1	2
		2.1.2 Control of access to CCTV room physically	1	
	2.2 DB security of PI	2.2.1 DB encryption	1	6
		2.2.2 Control of access to DB	1	
		2.2.3 Storing of DB log	1	
		2.2.4 Preserving an expired member separately	1	
		2.2.5 Security of bio information DB	2	
	2.3 Backing up safe DB of PI	2.3.1 Encryption of back-up DB	2	2
	2.4 Blocking the stored PI from access to the network	2.4.1 Intrusion blocking system	1	2
		2.4.2 Intrusion detecting system	1	
	2.5 Security of Server	2.5.1 Security operating system	1	1
Usage and Provision Phase	3.1Safe certification in using/providing PI	3.1.1 Certification of e-signature	1	8
		3.1.2 Certification by multi-phases	1	
		3.1.3 Control of ID	2	
		3.1.4 Control of password	4	
	3.2 Control of Web/CS Application	3.2.1 Blocking a weakness of the web	2	7
		3.2.2 Analysis of weakness in the web site	1	
		3.2.3 Prevention of automatic admission	1	
		3.2.4Managing the right of application and controlling access to it	1	
		3.2.5 Control of access to the web server by a web server manager	2	
	3.3 Control of PI processing terminal	3.3.1 Prevention of virus	1	7
		3.3.2 Prevention of keyboard hacking	1	
		3.3.3 Control of storing PI	1(1)	
		3.3.4 Control of storing PI	4	
	3.4 Control of PI Storing Media	3.4.1 Control of CD/DVD	2	8
		3.4.2 Control of USB/portable storing device	3(2)	
		3.4.3 Control of laptop computer and PDA	3	
	3.5Control of PI included document	3.5.1 Control of digital document	2	4
		3.5.2 Control of print/copies	2	
	3.6 Control of Tasking Screen	3.6.1 Control of C/S screen	2	4
		3.6.2 Control of web screen	2	
	3.7 Control in using Internet	3.7.1 Control of internet service	1	1
	3.8 Control of Access to the Inner Network	3.8.1 Control of access to the wire(less) network	1	2
		3.8.2 Control of access to the weak	1	
	3.9 Control of Remote Access	3.9.1 Control of remote access	2	4
		3.9.2 Working online by telecommunication	2	
	3.10 Transaction of Safe PI through the Online	3.10.1 Separation of administrative organization	1	3
		3.10.2 Transaction exclusive wire/VPN	1	
		3.10.3 Sending encryption	1	
	3.11 Inspection and Blocking of Revealed PI	3.11.1 Blocking the revealed information on homepages	1	10
		3.11.2 Blocking of bulletin board	4	
		3.11.3 Blocking of PC for working	1	
		3.11.4 Blocking the revealed information in networks	1	

Phase	Control Items	Detailed Conditions	Q&A	
		3.11.5 Blocking of search engine's information	3	
	3.12 Recording PI Processing History	3.12.1 Monitoring of completed contents	2	5
		3.12.2 Logging of completed contents	1	
		3.12.3 Safe storing of log	2(1)	
	3.13 E-payment in Using/Serving PI	3.13.1 E-payment online	2	2
	3.14 Control of using Specific Information	3.14.1 Control and application of CCTV video information	2	5
		3.14.2 Control and application of RFID tag information	1	
		3.14.3 Control and application of bio information	2(2)	
Destruction Phase	4.1 Expiration of Safe PI	4.1.1 Expiration of storage media	3	8
		4.1.2 Expiration of selected file	2	
		4.1.3 Control of access and its record in expiring it	3	

4.2 Technical Protection Measures Checklist (Questionnaires) and Its Application

The aim of the present research is to present technical protection measures and specific requirements to be used in practice at public institutions to check the current status of the protection of PI. Therefore, questionnaires were developed to audit the status of information protection. The questionnaires comprised 107 items. They are divided into the following phases: collection phase (16); retention phase (13); usage and provision phase (70); and destruction phase (8). In addition, 13 optional items were included, indicated by brackets (refer to **Appendix 3**), that could be selected based on the technical environments of the public institutions. These questionnaires are composed of mandatory and optional requirements (refer to the last column of the table in Appendix 3). Classification of requirements as mandatory or optional is done according to these principles. First, checklist items based on explicit clauses of Korean laws, guidelines and standards of PI protection are mandatory. Second, essential and critical items that can give rise to PI leakage and disclosure if not applied in public institutions are mandatory. Third, items developed and supplied by the government for strengthening security of public institutions such as GPKI, G-PIN and GVPN are mandatory. Fourth, rational protection measures previously applied in many institutions and verified as effective and cost-efficient are mandatory. Accordingly, items that were regarded as strong but impractical measures until now because they suffer from performance problems and excessive cost are optional. Examples of this category are DB Encryption, DRM and electronic approval systems.

We provide a method for applying this checklist to Korean public institutions. First, we check if they comply with the mandatory requirements of general PI given by the PI lifecyle. Second, if they have specific PI such as personal image data, biometric information and RFID data, we check if they comply with the requirements(refer to 1.4, 1.5, 2.1, 2.2, 3.14 in **Appendix 3**) for specific PI through new technologies such as CCTV, RFID, Biometrics. Third, we check if they comply with the optional requirements of general PI for additional protection. Fourth, we diagnose the present state of PI protection in institutions and make a reinforcement plan for PI protection based on the results of a series of checks.

Next, we introduce an actual case of the application of this checklist using the Seoul TOPIS(Transport Operation and Information Service) as a example of a Korean public institution. The Seoul TOPIS is a management center that supervises overall transportation in Seoul on the basis of information collected from related systems and the network of traffic counters and CCTV cameras that monitor traffic conditions on major arterials. From the viewpoint of privacy, in TOPIS, personal image data is mainly collected through CCTVs and processed. And the linkage of personal image data and other personal data such as location information and vehicle registration information is done by TOPIS. Therefore it is required to protect personal image data and other related personal data before strengthening PI protection in TOPIS. In applying this checklist to TOPIS, first, we check if they comply with the mandatory requirements of general PI as given by the PI lifecyle. Second, if they have personal image data as specific PI, we check if they comply with requirements(refer to 1.4.1, 2.1.1, 2.1.2, 3.14.1 in **Appendix 3**) for specific PI. Third, we check if they comply with the optional requirements of general PI. Via this checklist and an application method such as this, Korean public institutions are guaranteed to have strong and effective technical protection measures during every phase of the PI lifecycle.

5. Conclusion and Expected Outcome

This paper presented the scope and specific technical items to protect PI in a detailed and comprehensive manner by analyzing legislation, guidelines, and manuals pertaining to PI protection at public institutions. It needs to consider the unique characteristics of public institutions in Korea, specifically e-government services, expansion of the level of sharing of government information, including PI, and collection and usage of resident registration numbers. We should prepare for the implementation of the PI processing system. It is extremely important for those responsible for protection of PI in each public institution. They should establish an inclusive PI protection plan as required by national policies and legislation. This will enable institutions to take appropriate technical protection measures. The "Technical protection measures and items, checklist for each item and list of related technologies" presented in this paper have great significance, since they go beyond merely supporting those responsible at organizations for establishing appropriate PI protection plans and the conduct of appropriate protection measures. They present the appropriate scope of technical protection regulations that Korean laws require, as well as providing clear standards to check the current level of technical protection realized in organizations. Each of the protection control items and specific requirements were developed in the form of questions for practical utilization. They provide a list of questions to check the technical protection activities and the measures realized. In addition, PI protection technologies that can be used currently were broken into separate elements and linked to each of the protection items presented, improving the level of understanding of protection activities. Some might say that these research results are no different to other manuals or handbooks such as the KISA(Korea Information Security Agency) explanation manual for personal information protection. But there are significant differences. First, the domain covered is different. The KISA manual is only based on relevant acts and regulations of the private domain. The checklist resulting from this thesis covers the public and private domains and public mandatory issues that are required from relevant laws are clearly covered. Second, it is a practical supporting tool for checking and reviewing technical protection duties rather than merely an explanation manual to help understanding or awareness. Because each of the control items and checklist requirements in **Appendix 3** were based on a distinctive feature in a public telecommunication network and specific characteristics for applicable entities in the public domain, they provide specific checking tools and guidelines for public officials specially. Also they provide organizing principles of mandatory and optional requirements, and considerations applicable to public institutions.

In conclusion, the research findings of this paper are expected to provide an effective standard for technical management activities for those in charge of protection of PI in Korean public institutions, especially in the following aspects: clear understanding of the scope and legal requirements during each processing phase of PI; supporting establishment of appropriate protection plans; and helping with the performance of clear and detailed technical protection measures. Furthermore, they will help minimize the security flaws due to limited activities for PI protection.

References

[1] 2008 National Audit Videoconferencing Report, MOPAS Korea, KISA, Oct. 2008.

[2] "2009 National Information Protection White Paper," NIS of Korea, Title 2, pp. 64, Apr. 2009.

[3] http://www.moleg.go.kr/english/korLawEng, http://elaw.klri.re.kr

[4] Andelmounaam, Internet PET, IEEE Security & Privacy, 2003.

[5] Kihyo Nam et al., "Recent Trend of personal information Protecting Technology and Vision in the Future," *KIISC Journal*, Vol.18, No.6, pp.11-19, Dec. 2008.

[6] Report of personal information Managing Model for Safe Collection, Preservation, Management, Service and Expiration of personal information, KISA, Dec. 2006.

[7] Carlisle Adams, "A Classification for Privacy Techniques," *univ. of ottawa law & technology journal*, 2006.

[8] Klaus Finkenzeller et al., "RFID HANDBOOK," 2nd Ed. in Korea, ISBN 89-314-2769-7, 2004.

[9] L. Sweeney, "Privacy-Enhanced Linking," *ACM SIGKDD Explorations*, vol. 7, no. 2, Dec. 2005.

[10] Yeonjung Kang et al., "Classification of PET on Life-cycle of Information," *International Conf. on Emerging Security Information, Systems and Technologies*, IEEE C&S, 2007.

[11] Privacy-Enhancing Technologies: White Paper Privacy-Enhancing Technologies, Ministry of the Interior and Kingdom Relations, the Netherlands, Dec. 2004.

[12] Wan S. Yi et al, "Government Information Security System with ITS Product Pre-qualification," *JWIS2009*, Aug. 2009.

Mina Shim received a B.S. degree in Computer Science from Sungshin Women's University, Korea, in 1996, and a M.S. degree in information security from Graduate School of Information Security, Korea University in 2006. She worked at Trigem Computer Inc. and Sun Microsystems Education Center in Korea, and then is currently with the Graduate School of Information Management and Security as a lecturer and researcher. Her research interests include privacy and personal information protection, PET, risk analysis and management, and information security management and policy.

Seungjo Baek received a M.S. degree in information security from Korea University, Korea in 2007. He is currently with the Center for Information Security Technology in Korea University, Korea as a researcher. His research interests include information security policy, privacy, intellectual property rights, cybercrime and digital forensic policy.

Taehyoung Park received a Master's degree from Korea University of Public Administration, S. Korea in 2004, and held office as researcher in Korea Institute of Public Administration for 4 years. He is currently with the Information Security Policy Lab in Korea University, S. Korea. His research interests include E-Government, performance analysis & evaluation of public service, enterprise architecture and privacy.

Jeongseon Seol received a Bachelor of law degree from Yonsei University, Korea, in 1981, an MBA degree from Graduate School of Business of Georgia State University, U.S. in 1989. He is a former deputy minister of the Korea Communications Commission and currently a vice chairman of Korea Telecommunication Operators Association. He passed the high civil service examination in 1980 and served as a postmaster at the Daejeon Yuseong post office (1992-1994) and moved to Industry Canada Canadian Radio-television and Telecommunications Commission in 1994. Also he served as administrative officer of Chief Economic Advisor Office of the President (1999-2001) and office of industries deputy minister of the Ministry of Knowledge Economy (2008).

Jongin Lim received the B.S., M.S. and Ph.D. degrees in Mathematics from Korea University, Seoul, Korea, in 1980, 1982 and 1986. He has been the Dean and professor of Graduate School of Information Management and Security, the Center for Information Security and Technologies (CIST), Korea University, Seoul, S. Korea since 2000. He is also currently editor of *Journal of Digital Forensics, Security and Law* (JDFSL) and vice-chairman of Korea Institute of Information Security and Cryptology. Prof. Lim's areas of research interests include cryptography, information security policy and digital forensics.

Appendix

Appendix 1. Protection measures in the collection stage of personal information according to related laws

Phase	**Laws**	**Number of provision**	**Contents**
Collection Phase	A	Article 3, clause 2	(principle of PI protection)①clarification of the purpose of collecting PI, minimum collection, restriction on uses other than the purpose
		Article 4	(collection of PI) ①principle of limitation of collection of PI ②rights of PI providers stated in documents or on web site
		Article 6	(agreement in advance when PI files are retained or changed)①subject of discussion
		Article 6	(agreement in advance when PI files are retained or changed)③exception of clause 1
		Article 7, clause 2	(PI protection policy)①contents of PI protection policy ②policy publication method
		Article 9, clause 2	(confirmation of identity online)①measures to secure safety ②general measures ③request for cooperation
		Enforcement Decree(ED), article 4, clause 3	(entrusting installation/management of closed-circuits) ① conditions of the commission ②necessary conditions for PI protection ③publication items on the information bulletin board
		ED, article 5	(subject of discussion)"clauses set by a Presidential decree"
		ED, article 6	(excluded items for subject of discussion)②"PI files set by a Presidential decree"
		ED, article 7	(public notice of PI files) ① publication of PI files kept by the public institution ③ restriction on public notification of processing information with perusal restriction
	B	Article 10	(principle of confirmation of the administrative organ)
		Article 11	(principle of the administrative information joint use) administrative information joint use and restriction on collection the same information when provided to other institutions
		ED, article 6	(receiving of electronic documents) ①receiving of designated electronic documents such as computer ②notice and confirmation of the fact that electronic documents have been received ③notice of the fact of the reception
		ED, article 21	(notification in advance for information file implementation) ①notification matters when information files are implemented, retained, changed, or destroyed
	G	Article 22	(collection/use/consent of PI) ①official announcements when PI is collected and when the consent is obtained ②collection and use of PI without consent
		Article 23	(restriction on collection of PI) ①restriction on PI collection ②minimum information collection
		Article 25	(entrusting of PI)①notification and consent matters when PI is entrusted to a third party ②exception of notification and consent procedures ③purpose of handling PI ④management/supervision ⑤responsibility for compensation for damages
		Article 26	(transfer of PI due to receiving of work, etc) ①notification of the fact that PI was transferred, based on a method set by a Presidential decree, and the items ②notification of the fact that PI has been transferred ③use and provision of PI, within the scope of the original purpose
Storage and Retention Phase	A	Article 3, clause 2	(principle of PI protection)② guarantee that the processed information is accurate and is the latest, securing safety
		Article 5	(scope of possession of PI files)
		Enforcement regulation(ER), article 3	(PI file collection) published once a year
		ER, article 4	(management of computing rooms, etc) ①securing safety of PI ②measures to prevent crimes such as installing surveillance equipment, and regular inspections
		ER, article 5	(management of input and output data) ①measures to prevent leak of inputted data ②measures to prevent leak of recording mediums, discarding output material when no longer required ③record to input and output management ledger and its management ④automatic recording of appropriate output material
		ER, article 11	(accuracy of processed information) ①designation of the preservation period for processed information and PI files, and their management
	B	ED, article 11	(installation of an authentication management center) installation of administrative e-signing authentication management center
		ED, article 15	(confirmation of the time of electronic documents)
		ED, article 16	(management of authentication records, etc) ①administrative e-signing verification key,

Phase	Laws	Number of provision	Contents
			certificates, safe keeping and management of authentication work records ② maintenance and preservation of administrative e-signing verification keys and certificates ③confirmation of certificates
		ED, article 34	(protection measures for administrative information, etc) ①management of administrative information by classifying ②study of protection measures when using administrative information ③edit/supplementation when information files are modified ④management and preservation of official electronic documents
		ED, article 35	(security measures related to safekeeping/distribution of electronic documents) ①"security measures for which safety has been confirmed by the director general of national intelligence" ②review of level of security ③other security measures related to maintenance/distribution of electronic documents
	C	Article 28	(installation of a resident registration computing center, etc)②construction of a resident registration computing backup system
		Article 31	(obligations by the institution that maintains resident registration chart, etc) ①safety measures to prevent disappearance, theft, leak or damage to resident registration charts ②restriction on computerized processing using resident registration charts, for purposes other than possession and the purpose of use ③leak of the secret of handling of matters related to resident registration
		ED, article 10	(management/preservation of resident registration charts, etc) management/preservation methods of resident registration charts, resident registration charts by generation
		ED, article 46	(running of a resident registration computing center, etc) ④safety measures for resident registration computing center and resident registration computerized information back-up system data
	D	Article 7	(the original ledger for vehicle registration)③prevention measures against leak of registration ledger and information within, as well as preservation measures ⑤prevention of leak of PI when registration ledger is viewed or delivered
		Article 69	(computer processing of work related to vehicle management) ①work using computer information processing organization
	G	Article 27	(designation of the person in charge of managing PI)①②③
		Article 27, clause 2	(making public the policy on how PI is handled) ①② items of PI handling policy that are made public ③reason and details when the policy on handling PI is changed
		Article 28	(protection measures of PI) ①technical/managerial measures for protection of PI ②limit the number of persons handling PI to the minimum
		ED, article 15	(protection measures for PI) ①technical/managerial measures needed for securing safety of PI ②announcement of detailed standards of protection measures
		ER, article 9	(protection measures for PI) ①managerial measures needed to secure safety of PI ②technical measures needed to secure safety of PI ③announcement of specific standards of protection measures that reflect characteristics of the types of businesses
Usage and Provision Phase	A	Article 9	(securing safety of PI, etc) ①measures to secure safety when PI is handled, transmitted and received ②measures to secure safety of PI when it is processed by entrusting to a third party ③outsourcing method/procedure ④ announcement of outsourcing ⑤
		Article 10	(restriction on use and provision of processed information) ①restriction on use and provision of PI files for purposes other than the purpose of possession ②minimization of use and provision ③excludes use and provision other than for the purpose of possession ④measures to secure safety of processed information ⑤restriction on use and provision for third parties without consent ⑥announcement of legal grounds and purpose when used or provided for a purpose other than the original purpose
		ED, article 10	(securing safety of PI, etc)①
		ED, article 11	(use/provision of processed information) ① clarification of the scope of processed information ②use of processed information and keeping a provision ledger
		ED, article 12	(restrictions on the use/provision of processed information) ①restrictions on the items and measures when information network is used and provided ②stop use and provision when not performed
		ER, article 6	(installation/management of terminals) ①user ID and password assigned to each of the PI terminals ②name of the PI file, time that PI was processed, the author and check of used terminal
		ER, article 11	(accuracy of processed information) ②notification of correction/deletion to processed information

Phase	**Laws**	**Number of provision**	**Contents**
	B	Article 12	(principle of PI protection)
		Article 18	(transmission/reception of electronic documents)①transmission using a method of ID confirmation using public certificates, etc ②
		Article 21	(joint use of administrative information) ①administrative information that calls for joint use ②exception to administrative information joint use ③transmission method for protection of administrative PI ④maintenance of accuracy of administrative information
		Article 22	(procedures for administrative information joint use) ①writing up of electronic creation/distribution/storage lists ②distribution of the lists and investigation of joint use information ③establishment of administrative information joint use plan, measures ④administrative information joint use center ⑤joint use work outsourcing
		Article 22, clause 2	(joint use of administrative information such as public institution)①administrative information joint use center ②administrative e-signing
		Article 22, clause 3	(administrative information handling/obligations of users) restriction when administrative information is handled/used
		Article 27	(establishment and enforcement of security measures by information network and such) ①securing of safety and reliability for administrative information, etc, and information network of e-government ②establishment/enforcement of administrative information and such as well as information network ③measures to secure safety when e-documents are kept and distributed, confirmation that it was been carried out ④
		Article 30	(working remotely online) prevention of illegal access and security measures when working remotely
		Article 35	(confirmation of identity) method for identity confirmation when processing civil petitions
		Article 39, clause 2	(electronic public service security measures)①②
		ED, article 18	(transmission method for administrative information) transmission/reception method for joint use of administrative information amongst institutions
		ED, article 22	(request for provision of administrative information)①request of the purpose for use of administrative information being kept and managed ②request for provision of administrative information in the minimum scope
		ED, article 24	(joint use of administrative information using information network)①subject of discussion with administrative information joint use center ②link with/use information network
		ED, article 26	(administrative information joint use center)②administrative information joint use center work
		ED, article 30	(stop of provision of administrative information)①stop of provision of administrative information, request for return and use prohibition ② notification of the reason for stop of provision and use prohibition ③duplication, copy, continued preservation, use prohibition of administrative information
		ED, article 44	(confirmation of identity) ②electronic identity confirmation method, alteration/leak of PI or measures to prevent illegal use
		ED, article 49	(scope of security measures for electronic public service) “security measures for electronic public services"
	C	Article 29	(viewing or delivery of transcript/abridged copy)⑤
		ED, article 49	(transcript/abridged copy of resident registration chart using civil petition machine)①comparison/comparison according to computing organization ②safety management measures such as protection of resident registration computing system as well as protection of PI ③ check of the operation of civil petition machine as well as state of security, and taking of appropriate measures, stopping when leak is detected
		ED, article 56	(processing of electronic documents related to resident registration, such as civil petition) ③alteration/forgery prevention and purpose confirmation
		ED, article 57	(confirmation of authentication of name and resident registration number)①construction of "real name confirmation system for election" ②use of real name confirmation system according to clause 59 of 「public election law」 ③safety management measure ④guidance/supervision of clause 3 ⑧
		ED, article 58	(confirmation of authenticity of resident registration cards)①confirmation of authenticity using computing organization ②scope of use for authentication confirmation system ④use limitations of authentication confirmation system ⑤
	D	ED, article 14	(use of computing data) ①use scope of data that contains PI ②application notification
	E	Article 24	(provision of administrative data)①②③confirmation of safety of administrative data ④limitation on provision for purpose other than collecting statistics ⑤stop and limitation of

Phase	Laws	Number of provision	Contents
			provision of administrative data when protection measures on data does not take place
		Article 30	(provision of statistical data)①②③④
		Article 31	(use of statistical data)①②③④
		Article 33	(protection of secrecy)①②
		ED, article 48	(protection of statistical data)①②
		ED, article 50	(measures for protection of secrecy)①②③
	G	Article 24	(use limitation on PI) limitation of use for purpose other than collection of personal data
		Article 24, clause 2	(consent of provision of PI, etc)①notification and obtaining of consent when provided to a third party ② provision of PI to a third party and limitation on use for other than the intended purpose
		Article 63	(protection of PI when transferred to the outside)①limitation on signing of contract for illegal PI ②obtaining of consent when PI is transferred to the outside ③notification items when obtaining consent ④protection measures
		ED, article 67	(protection measures when PI is transferred to the outside)①protection measures when PI is transferred to the outside ②contract contents
Destruction Phase	A	Article 10, clause 2	(destruction of PI files)①immediate destruction when possession of PI file is not necessary ②notification of the destruction of PI files ③
		ED, article 12, clause 2	(destruction method, etc, for PI files)①use of a method that makes restoration of PI impossible ②notification of the fact of destruction of PI files
	G	Article 29	(destruction of PI) immediate destruction of PI
	F	Article 19, clause 3	(management of official candidates) ②consent method when information of official candidates is collected and managed

Appendix 2. Regulations of protection measures in the treating process of Personal Information pursuant to relevant Guidelines and Manual

Stage	Title	Provision No.	Contents	Stage	Title	Provision No.	Contents
Collection Phase	R	Article 4	①②	Usage and Provision Phase	R	Article 6	②
		Article 5			P	Article 7	①②③
		Article 11				Article 8	①②
		Article 16			N	Article 4	②
	P	Article 4	①②			Article 10	
		Article 5	①②④			Article 16	
	N	Article 4	①		O	Article 4	②
		Article 7	①③④			Article 11	①②③
		Article 9	①②③			Article 18	
	O	Article 4			Q	Article 14	③
		Article 10	①②			Article 17	
	Q	Article 4			K	Article 9	①②③
		Article 5	①②			Article 10	
		Article 6	①②③④			Article 12	⑤
		Article 9				Article 13	①
		Article 10	①②③			Article 22	④
	K	Article 8	①②③			Article 30	①②
		Article 12	①④⑤			Article 32	
		Article 18	③		S	Article 4	①②
		Article 22	①②			Article 8	①②
	M	Title III. 1.	1-1.			Article 9	①②
Storage and Retention Phase	P	Article 6				Article 10	①②
	N	Article 11	①③④			Article 11	①②
	K	Article 12	②			Article 15	②
		Article 16			M	Title III. 3.	3-4.
		Article 17		Destruction Phase	R	Article 15	
	L	Article 4	①②		P	Article 9	①②
		Article 5	①③		N	Article 13	

Stage	Title	Provision No.	Contents	Stage	Title	Provision No.	Contents
	S	Article 22	①②		Q	Article 16	①②
					K	Article 19	①②
						Article 20	①③
					M	Title III. 4.	4-1.

Appendix 3. Protection measures checklist for each personal information processing phase at public institutions (Questionnaires) *※M(mandatory requirement), O(optional requirement)*

Phase	Control Items	Detailed Condition	Question	Option
Collection Phase	1.1	1.1.1	Is the institution using a resident registration number replacement technique such as public I-PIN or private I-PIN in order to minimize the collection of resident registration numbers when collecting PI online?	M
		1.1.2	When sensitive information such as resident registration numbers is collected on the institution's web site due to unavoidable circumstances, is it always encrypted?	M
		1.1.3	Does the institution support e-signing authentication using certificates of various types such as GPKI and NPKI, when collecting PI?	M
		1.1.4	Does the institution encrypt resident registration numbers when they are entered by users for the purpose of confirming their real name?	M
			Does the institution immediately delete resident registration numbers when they are entered by users for the purpose of confirming their real name, after accomplishing the objective?	M
	1.2	1.2.1	Does the institution use techniques against keyboard hacking for the terminals used in collecting PI?	M
		1.2.2	Is the institution preventing leakage of PI when sensitive information such as resident registration numbers or account numbers are entered for registering at the site by civil affair workers, by replacing a certain number of letters with asterisk (*) or some other arbitrary letter?	M
	1.3	1.3.1	Does the institution use the following encryption methods for sessions between the server and users, which include PI and authentication information collected at the web site? 1. Receiving/transmitting by encrypting PI by installing SSL (Secure Socket Layer) certificate in the web server. 2. Receiving/transmitting by encrypting PI by installing an encryption application program in the web server.	M
		1.3.2	Does the institution use VPN in receiving/transmitting PI and authentication information collected in C/S environment, which encrypts the section between collection terminals and PI DB?	M
	1.4	1.4.1	Does the institution restrict voice recording feature of CCTV?	M
			Does the institution place a limit on the pan/tilt/zoom functionality to within the scope of accomplishing the objective of the installation?	M
			Does the institution use a masking technique on video information of individuals, which is exposed and unnecessary in accomplishing the objective for the installation of CCTV?	M
			Does the institution have technical measures in place that allow only those with privileges to see the original image from CCTV without masks, by masking sections and locking those sections with passwords by use of a masking function that is included in the camera?	O
	1.5	1.5.1	Does the institution that collects PI to be included in RFID tag encrypt the PI?	M
		1.5.2	Does the institution that collects biometric information encrypt the collected information before receiving and transmitting?	M
			Is only the minimum biometric information collected to accomplish the objective, such as identification?	M
Storage and Retention Phase	2.1	2.1.1	Does the institution have surveillance equipment such as CCTVs or surveillance cameras or access control systems such as electronic pass or biometric recognition systems installed in computing labs or data rooms where PI files or mediums are being kept, in order to control entry of non-authorized personnel and record and manage access logs?	M
		2.1.2	Does the institution have surveillance equipment and access control systems that can control entry of non-authorized personnel installed, by monitoring of CCTV, and are the entry details recorded and managed?	M
	2.2	2.2.1	Does the institution encrypt important PI such as resident registration number, account number, and password, when storing them in the database containing PI?	M
		2.2.2	Does the institution minimize access privileges for users and groups to important PI in the PI database or in database tables, and carry out access control?	M

Phase	Control Items	Detailed Condition	Question	Option
		2.2.3	Does the institution log name of the PI file and the specific item accessed, access time, user that accessed it, IP, etc, when PI DB is accessed?	M
		2.2.4	For institutions that operate under a membership system, when membership is cancelled for a user and their information is retained for the remainder of the retention term as specified by law, is the information separated from information of other ordinary members and kept in a separate database for users with cancelled memberships, and is the use and access to this database controlled strictly?	M
		2.2.5	Does the institutions that collect biometric information store information in a database physically separated from other PI such as name and address and is high level of access control being provided?	M
			For institutions that collect biometric information such as fingerprints for the purpose of user identification, is one-way encryption being done when storing biometric information so that they can't be decrypted?	M
	2.3	2.3.1	Is the institution carrying out protection using strong access control while regularly dispersing or backing up data from DB to a remote place?	M
			Does the institution encrypt data stored in the backup database in order to prevent exposure of PI when the data stored in the database is leaked out?	M
	2.4	2.4.1	Does the institution use an intrusion prevention system that protects the internal network in order to prevent leak of PI from various attacks from external networks?	M
		2.4.2	Is the institution implementing a system that can prevent leak of PI by detecting various attacks from the outside, such as intrusion detection system (IDS), intrusion prevention system (IPS), or threat management system (TMS)?	M
	2.5	2.5.1	Is the institution using a secure operating system with a secure kernel that integrates identification and authentication of users, compulsory access control, optional access control, intrusion detection, etc, in order to protect its servers and PI processing systems from attacks that went through intrusion interception system and intrusion detection system unscathed?	O
Usage and Provision Phase	3.1	3.1.1	Does the institution provide authentication using e-signed certificates such as GPKI, NPKI, etc, as user authentication method for use and provision of PI?	M
		3.1.2	Does the institution use additional authentication techniques such as biometric authentication such as fingerprint recognition, secure tokens, OTP, USB plug-in, or smart cards, for terminals that handle especially sensitive PI, for enhanced security?	M
		3.1.3	Does the institution assign and manage a single unique ID for each employee?	M
			Is access and use being strictly controlled in order to prevent illegal use of IDs and borrowing of IDs for important PI processing systems? (ex: 1 person, 1 PC technique using mapping between MAC/IP of the terminal and the individual's ID)	M
		3.1.4	For an institution that performs authentication using ID and password, when unsafe passwords are attempted to be used, does it automatically require the user to enter a different one?	M
			For an institution that performs authentication using ID and password, is there a system in place that regularly checks for unsafe passwords and require the user to enter a different password if theirs is deemed unsafe, which works by setting up of the expiry date of the password, limiting use of the same or similar password, and setting up the minimum number of letters for the password?	M
			For an institution that performs authentication by ID and password, can it prevent further attempts when the number of attempts exceeds a certain value, with display of a warning message?	M
			For an institution that performs authentication by ID and password, does it perform one-way encryption when storing passwords so that they can't be decrypted?	M
	3.2	3.2.1	Does the institution develop applications so that they are prepared for main attacks targeting web servers and web applications, described in OWASP top 10 security vulnerabilities and the 8 key vulnerabilities by the National Intelligence Service, and does it constantly review vulnerabilities and update the applications? (Reference: http://www.owasp.org/, http://www.ncsc.go.kr/)	M
			Does the institution have a firewall installed in order to protect against main attacks targeting web services and web applications, described in OWASP top 10 security vulnerabilities and the 8 key vulnerabilities by the National Intelligence Service?	M
		3.2.2	Does the institution perform analysis of vulnerabilities for exposure of PI due to technical errors in web site design or because of availability of the source code of the web site due to traditional development practices? (ex: privilege authentication error, search engines finding restricted pages, exposure of web pages designed for administrators, exposure due to directory listing, etc)	M

Phase	Control Items	Detailed Condition	Question	Option
		3.2.3	Does the institution use a automatic-sign-up prevention technique that requires users to enter a random string of text when they sign up online or when they are authenticated, in order to prevent automatic creation of accounts by a program?	O
		3.2.4	Does the institution have privilege management system with user and group level management for processing of PI, and does it perform access control for PI processing applications based on this?	M
		3.2.5	Does the institution perform strong authentication and access control for web server administrators?	M
			Does the institution make it so that whether or not administrator accounts have been exposed or being misused can easily be found by automatically notifying to the administrator when there is a log-in or log-in attempts to an administrator account?	M
	3.3	3.3.1	Does the institution have an anti-virus program installed which constantly checks for intrusion to a PI processing terminal by malicious programs such as computer viruses or spyware, and does it perform automatic patching and update?	M
		3.3.2	Does the institution have a keyboard hacking prevention technique in place for PI processing terminals that encrypts in the keyboard driver level sensitive PI entered by use of diverse types of keyboards such as USB, PS/2, and wireless?	M
		3.3.3	Does the institution use server based computing (SBC) or application virtualization which allow all work to be performed on a server with work terminals only acting as input and output terminals, in order to fundamentally eliminate or minimize PI left on work terminals and remote PCs?	O
		3.3.4	For an institution with a civil petition machine installed, is its input/output interface isolated?	M
			For an institution with a civil petition machine installed, is unnecessary OS functionality and features unrelated to civil petition being controlled?	M
			For an institution with a civil petition machine installed, is installation and use of non-business services such as messenger and remote control solution being controlled?	M
			For an institution with a civil petition machine installed, are unnecessary ports removed and is there a OS firewall in operation?	M
	3.4	3.4.1	For an institution that provides PI to the outside using CD/DVD, is the CD/DVD encrypted during manufacturing so that if the user doesn't know the password, the CD/DVD itself can't be opened?	M
			For an institution that provides PI to the outside using CD/DVD, is there DRM in effect so that the files including PI stored in the medium can be copied and printed only if privileges are given?	O
		3.4.2	Does the institution use secure USB which provides functionality such as copy protection of specified data, through user identification, encryption/decryption of designated data, setting up of the number of uses, use period, use-approved PCs, as a removable storage of PI?	M
			Does the institution provide a total delete feature when the number of wrong passwords entered exceeds a specified value, when the USB storage device is lost or stolen, for protection of data?	O
			Does the institution provide a tracking feature that becomes activated when a lost or stolen USB storage device is used, which transmits the information of the PC being used as well as the network it's on to the individual's email and to the server?	O
		3.4.3	Does the institution record and manage notebook/PDA's check-in and check-out as well as details of use for each of the users?	M
			Does the institution have a measure in place for lost or stolen notebooks which prohibits unauthorized users from using them, by having strong passwords for the notebooks?	M
			Does the institution strongly encrypt the data and contents of the notebooks so that unauthorized users can't access them when they're lost or stolen?	M
	3.5	3.5.1	For an institution with large volume of information or sensitive information, does it automatically encrypt digital document files with PI when they are downloaded by employees from an internal system?	M
			For an institution with large volume of information or sensitive information, does it apply DRM to digital documents with PI in order to prevent access such as copy and printing out for unauthorized digital documents?	O
		3.5.2	When PI is printed out, does the institution use a watermarking technique to include the name and logo of the institution, serial number, unique ID of the printer, name of the person who printed, print time, etc, in the printed out material?	M
			Does the institution use an effective alteration/forgery prevention technique when issuing civil	M

Phase	Control Items	Detailed Condition	Question	Option
			petition documents?	
	3.6	3.6.1	Does the institution provide screen copy prevention feature when using C/S programs, which works to deter screen capture programs?	M
			Does the institution control menus such as save, output, and copy on C/S program screens according to the privileges?	M
		3.6.2	Does the institution control functionality such as drag & drop and copy & paste using the mouse, and the view source feature by right-clicking the mouse on the screen, as well as screen capture?	M
			Does the institution provide privilege-based web browser menu inactivation feature and assign privileges specific to pages (print, save, view source)?	M
	3.7	3.7.1	Does the institution control the use of internet services that may serve as the vehicle for leak of internal information, such as illegal internet sites, non-work-related sites, web mail, P2P, messenger, web storage, FTP, Telnet, shared folders?	M
	3.8	3.8.1	Does the institution provide automatic detection as well as authentication/access control through IP/MAC resource management and monitoring, in order to control unauthorized use of internal wireless and wired LAN using notebooks or mobile devices?	M
		3.8.2	Does the institution provide network access control (NAC) which automatically prevents terminals without anti-virus programs installed and which are vulnerable to threats because security patches haven't been installed from connecting to the network, and which carries out measures to strengthen security?	M
	3.9	3.9.1	Does the institution monitor remote access to PI processing systems and record access details?	M
			When abnormal requests for viewing PI comes in from a remote system, characterized by abnormal IP range, time zone, or processing volume, does the institution give warning and isolate them?	M
		3.9.2	Does the institution use GVPN, an online government remote work service, when employees do work involving PI processing from a remote location?	M
			Does the institution use VPN, a sectional encryption technique, when employees do work involving PI processing from a remote location?	M
	3.10	3.10.1	Are the corporate network and the public network strictly separated, and is the processing and transmission of PI within the organization done on the corporate network?	M
		3.10.2	Is online transmission for provision of PI to related institutions as well as use of PI within the organization being done using a high speed government network or a dedicated line or VPN?	M
		3.10.3	When PI is transmitted online to related institutions as well as when it is used within the organization, is the contents encrypted before they're sent?	M
	3.11	3.11.1	Is there PI leak check and isolation features provided regarding all types of web page contents?	M
		3.11.2	Are there PI leak check and isolation features for the bulletin board posts on the web site?	M
			Are there PI leak check and isolation features for all types of attachment files within the bulletin boards on the web site? (ex: Hangul, MS-Word, Excel, Powerpoint, Acrobat PDF, Alzip, HWX, ZIP, TAR, MS Office)	M
			Is there a leak check feature for OLE files included in attachment files in the bulletin boards on the web site? (ex: HWP (including XLS, PPT, DOC), XLS (including DOC, PPT), PPT (including DOC, XLS), DOC (including XLS, PDF, PPT))	M
			Is there a secure write feature that allows only those with privileges such as administrators to see the posts containing PI?	M
		3.11.3	Is there a system in place that automatically detects and deletes PI left behind on PCs after the objective has been accomplished?	M
		3.11.4	Is there a PI leak interception feature that prevents PI, such as resident registration numbers or credit card numbers, from leaking out, in inbound and outbound network traffic that uses various protocols such as email, instant messenger, FTP, and HTTP?	M
		3.11.5	Is whether or not PI is being exposed from the domain by search engines such as Google and MSN regularly checked?	M
			When it becomes known that PI is exposed on web pages by search engines, does the institution request deletion of the pages to the search engines?	M
			Does the institution check whether exposed web pages still exist on web servers and delete as necessary?	M
	3.12	3.12.1	Does the institution monitor all details of PI processing, such as viewing of PI stored in a database, output, file download, etc, through terminal systems, remote systems, and one-stop service?	M
			Does the institution prohibit perusal and give warnings when employees view a large volume	M

Phase	Control Items	Detailed Condition	Question	Option
			of PI outside of reason such as information on co-workers or famous people or when they view unauthorized contents, by monitoring details of PI processed?	
		3.12.2	Does the institution log details of PI processed, such as names of individual files, processing body, processed time, terminal used, etc?	M
		3.12.3	Does the institution back up PI database to a separate storage device that exists in a separate network in order to safely record and preserve access and use logs?	M
			Does the institution save logs to a WORM (Write Once Read Many) storage device for which alteration, forgery, and deletion are not possible?	O
	3.13	3.13.1	Does the institution have in place an online electronic approval system that have internal employees state their ID, time, file name, purpose, etc, in advance, when they access, use, provide, or destroy PI, and have them obtain approval from the person in charge?	O
			Does the institution record and safely maintain approval request details from the online electronic approval system according to the six principles (who, what, when, where, why, how)?	O
	3.14	3.14.1	Does the institution provide access control for the CCTV operating system which collects video information by use of CCTVs?	M
			For an institution that collects video information by using network cameras, does it provide security measures such as dedicated network isolation, encryption of video information stream, and strong access control for specific IPs?	M
		3.14.2	For an institution with RFID system installed, does it prevent exposure of tags with PI to those without legal privileges, by encrypting data transmitted between RFID tags and the reader?	M
		3.14.3	For an institution that collects biometric information, does it change characteristic information extracted from the actual biometric information when biometric information is used, such as for biometric authentication, in order to prevent illegal use of biometric information?	M
			For an institution that collects biometric information, does it provide protection measures that can detect and track exposed biometric information, such as watermark technique?	O
Destruction Phase	4.1	4.1.1	Does the institution completely destroy processing information left on the storage device after PI is safely moved from off-line storage mediums such as external hard disks and USB memory devices, so that the processing information can't be restored?	M
			Does the institution completely initialize storage mediums that are to be disposed and discarded, in the unit of the drive, by exposing them to strong magnetic fields, so that restoration is not impossible? (ex: Degausser)	M
			Does the institution physically destroy expired printed-out material using a trash burner or shredder so that they are rendered not recognizable?	M
		4.1.2	Does the institution provide a selective destruction technique that can selectively and permanently delete PI stored in file format, by folder, file, and disk?	M
			Does the institution completely destroy temporary files, virtual memory files, and deleted files in the recycling bin left on the PC, which have the potential to expose PI, after PI processing has been completed, so that they can't be restored?	M
		4.1.3	Does the institution provide electronic approval feature that allows one to obtain approval from the person in charge before PI files are destroyed, according to the person destroying, target, purpose, method, etc?	O
			Does the institution provide access control based on privileges and authentication of the person destroying, so that only those with privileges can destroy files?	M
			Is the tool used for destroying PI log the user, time, destroyed file, and name of the medium, when PI files are destroyed?	M