

MAR - 5 2009

FCC Mail Room

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2007

Date Filed: February 25, 2009

Name of company covered by this certification: Korea Telecom America, Inc.

Form 499 Filer ID: 821756

Names and Titles of Signatories:

Taisik Kim, Executive Director
Jongtak Hahn, Vice President

I, Taisik Kim, Executive Director of Korea Telecom America, Inc., certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

I, Jongtak Hahn, Vice President of Korea Telecom America, Inc., certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.



Taisik Kim
Executive Director



Jongtak Hahn
Vice President

Dated: February 26, 2009

No. of Copies rec'd 0
List A B C D E

Statement Regarding Compliance with CPNI Regulations & Report on Unauthorized Disclosure of CPNI

The internal operating procedures and practices of Korea Telecom America, Inc. ("KTA"), which are mandated by its parent company KT Corporation, ensure that KTA complies with the Commission's rules at 47 C.F.R. § 64.2001 *et seq.*, governing the use and disclosure of Customer Proprietary Network Information ("CPNI"). KTA's compliance with the Commission's CPNI rules is demonstrated by the policies, practices, and training procedures detailed below.

In connection with the use of CPNI for marketing purposes, KTA's utilization of CPNI is limited to the marketing of offerings among the same categories of service to which the customers already subscribe. KTA has established a review and approval process that calls for the records of such offerings to be maintained.

As a general rule, KTA does not release or disclose customers' CPNI to third parties, but when it does so, it is only upon the customer's written consent as required by law or as described in the next paragraph. Without written consent, CPNI will only be disclosed if the request is made pursuant to a valid court order, warrant or appropriate notice from a government agency.

Other than as described above, KTA will release or disclose customers' CPNI only for the express and limited purposes of initiating, rendering, billing and/or collecting for services provided by KTA. In such cases, disclosure is only made pursuant to a written and binding agreement that contains restrictions regarding the confidentiality and safeguarding of customer information.

The customer service representatives of KTA do not discuss or disclose customers' call detail records on customer-initiated telephone calls, except for the limited discussion of call detail records first identified by the customer.

KTA does not provide any online access to customers' CPNI or call detail records until the customer requesting such information provides a password that has been established by the customer after that customer has been authenticated through a method that does not include the use of readily available biographical information. KTA notifies a customer immediately whenever such customer's password, means of authentication, online account or address associated with the account is created or changed.

KTA does not provide customers with access to call detail records at retail locations because KTA sells only pre-paid calling cards at retail locations.

KTA does not provide customer call detail records to business customers. KTA also employs several internal operating processes and procedures to ensure compliance with KTA privacy policies which are generally in compliance with the Commission's

CPNI regulations. For instance, KTA has developed extensive and detailed employee training manuals focusing on protecting the privacy of customers. KTA has implemented and administers an employee disciplinary program to ensure compliance with internal procedures. Consequences for non-compliance include the potential termination of employees, when appropriate. KTA has established processes for resolving customer complaints regarding unauthorized access to CPNI and for identifying, responding to, documenting and, as appropriate, notifying law enforcement and customers of any breaches of customer CPNI. In addition, KTA has developed educational materials to inform customers about CPNI protections and KTA's authentication and protection practices.

Manual for CPNI Protection

2007. 10

Department of Information Protection

Table of Contents

I. Overview	
1. The Purpose of this manual-----	3
2. Basic Principle-----	3
3. Definition of CPNI-----	3
4. The people and the place it is applied to-----	3
5. Approval and examination of the manual-----	4
II. Organization for the protection of CPNI	
1. Framework to execute the CPNI protection policy-----	4
2. Mission-----	6
III. Responsibility of a CPNI treating agent and protection of customer's rights	
1. Responsibility of a CPNI treating agent-----	7
2. Protection of Customer's right-----	8
3. Education for the protection of CPNI-----	9
IV. Protection in case of collecting of using CPNI	
1. Limitation of CPNI collection and use-----	10
2. Approval of CPNI collection and use-----	11
3. Opening of CPNI treatment policy in public-----	13
4. Management of CPNI-----	14
5. Consignment of CPNI treatment-----	15
6. Analysis of probability for the infringement of CPNI-----	16

V. Protection of operating system

1. The systems to be protected-----	17
2. Authorization for the access-----	17
3. Certification for access and management of log-----	18
4. Protection of data-----	19
5. Protection of system-----	20
6. Security review for CPNI protection-----	22

VI. Investigation/Inspection about the protection of CPNI

1. Type and contents of investigation/inspection-----	24
2. Constitution of inspection unit-----	25
3. Procedure of investigation and storage of result data-----	25

VII. Customer care and process of the infringement of CPNI

1. Types and countermeasure of the infringement of CPNI-----	27
2. CPNI infringement countermeasure organization and the role-----	28
3. Recognition and countermeasure of CPNI infringement-----	28
4. Prevention activity and recurrence prevention-----	29

I. Overview

1. The Purpose of this manual

It prescribes the matters delegated by “information protection guideline, chapter2” or the matters entailed in order to execute the guideline.

2. Basic Principle

- Abiding by the statutes, codes and guidelines for the protection of CPNI
- Classifying CPNI as “class A” data based on “the guideline for information protection”, and taking managerial and technical measures that are applicable to the “class A” information

3. Definition of CPIN

- Information that exposes the identity of an individual by itself: name, residential registration No
- Information that exposes the identity of an individual if combined: Phone number and date of birth, address and date of birth
- Information that may cause financial or mental damage of an individual: account No, password, bank account No, credit card No

4. People and place it is applied to

- people
 - The employees and the management of KT
 - The People who handle the CPNI through a contract
 - The outsourced people by a contract, who develop, operate or maintain/repair systems that store or handle the CPNI regardless of their residency in KT.
- place
 - Every KT branch and agency, and any place where the business

related to KT is executed.

5. Approval and examination of the manual

○ Approval

- It should be approved by the company CPNI officer and then be officially announced to the employees and the management.

○ Examination

- It should be examined more than once a year and additionally complemented and revised in the case of as follows;
 - Significant infringement of CPNI (disclosure or falsification)
 - Introduction of certain technology that may do harm on the protection of CPNI
 - Major change of business, procedure, and technological infrastructure, mission, etc
 - Major change of information protection environment
 - Change of related statues, code or guidelines.

II. Organization for the protection of CPNI

1. Framework to execute the CPNI protection policy

Privacy officer, privacy director, and privacy ranger should be designated in order to execute the CPNI protection policy

○ Company CPNI officer: director of information protection department

- the employee in the information protection department who is in charge of CPNI protection shall mainly support the director

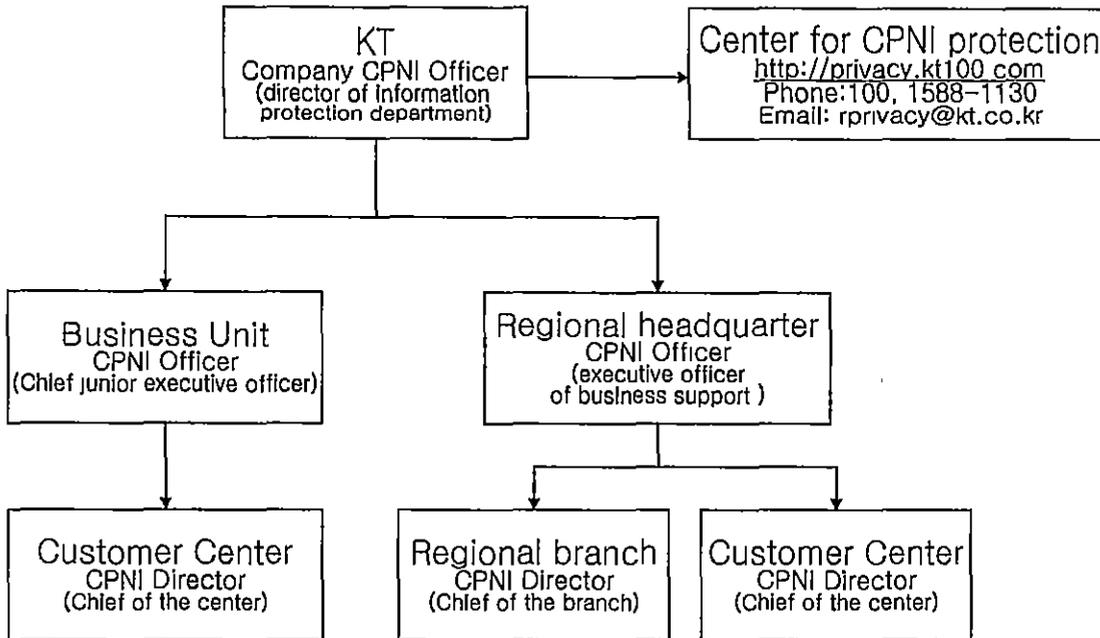
○ Sub level CPNI officer

- Every business unit in the headquarter , and regional agent who deals with CPNI, should designate their own CPNI officer
- Criteria to designate the officer
 - Each office in the main headquarter: Chief junior executive officer
 - Each regional headquarter: executive officer in charge of business support (an employee in charge of business support

may be designated only in case of Jeju branch)

- Affiliated organization: the head of the organization
- Delegation of the power and the responsibility
 - Each office in the headquarter: other executive officer than in chief, may take the power and the responsibility according to their business in charge
 - Detail scope of delegation shall be coordinated with the company CPNI officer
- CPNI Director
 - Chief of a department or an agency where handle the CPNI (by collection, input, inquiry, modification, printing, etc) for the service planning, marketing, CRM, etc
 - Office in the main headquarter, regional headquarter: designate a position in charge of the protection of CPNI
 - Affiliated organization: designate a department in charge of the protection of CPNI
- CPNI Ranger
 - CPNI director may designate a person as CPNI ranger to carry out a practical task.

[Framework for the protection of CPNI]



2. Mission

○ Mission by positions

Position	Mission
Company CPNI Officer	- Representing the company on the issue of CPNI - Responsible for the overall matters on the CPNI <ul style="list-style-type: none"> • Providing a vision and a strategic plan on the protection of CPNI • Educating employees on the protection of CPNI • Managing and auditing on all the tasks over the company about protecting CPNI
Sub CPNI Officer	- Responsible for the CPNI matters in charge <ul style="list-style-type: none"> • Providing a vision and a strategic plan on the protection of CPNI when executing a business • Educating employees on the protection of CPNI • Managing and auditing on the tasks about protecting CPNI

	<ul style="list-style-type: none"> • Analyzing causes of CPNI infringement and design a plan to prevent a recurrence * a chief of regional headquarter are responsible for the overall matter on the CPNI issue, but CPNI ranger may execute practical tasks
CPNI Director	<ul style="list-style-type: none"> - Managing an accessibility over the CPNI(permit/level of permit/block, etc) - examining appropriateness on producing, using(inquiry, printing, sampling), utilizing(telemarketing, PR), and providing alliances/affiliated companies with CPNI - periodically examining the CPNI access records(logging and printing history books)

III. Responsibility of a CPNI treating agent and protection of customer's rights

1. Responsibility of a CPNI treating agent

1) Prohibition of CPNI disclosure, misusing and abusing.

○ None who treats CPNI may utilize CPNI for the purpose of illegal disclosure, modification or personal needs, the CPNI that one obtained through their business.

- Illegal disclosure includes printing, saving on storing media such as discs or CD, writing on paper, and sending/forwarding an email

○ None can collect or utilize CPNI under the name of KT without KT's apparent permit; none can shift responsibility on KT for the unauthorized usage.

2) Writing a pledge about the CPNI treatment.

○ All the employees and agents who treat the CPNI of KT customers should write a pledge about the responsibility for the protection of CPNI.

○ All the employees and agents who treat the CPNI of KT customers should have training as to when/when not to use CPNI and disciplinary plan for violations of procedure. Employees who violate it should have retraining.

○ Time to writing a pledge and management of pledges

Life is wonderful **KT**

- Sub CPNI officer should annually collect pledges until the end of the first quarter
- Employees who are newly admitted or transferred should write a pledge right after the personnel order
- The pledges should be safely stored in the cabinet that can be locked
- The pledge form follow "the guideline for information protection"

3) Protection of customer's PIN and password

○ Inform customers that they should designate their own PIN and password

- Inform customers about how to safely manage their own PIN and password such as a rule of creating a PIN and importance of periodical change of password
- Inform customers that they should change their password in case their password was disclosed to other people

○ Filter certain passwords that are vulnerable to particular systems

4) Prohibition of CPNI sharing

○ Prohibition of sharing files or folders that are saved on the PC for business use

- It includes uploading a CPNI on the web disc or internet bulletin board
- If it is necessary to share a certain information for certain business purposes, it can be shared during the limited amount of time by using password and the sharing setup should be canceled right after the business purpose is achieved

○ Prevention of possibility of unintentional disclosure of CPNI

- Using a dangerous service such as P2P, with a PC that has CPNI or PC for business use, is prohibited

2. Protection of Customer's right

1) Approval or withdrawal of CPNI collection and use.

○ Customers can request approval or withdrawal of approval on the

consignment of their own CPNI and its provision to the third party.

○ Department of customer service or department of product planning should build up a system that can immediately respond to customers' request on the approval or withdrawal through phone, email, or homepage.

2) Access to one's own CPNI and inquiry of detailed history of its use

○ Department of customer service or department of product planning should educate their employees and build up a function in their system, the function that allows customers to access to their own CPNI and to modify it if necessary and the function that provides customer with detailed history of its use and provision to the third party. The record should be maintained at least for 1 year.

3) Protection of children under 14

○ Approval from a legal representative is needed when collecting, utilizing and providing the third party with CPNI from children under 14

○ A minimum amount of information about a legal representative should be requested when getting an approval and the personal information of the legal representative should be used only for the purpose of approval.

○ A legal representative should be allowed to have the same right to give an approval or ask withdrawal of one's own CPNI collection and use, and to access to and modify one's own CPNI as the principal of CPNI.

○ A department of business planning that provides children under 14 with a service should establish a institution and detailed policies to protect them based on the related statues, code, guideline, and this manual.

4) Protection of teenagers on the internet

○ Designation of teenager protection officers and their mission

- A chief of a department that deals with tasks related to teenagers protection should designate a teenager protection officer in order to block and manage harmful information and to design a plan to protect teenagers

- A teenager protection officer should take a measure to block and delete a teenager-harmful media but contents and procedure of such a measure should be prescribed in the contract.

○ Prohibition of advertisement for the teenager-harmful media

- An advertisement that is prohibited based on the "Teenager Protection Act" cannot be translated through the internet nor be displayed without limiting teenager's access.

3. Education for the protection of CPNI

1) Education of CPNI rangers.

- Hosting agency: Department of information protection (DIP)
- Education period:
 - Official education: more than once a year
 - Special education: when some issues about CPNI protection are raised
- Target: CPNI rangers by fields
- Contents:
 - Related statutes
 - Codes, guidelines, and manuals on the protection of CPNI
 - Response plan in case of the CPNI infringement or disclosure
- Distribution of educational materials:
 - Periodical articles or special ones can be distributed by the DIP.

2) Education of employees or agencies who treat CPNI

- DPI may design a plan and execute it to educate all the employees, management and consigned agencies, if necessary.
- DPI may add a CPNI protection education to the education for the promoted, the newly recruited, or the experienced.
- Sub CPNI officers should complete a course for the protection of CPNI protection and educate their subordinates and consigned agencies.
- When a issue about CPNI protection is raised, sub CPNI officers should educate their subordinates and consigned agencies based on the materials that DPI distributed.

IV. Protection in case of collecting of using CPNI

1. Limitation of CPNI collection and use

1) Limitation of CPNI collection

○ Limitation of CPNI collection : minimum amount of information should be collected only in case of

- Carrying out a contract for service provision
- Billing
- Or managing signed-in subscribers of homepage

○ In the case of other else, CPNI should be collected after getting an approval from the customers to whom the purpose of collection and use should be explained.

○ The items of basic collection and of optional collection should be easily discernible.

○ Service request should not be rejected only because customers don't give an approval for the optional information collection.

○ Prohibition of information collection that can infringe human right

- Race or ethnicity
- Ideology or faith
- Hometown
- Political inclination or criminal history
- Medical history, health information

2) Limitation of CPNI use

○ Use of CPNI should be limited within the scope of customer's approval and an approval from sub CPNI officer is also needed.

○ When providing the third party with CPNI on the purpose of the business itself or an extra profit, CPNI should be used within the scope of customer's approval about the recipients, the purpose of the use, the items provided.

○ Providing criminal investigation agencies with CPNI according to the "guideline for information protection" that is based on the "Telecommunication Business Act" and "Communication Privacy Act"

○ When customers requested to modify their information, the use of CPNI is prohibited until the modification is completed.

2. Approval of CPNI collection and use

1) Ways to get an approval for CPNI collection and use

- Notifying and getting an approval in writing
 - Explain detailed points of a “written consent for the collection and the use of CPNI” to customers, the consent whose form is attached to a “request form for subscription” or a “request for change of user’s name”, and customer’s signature is also needed.
 - Customers can submit the form by fax or mail.
 - Notifying and getting an approval by telephone and voice record
 - Explain detailed points of a “notice about the collection and the use of CPNI” to customers by telephone, or lead customers to read a “guideline of CPNI treatment” that is on the company homepage (<http://www.kt.co.kr>), and then acquire a oral consent by telephone.
 - Notifying and getting an approval by internet or email
 - Post a “notice about the collection and the use of CPNI” on the internet homepage and let customers to mark whether they agree or not.
 - Send an email that include a “notice about the collection and the use of CPNI” and get a return main that has customer’s consent.
 - Notifying and getting an approval by other ways
 - When it is very hard to explain all the contents of the notice due to the feature of certain media, an approval can be gotten only by notifying how to get detailed information through the internet or telephone.
- 2) Acquisition of approvals and management of evidential references**
- When subscribing with written forms
 - After a customer gives a signature for the agreement of CPNI provision, give a copy back to the customer and send the original copy to the image management center (IMG)
 - An original copy and a electronic copy should be stored and managed base on the related guidelines.
 - * A sending period can be flexibly decided within 3 months after due consideration of related equipments and response quality to the customers’ claims.

- When subscribing by telephone (by Inbound call or by telemarketing)
 - When collecting CPNI, employees of Call-center or telemarketers should explain detailed point of the notice to customers and should get an approval with recording the conversation of the call.
 - Recorded conversation should be submitted to KT based on the related guidelines.
 - * A department of service or product planning should write and print a documented notice or establish criteria to post a notice on the product web pages.
 - * When customers subscribe by phones, it may establish an alternate plan such as sending a notice by mail or notifying it on the company homepage

3) An approval to transmit commercial purposed information

○ When commercial information that is allowed based on the “article 52 of Information and Communication Network Act” is sent to customers, Customers’ privacy should not be infringed. And the transmission or the information should be stopped immediately if a customer requested to do so.

- When commercial information is transmitted, an [Advertisement] sign must be attached on the subject and managerial and technical countermeasure should be prepared for customers to be able to deny it for free.

4) Review of “subscription request form” and “notice about the collection and the use of CPNI”

- A department of service or product planning may request a consultation from the company CPNI officer to review the form and the notice if they are legally appropriate or not.

3. Opening of the CPNI treatment policy in public

1) Notification of the CPNI treatment policy

- Obligation to open the CPNI treatment policy
 - It should be made and be opened to the public to make customers to easily access to it. And it should be notified to

customers when it is changed.

- Things to be included in the CPNI treatment policy
 - The purpose of the CPNI collection and use, items of CPNI collected, and collecting method.
 - In case of providing the third party with CPNI: recipients' names, recipients' purpose of use, and detailed CPNI item provided.
 - The period during which CPNI is stored and used, the procedure and method of CPNI destruction, legal basis and detailed item list to be kept when stored.
 - Detailed tasks to be consigned and the name of consignees
 - Rights of users or legal representatives, and its execution procedure
 - Information about installation and operation of a system that automatically collects CPNI, and about its denial
 - Name of CPNI officer, title and contact information of CPNI related business unit.
- Ways to open the policy in public
 - Display it on the main page of internet homepage or on the directly linked page from the main page
 - Post it on the bulletin board or wall of office where customers can easily find it
 - Publish it consecutively more than twice on periodicals, news letters, pamphlets, or bills.
- Ways to notify the policy when it is changed
 - Display it on the public announcement section of the main home page or on the pop-up window.
 - By mail, fax, email, or by other similar methods
 - Post it on the bulletin board or wall of office where customers can easily find it

2) Electronic notification of the CPNI treatment policy

- Not only a documented paper copy of the policy but also a electronic copy should be available on the homepage
 - Refer to <http://www.kisa.or.kr>

4. Management of CPNI

1) Confirming of one's identity and managing of materials

○ Confirm customer's identity when treating a task that may cause financial or mental damage with errors during the treatment for the service subscription/change request. The related materials that include CPNI such as request form and a copy of ID, should be safely stored in the cabinet locked

○ The information that is utilized for the identity confirmation should be limited to a minimum.

○ CPNI should keep updated correctly.

2) Producing and storing of CPNI

○ CPNI cannot be produced or stored on the PC, shared server, or homepage.

○ Only if it is sure to be necessary for business, it can be produced and stored with the approval from the CPNI director, and managerial measures should be prepared to protect CPNI, and CPNI should be treated as A class data based on the manual.

- CPNI should be encrypted if it is hard to treat CPNI as A Class.

3) Protection of CPNI when printing or copying

○ An approval from CPNI officer in charge should be acquired when printing, or copying (including download) CPNI.

○ Login history should be stored

○ Modification during printing or copying should be prohibited and technical protection method should be applied for only approved person to get an access.

○ Following items should be managed specially

- Serial number of printed/copied file
- Format/date/purpose of printed/copied file
- Belonged unit/name of a person who printed/copied a file
- Name of recipient of printed/copied file
- Terminated date and the name of a person in charge of the termination

○ Following items should be managed specially

- If DRM is established, prior approval can be replaced with post review.

5. Consignment of CPNI treatment

1) Items that should be included in a contract

- Obligation to abide by related statutes and other codes of KT
- Prohibition of abuse of CPNI including disclosure and illegal modification
- Prohibition of provision to the third party
- Qualification of employee who is dispatched to KT
- Collection of a pledge from the employees and education of them
- Periodical review on the actual condition of CPNI treatment
- Consent for the investigation and the report in case of disclosure of CPNI
- Obligation to take a technical measure for the CPNI protection
- Clarification of responsibility: penalty can be imposed in case of violation of related statutes and codes, the penalty that includes a cancellation of contract and compensation for damages.

2) Notification of details consigned

- When a certain business is consigned to others, details related to CPNI treatment should be notified through guidelines or subscription request form.

3) Direction and supervision of consigned company

- Proper education, periodical review should be executed for the employees and management of consigned company to abide by related statutes, guideline, and manual.
- The access authorization to the KT's information system for the employees and management of consigned company should be managed based on this manual "Chapter V-2" and the authorization list should be reported to the CPNI director.

- The access authorization should be limited in case of personnel change.

4) Other matters related CPNI consignment should be treated based on the "guideline of information protection" and the "code of security"

6. Analysis of probability for the infringement of CPNI

1) VOC Analysis

○ More than once a quarter, the company CPNI officer should analyze VOC that is classified as CPNI disclosure.

○ The countermeasure should be taken after the VOC analysis so that similar complaints should not be made. Special review should be executed in case potential risk of infringement is detected.

2) Acceptance of complaints from outer agencies

○ Analyze the complaints and take a countermeasure to prevent them from recurring if it is necessary.

V. Protection of operating system

1. The systems to be protected

- A system that includes CPNI
- A system that include an information that is collected providing with a certain service: recorded voice, customers' individual information collected confirming their identity
- A system that has the function of input, inquiry, searching, and sampling, and printing of CPNI
- A system that maintain records of breaches, notification to law enforcement, customer notification, for at least 2 years. Include dates, description of CPNI involved and circumstances of breach

2. Authorization for the access

1) For users who treat CPNI

- The CPNI officer whose business unit treats CPNI can authorize the access to their system.
 - PINs should be issued minimally
 - Login history should be stored for 5 years
 - Authorization should be changed or canceled in case of personnel change
 - Data accessed should be differentiated according to the feature of tasks

○ Users who treat CPNI cannot utilize the authorization for the other purpose than its original purpose, a PIN and a password should be managed based on the "guideline of information protection"

2) For developers and operators of the system that treats CPNI

- The CPNI officer whose unit has developers and operators of systems that treats CPNI, can authorize the access to their system.
 - PINs should be issued minimally
 - Login history should be stored for 5 years
 - Authorization should be changed or canceled in case of personnel change

- A system for developing and testing should be separated from the operating system and its data so that CPNI would not be disclosed

- Developers and operators cannot utilize the authorization for the other purpose than its original purpose, a PIN and a password should be managed based on the "guideline of information protection"

3) For operators of the system that holds CPNI (including DB operator)

- The CPNI officer whose unit has operators of systems that holds CPNI, can authorize the access to their system.

- PINs should be issued minimally
- Login history should be stored for 5 years
- Authorization should be changed or canceled in case of personnel change
- Authorization for the operators should be limited to the minimum and a system to review the abuse of the authorization should be established and operated.

- Developers and operators cannot utilize the authorization for the other purpose than its original purpose, a PIN and a password should be managed based on the "guideline of information protection"

3. Certification for access and management of log

1) Certification for access

- The access to CPNI should be given by inputting PIN and password, but using more complicating certification method is recommended.

2) Management of log

- Things to be recorded: time and date of log in and out, detailed working history such as modification, deletion and print of CPNI, IP address of whom log in

- Prevention of falsification and alteration: log file should not be inquired, printed or modified by other than purpose of backup

- Log storing: It should be periodically stored on media such as CD-Rom that be rewritten.

- Backup media should be stored in a restricted area and access to it should be gained only by approval

- Period to store: backup log should be stored for 5 years

4. Protection of data

1) Hiding the important data

○ Among stored CPNI, data that identify customers such as password should be encrypted in one-way.

- In case of certification, data that customers input should be encrypted in one-way and it should be compared with original key.
- In case of password lost, password should be reset after confirming the identity and the default password should be sent to customers encouraging them to change it.
- If the default password would not be changed for a certain period, the access should be rejected.

○ Saving of important CPNI on PCs should be limited to the minimum and it should be saved in a encrypted format under the approval of the CPNI officer

○ Important data should be masked when they are treated in the CPNI system

- Residential registration No, banking information, password, etc should be masked
- In other case, it may be masked according to the purpose of tasks (a separate guideline that give a criteria for masking should be made)

2) Managing CPNI of terminated customers

○ CPNI of terminated customers should be managed in a separate table from that of current customers

- CPNI of terminated customers can be inquired and provided only by customer's complaints or related statutes.
- Authorization of access to it is limited to only minimal number of people necessary

○ Permit access to CPNI of terminated customers

- Access to it is permitted only be approval of CPNI officer

○ Period to store CPNI of terminated customers

- It should be deleted periodically by the related statutes such as

Commercial Act and Corporate Tax Act(more than once/month)

- It can be stored for 5 years after termination, but in case of delinquency, it can be stored until the payment

3) Destruction of CPNI

- CPNI whose purpose of collection/use is terminated should be deleted
 - Exception: when customers approve or related statutes allow it
- When the Media that holds CPNI is changed into new ones due to the expiration of use-by date or the occurrence of a defect, the current media should be destructed irrecoverably.
 - PC and window server: use a solution for pc format that is distributed based on "manual for internal PC management"
 - S.W(safe disk deletion) is distributed to S/W manager of each business unit or CPNI manager of regional headquarter and customer service center
 - Hard Disk for server or other storage: low format or completely destroy data by using such equipment as Degausser that deletes data with electronic signal
 - * Degausser: equipment to delete data in magnetic tape or disc media
- Paper on which CPNI is printed should be destroyed with a shredder or be incinerated

5. Protection of system

1) Protection of the system that holds or treats CPNI

- A system that holds or treats CPNI should be protected with a firewall, an intrusion detection system, etc
- A operating unit whose system holds or treats CPNI should periodically make a diagnosis of security weakness, and strengthen a prevention activity against web-viruses

2) Protection by employees who treats CPNI

- Copying and interconnecting of data should be limited to the minimum and only minimal data that is needed for business can be transmitted
- When important CPNI is transmitted through other networks than KT intranet, it should be protected by encoding
 - When interconnection system can not be encoded
 - CPNI should be interconnected through dedicated lines or its

transmission may be approved only if the interconnected system is not open to the outer network such as the internet.

3) Protection by the unit in charge of homepage management

○ A homepage that is operated on the basis of membership should be classified as a system that holds and treats CPNI, and managerial and technical measures should be taken for it as an equivalent system

○ "A manager in charge of homepage membership" who treats complaints about CPNI from the use of homepage, should be designated.

○ "A guideline to treats CPNI" should be posted on the homepage

○ In case of change of the guideline, the reason and contents of the change should be notified to customers

○ When a service contract is contracted or a financial service is provided through the homepage, an identity should be confirmed with PIN and password or a public key certificate.

○ Things to be included in the guideline

- The purpose of collection of CPNI from the homepage and the scope of the use
- CPNI officer
 - Affiliation and name: a department of information protection
 - Contact mail: privacy@kt.co.kr
- CPNI director and ranger
 - Affiliation, position, name, email address, and phone number
- Information about operating a access information file(Cookie)
- The purpose of provision and the detailed item provided in case of provision to affiliated or allied companies.
- The method to agree or to reject in case of provision to affiliated or allied companies.
- A period of CPNI storing and using
- The right of a legal representative and the method to exercise the right in case of collection of CPNI under 14
- Information about treatment of complaints related to CPNI: inform customers of CPNI director and ranger's contact info.
- Detailed technical method to protect a homepage
Ex) about firewall, encoding, encryption, etc

- Measures to protect a homepage from intrusion based on the “guideline of information protection”

4) Security management of PCs related to CPNI

- Prevention from worm viruses and disclosure should be based on the “guideline of information protection” and the “manual for internal PC management”

6. Security review for CPNI protection

1) The Conditions for the security review

The security review should be requested to the company CPNI officer in case of as follows

- When newly establishing a system that holds and treats CPNI
- When using a technique that may cause infringement of privacy
- When changing a current system that holds and treats CPNI
- When interconnecting systems or providing the third party with CPNI
- When requesting a security review due to the development of a new

system, CPNI related security review can be also requested together

2) Documents to be submitted when requesting a security review

- A business plan
- A business process flow chart for a system
- A flow chart of CPNI: in order to analyze CPNI by the steps
- The whole configuration chart

3) Method of security review

- A unit to whom a security review requested should develop and utilize a check list referring to the “guideline of CPNI security review” by KISA (Korean Information Security Agency)

- A security review can be executed with KISA and the ministry of information and communication (MIC) when a trouble is expected by related statuses.

4) Carrier’s responsibility of security

- Carrier files annual compliance certification.
- Carrier must notify FCC of any failure of opt-out mechanisms within 5 days.
- Carrier must notify US Secret Service and FBI within 7 days of CPNI

breach.

○ Carrier has to notify customer at least 7 days after law enforcement informed, except when "urgent notification" is necessary.

5) Breach of CPNI Privacy

○ In the event KTA experiences a privacy breach and CPNI is disclosed to unauthorized persons, federal rules require KTA to report such breaches to law enforcement. Specifically, KTA will notify law enforcement no later than seven (7) business days after a reasonable determination that such breach has occurred by sending electronic notification through a central reporting facility to the United States Secret Service and the FBI. A link to the reporting facility can be found at: www.fcc.gov/eb/cpni. KTA cannot inform its Customers of the CPNI breach until at least seven (7) days after notification has been sent to law enforcement, unless the law enforcement agent tells the carrier to postpone disclosure pending investigation. Additionally, KTA is required to maintain records of any discovered breaches, the date that KTA discovered the breach, the date carriers notified law enforcement and copies of the notifications to law enforcement, a detailed description of the CPNI breach, including the circumstances of the breach, and law enforcement's response (if any) to the reported breach. KTA will retain these records for a period of not less than two (2) years.

VI. Investigation/Inspection about the protection of CPNI

1. Type and Contents of Investigation/Inspection

1) Periodic Investigation/Inspection

- Period: More than one (1) time per year
- Target: Working process and systems of department dealing with the CPNI; Target is selected according to the following criteria
 - Organization which has received multiple customer complaints directly or through outside organizations with regard to CPNI outflow.
 - Organization which has been unsuccessful in addressing issues for

which it has received correction orders from KCC (Korean Communications Committee) or the National Assembly as a result of inspection.

- System that has been reported as being in the urgent need for technical protection for safeguard of CPNI.
- Organization which has low participation rate in CPNI education.
- Organization which has announced the completion of system that is used for storage and process of CPNI, but has not performed the pre security review (the protection of CPNI field).
- Organization which has not been a target of periodic investigation or inspection for 3 years in the past.

2) Non-Periodic Investigation/Inspection

○ Condition

- Preparation for inspection or investigation by outer organization such as the KCC or the National Assembly.
- When a new intrusion method is known with regards to CPNI.
- When change of business environment such as the law amendment calls for a response from CPNI perspective.
- When a complaint regarding CPNI disclosure is received.
- When a person in charge of CPNI deems it necessary.

○ Target

- Department, Organization or system in accordance with the condition

3) What to inspect (Periodic and non-periodic Inspection/Investigation)

- Establishment and Compliance of the CPNI manual and procedure
- Compliance of manual regarding collection, utilization, and termination of the CPNI
- Observance of the statutes
- Managerial treatment
 - A written pledge of security
 - Education about the protection of CPNI
- Technical treatment of the CPNI management system
 - Management of access authority
 - Limitation of access to critical data

Life is wonderful **KT**

- Approval in sampling and providing data
- Logging in for access to critical data
- Execution of security review when planning and developing system

2. Constitution of Inspection Unit

- Host of investigation/Inspection: Department of information protection
 - Form a joint investigation unit with experts from other organization when needed

3. Procedure of investigation/inspection and storage of result data

1) Investigation/inspection planning

- The hosting organization, in the event of periodic investigation, establishes a plan (Investigation/Inspection) and obtains approval from the person in charge of company's CPNI and then notifies the target organization.
- The investigation plan specifies scope of audit, target, period, auditor, and audit method.
- Use of check list is required.
- Report the investigation result immediately to the person in charge of company's CPNI
- In case a threat is expected due to the severe violation revealed in the non-periodic investigation, report to the committee of CPNI and set up a countermeasure plan.

2) Protection of data of investigation result

- All data that were generated from system investigation, such as a list of screen dump, system log, and collected evidence.
- Audit result report.

3) Method of data storage

- Printed data and evidence: Store in the access controlled documentation room or a cabinet with a lock
- File type data: Save in a PC or a shared server on which the documentation security or PC security solution has been installed with

individual password set up.

- Control of access to the storage server
 - Access right granted only to the department in charge of CPNI inspection.
 - Appoint the server administrator and have the server run by the administrator.
 - Server to be connected to intranet only when needed; in general, server not to be connected to network.
 - Server access account to be issued with the department manager's approval.
 - Any search of inspection result data open to all members of department; generation and modification of such data to be done only by a person who participated in relevant inspections.
- Maintenance of data storage cabinet
 - The department security personnel keep the key.
 - Data in the cabinet to be viewed after obtaining department manager's approval.
 - Create and maintain a log for accessing cabinet data.

VII. Customer Care and Process of the infringement of CPNI

1. Types and countermeasure of the infringement of CPNI

1) Types of the infringement of CPNI

- Disclosure of CPNI
- Modification and termination of CPNI
- Access to the service made impossible due to hacking, worm, virus and etc.

* Access to the service made impossible due to hacking, worm, virus, and etc. is classified as an infringement of network or system.

2) Definition of infringement level and countermeasure

× Follows the definition of the enterprise risk management process

Level	Definition of infringement level	Countermeasure

Normal	Simple suspicion about information disclosure or a case that is solved by the customer service agent	Taken care by customer care department
Warning	Disclosure of small amount of CPNI data repeatedly occurs for the similar purpose, or correction order by the KCC or complaint by citizen's group has been received.	Report to customer care department and all related department as well. Countermeasure taken with department of information protection in charge.
Emergency	Disclosure of large amount of CPNI occurs and as a result legal suit arises for monetary compensation or criminal prosecution, or KCC imposes fine for the matter.	Enterprise risk countermeasure team lead by Corporate Risk Officer take care of customer complaints and press issues.

2. CPNI infringement countermeasure organization and the role

1) Countermeasure organization and role (Refer to the attachment 1)

- Department of Information protection: Managing entire process
- Press Relations team: Respond to and communicate with press
- Department of Business Cooperation: Respond to and communicate with government and citizen's group
- Judicial affair team: Countermeasure to law suit
- Department of IT, Department of Network Service: Recovery of infringed system and supplementation of vulnerability

- The department that receives a report of infringement: Direct countermeasure to customer complaint and report to the person in charge of CPNI according to the reporting scheme by infringement level.

2) Operation of infringement reporting center

Medium	Number or Address	Responsible Unit
Report of CPNI infringement by a telephone	100 or 1588-1130 (Regional branch office or customer service center)	Customer center (After receiving the 1 st report, issue a VOC and transfer to the responsible unit)
e-Mail	privacy@kt.co.kr	Department of Information Protection
web	File a complaint at http://www.kt100.com	Department of Marketing

3. Recognition and countermeasure of CPNI infringement

1) Recognition of infringement through self-inspection, periodic, and non-periodic inspection

- Analyze probability of CPNI infringement through periodic analysis of access log for CPNI, and VOC
- In case an infringement is confirmed
 - Take a countermeasure according to the infringement level, by forming a CPNI infringement countermeasure team lead by a responsible department, performing an investigation and recovering the system.
 - Compensate for customer's psychological and physical damage.

2) Customer's complaint for report from other organizations

- Upon receiving complaints from customer: Analyze complaints and process by the infringement level.
- Upon receiving infringement notice from the KCC, KISA, and Cyber Criminal Investigation Unit: process the infringement according to the infringement level in cooperation with related departments.

4. Prevention activity and recurrence prevention

1) Operation of simulation training

- Host: Department of Information Protection
- Period: One (1) time per every year
- Target: Departments that manage and handle CPNI
- Contents: Simulation training based on the scenario of CPNI infringement

2) Recurrence prevention

- The head department of CPNI protection to analyze the cause establishes a countermeasure plan, and performs education for the recurrence prevention.
- The recurrence prevention plan may include setting up a guideline, amendment of the manual, and improvement of work process.

[Attachment 1]

Risk Management System of the protection of CPNI

