First Financial Holding Co., Ltd. & Subsidiaries
Information Management Regulations

Section 1 General Provisions

1. These Information Management Regulations (hereinafter referred to as this "Regulations") are established in accordance with the "Information Management Policy and Guideline" of this Company to ensure the security of the information operating systems, information equipment, information networks, and data; to strengthen internal control; and to comply with laws and regulations relating to information management.
2. Referenced documents
   (1) Government laws and regulations relating to information management, e.g. the "**Personal Information Protection Act**", "Financial Holding Company Act", "Self-Discipline Standards for Financial Holding Companies and Subsidiaries", and regulations specified by financial competent authorities.
   (2) Specifications and standards of international organizations and government, enterprise, and bank organizations and associations.
   (3) "Information Management Policy and Guideline" of this Company.
   (4) General information security standards or awareness among enterprises.
3. Scope of information management
   (1) Software management
   (2) Hardware and environment management
   (3) Network management
   (4) Internet application management
   (5) Email management
   (6) Data and document management
   (7) Information personnel management
   (8) Emergency response management
   (9) Information system continuity planning
4. Each subsidiary shall establish or revise regulations relating to information management in accordance with these Regulations and in coordination with its operating environment and business needs.

Section 2 Financial Holding Information Management

Chapter 1 Control of Application Systems

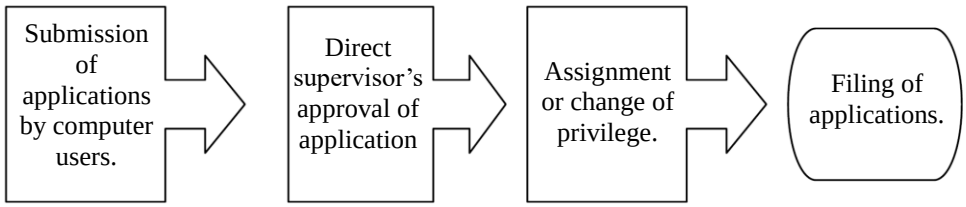
1. Privilege to access application systems

   The "Application System User Privilege Assignment and Change Application Procedure" is established to control the use of the business application systems of this Company.

   (1) After assigning to a new job requiring the use of application systems, employees shall complete the "Application System User Privilege Assignment and Change Application" (Form 1) to apply for the privilege to use relevant applications (APs).

      1) Employees requiring privilege to use APs shall complete the "Application System User Privilege Assignment and Change Application" and submit the form to their direct supervisor for approval before handling the form over to the registration unit to assign or change their AP privilege.

      2) After the registration made according to the information contained in the approved application form, the registration unit shall submit the form to the department chief for review before filing.



   (2) Assign appropriate privilege based on the approval of the applicant (employee)'s direct supervisor.

   (3) After the first-time login, employees must change their passwords before they can continue to use the AP. A password shall consist of six or more characters, including letters and non-letters.

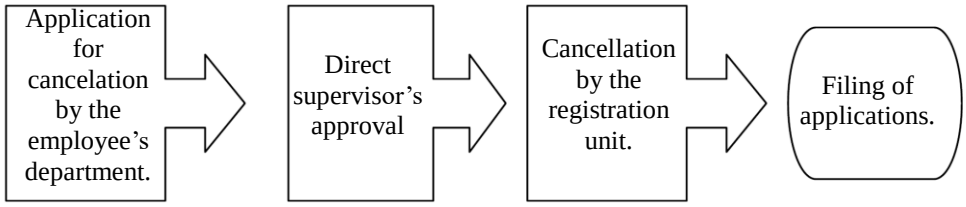
   (4) A user account will be locked after five login failures. A user must ask the system administrator to unlock the account. The system administrator shall find out and verify the cause(s) of login failures before unlocking an account.

   (5) When an employee resigns (including retirement), his/her AP privilege will be canceled on the effective date of resignation. The department of that employee shall apply for privilege cancellation according to the following procedures:

      1) When an employee resigns, the employee's department (or the employee) must complete an application form and submit the form to the direct supervisor for approval before handing it over to the registration unit to cancel his/her privilege.

      2) After cancelling the privilege of the applicant, the registration unit shall submit the

application form to the department chief for review before filing the form.



(6) Where an AP system is an externally developed (package) system with a dedicated user management mechanism, cancel privilege according to that mechanism.

2. Implementation and going live of new systems

(1) Information security needs shall be considered in the development of new APs. User tests and acceptance shall be implemented prior to system going live. Approvals shall be obtained prior to system going live.

(2) The access privilege of computer software shall be assigned to users and administrators based on the functions and nature of use in accordance with the division of administration and utilization principle.

(3) When purchasing computer software, applicants shall consider its security and obtain an approval prior to use.

3. Database management

(1) Database space allocation shall include space for files used in official operation and test operation. Privilege of the official operation database shall be assigned based on the nature of data.

(2) Dedicated personnel shall be assigned to maintain and administer database systems and adjust their performance at appropriate times.

(3) The construction, definition, architecture, or access privilege change of an official operation database shall be approved prior to implementation.

(4) The backup cycle and disaster recovery procedure of the official operation database shall be defined appropriate to the type and importance of the data stored inside. A database stored in other storage media for backup purpose is considered as a media file.

(5) When applying for the access privilege of official operation database, the "Application System User Privilege Assignment and Change Application Procedure" shall apply.

4. Program maintenance and change

(1) When a department needs to change (including addition and change) an application or program for business purpose, it shall complete the "AP System/Program Change Application" (Form 2) to specify the basis and content of change. After obtaining the supervisor's approval, this department shall hand over the form to the system development (maintenance) unit or outsourced developer (maintenance provider) to add or modify the program.

(2) After adding or modifying a program, run a test and the acceptance with the user

department before applying for use in the official operating environment.

(3) Before and after the change, inform relevant units or personnel of the change based on the actual operational needs.

(4) Where a change shall be suspended or terminated for special reasons in the process, the suspension or termination shall be approved by the applicant's chief in advance.

(5) Where an immediate change is required for an emergency or business needs, an applicant may make an oral application, implement the change with the chief's approval in advance, and supplement official application documents afterward for future references.

(6) A recovery procedure shall be considered for every change to facilitate quick recovery to normal operation after an operational error.

5. Data content change

(1) Where a department needs to add or change data to or in a computer file, it shall apply for appropriate user privilege.

(2) Where a department must change the data of a computer file not covered by the scope of computer authorization due to business needs, it shall complete the "Computer File Data Change Application" (Form 3) to specify the reason(s) for change and submit relevant documents. After obtaining the supervisor's approval, send the approved application to the Electronic Information Division to process the change.

Chapter 2 Hardware and environment management

1. Equipment security management
   (1) After completing the acceptance procedure, computer equipment shall be registered in the register for management and inventoried biannually.
   (2) Equipment maintenance
      1) Equipment maintenance shall only be implemented by authorized maintenance personnel. Users shall confirm their identity in advance and escort them throughout the maintenance.
      2) After repairing or maintaining computer equipment, maintenance personnel of the service provider shall keep a maintenance record for future reference. The records provided by the supplier can be used. Maintenance personnel may also use the maintenance record (Form 4) of this Company.
   (3) Security management of equipment placing in external space

      The same information security management and licensing regulations shall apply to computer equipment installed outside of this company to support business operations.
   (4) Security measures for equipment replacement and relocation

      Prior to replacement, confidential, sensitive data and licensed software contained in equipment with storage media shall be removed.

2. Environment management
   (1) A datacenter is a restricted area.
   (2) Security management of datacenters
      1) Access control measures shall apply to all datacenters to ensure that only authorized personnel can enter a datacenter.
      2) Visitors can enter a datacenter only with an authorization. The entry and exit time shall be recorded.
      3) The datacenter access privilege of employees shall be cancelled after their resignation.
      4) IT support personnel or maintenance service personnel can only enter a datacenter at the request or with an authorization. Their activities inside the datacenter shall be limited (e.g. access to sensitive data) and supervised.
      5) No smoking and eating is allowed inside a datacenter and potentially flammable or explosive objects are strictly prohibited in a datacenter.
      6) Fire equipment using as CO2, alkyl halides (halon or new halon), or other gas fire extinguishing chemicals that will not harm other computer equipment shall be used in a datacenter. Gas leakage shall be checked at least once a month.
   (3) Property management

      Employees shall not bring computer equipment, data or software outside of the office

without prior permission.

Chapter 3 Network management

1. Network security planning and management
   (1) Network security planning
      1) Security protection measure shall be taken when transmitting sensitive information via public networks in order to protect the integrity and confidentiality of data in public network transmission and the security of the connected system.
      2) The information department shall plan, implement, and manage the portal of this Company.
      3) Prior approval shall be obtained where necessary when linking the host or network equipment of an external network system to the intranet.
   (2) Security protection of web servers
      1) Users shall apply for web services in writing and operate in the network environment after obtaining an approval.
      2) In addition to the existing security settings of the operating system, identity authentication and privilege control mechanisms shall be established on web servers for official operation and storing important data to prevent illegal users from logging in to the server to steal and damage data inside.
   (3) Firewalls shall be installed to segregate and protect connections between the intranet and the internet.
   (4) Virus prevention measures shall be adopted and updated regularly to strengthen network security protection.
   (5) Confidential and sensitive data or documents shall not be stored in information systems intended for external uses.
   (6) Redundancy of network equipment and systems
      1) Network hardware equipment shall be equipped with a UPS to prevent unexpected power outage.
      2) System backup copies shall be made for firewalls and servers of the network system.
2. Network security audit
   (1) Records shall be maintained for the operation of important network equipment for future reference.
   (2) Personnel shall immediately report network intrusion behaviors involving threats to theft, damage or illegal acts for management.
3. Management of network access
   (1) Management of network use
      1) Personnel shall abide by relevant regulations and the scope of authorization while using any computer resources over the network.
      2) Personnel shall not transmit information violating the copyright law and relevant laws and regulations over the network.

(2) Identification of user identity

A remote user identification mechanism shall be established for public networks for use by non-organizational users or linking to the corporate network from an extranet to reduce the risk of unauthorized system access.

(3) Control of network connections

The scope of web services for cross-organizational network systems shall be limited.

4. When using the network equipment of a subsidiary or assigning a subsidiary to maintain network equipment, follow its regulations relating to network uses.

Chapter 4 Webpage management

1. **When a unit needs to post contents on the corporate website, please follow the regulations for content posting management.**

Chapter 5 Email management

1. Application and activation
   (1) Emails shall be set on the "one unit one account" principle. A unit may set additional email accounts for business needs.
   (2) Active employees of this Company shall complete the "Internet Account Application" (Form 6) or use the on-line application on the intranet when applying for an email account. After reviewing and registering, the Electronic Information Division will release an email account to the applicant in two workdays.
   (3) Users shall log in to their email account with the default password. The email account will be activated after they change the password.
2. Coding principle
   (1) Employee account: The string in front of the at sign (@) is the user account (i.e. employee ID), and the string after the at sign is the name of the e-mail server (fhc.com.tw).
   (2) Special account: A special account set for business needs, such as "fhc201". The account responsible person shall be the case officer or staff designated by the chief.
   (3) When using the e-mail account of a subsidiary before this Company establishes its own e-mail server, follow relevant management regulations of that subsidiary.
3. Points for notice
   (1) The email account of each user has a fixed capacity. The Electronic Information Division may adjust the capacity according to actual business needs.
   (2) Users shall properly keep and keep confidential their accounts and passwords and shall not lend them to others.
   (3) Users shall not send or store emails that violate the "Trade Secrets Act" of the Republic of China.
   (4) Users shall not transmit or store unverified or false information and data relating to this Company.
   (5) Users shall not transmit or store emails that contain hostile, assaultive, damaging, obscene, and other contents that violate the law or infringing the rights and interests of this Company or others.
   (6) Users shall not send emails irrelevant to their business in order not to waste the bandwidth resources of this Company.
   (7) Users shall not illegally intrude in unauthorized computer systems, interfere with other users on the network, damage communication equipment, or other engage in other similar behaviors.
   (8) Users shall not send or store emails that infringe the intellectual property rights and other

rights of this Company or others.

(9) Users shall respect the privacy and right of use of other users and shall not spy on others' emails or steal others' email accounts.

(10) When the size of an email exceeds the limit, users shall process this email as quickly as possible. Otherwise, the Electronic Information Division may directly delete the email to ensure that no email exceeds the regulated size.

(11) To prevent space wastage, emails will only be stored on the e-mail server for three months. All emails on the e-mail server will be erased after three months.

(12) When using the email service to support or promote other additional or integrated applications (e.g. e-news delivery and Call Center service channels), apart from notifying in writing the Electronic Information Division in advance, users shall exercise its due management diligence to maintain the network security of this Company.

(13) Users shall not use external email accounts that do not belong to this Company or a subsidiary on the Company's computers.

(14) Data backup copies of the e-mail server regularly.

(15) Real-time virus scan shall be activated on the email system.

(16) For the need of system maintenance, software update or data conversion, the Electronic Information Division may suspend the email service without prior notice where necessary.

(17) Users shall not claim compensation for service interruption; service suspension; service delay; errors in data transmission and/or storage; or data tampering or destruction after a third-party intrusion caused by equipment failure or operational negligence of others.

(18) This Company assumes no responsibility for indemnifying the direct or indirect loss or damages caused by posting or sending emails via this email service.

4. Penalty

(1) For violation of the "Points for Notice" in Article 3 of this chapter, the Electronic Information Division may notify users to make improvement, reduce his/her privilege, suspend his/her right of use, terminate his/her right of use, or report to the superior for punishment.

(2) Users shall assume full civil and criminal liabilities for violating the "Points for Notice" in Article 3 of this chapter or engaging in other illegal acts.

5. Termination of service

The email account of resigned (including retired) employees shall be cancelled as of the date of resignation (retirement).

6. This Company reserves the right to view and maintain a record of the emails of users in any of the following situations:

(1) Serious violation of the "Points for Notice" in Article 3 of this chapter.

(2) For the purpose of maintaining the smooth operation of the email system and the network security of this Company.

(3) For gathering evidence or investigating illegal acts regarding the harm on the rights and interests of this Company with reasonable bases.

(4) At the legal request of a judicial agency, other agencies, or a third party based on relevant laws and regulations.

(5) Other acts according to the laws and regulations.

Chapter 6 Principles for the retention, storage, and processing of computer files

1. Types of computer files
   (1) Computer stored file: Files directly related to computer operation and stores in media directly connected to computer equipment (such as disks).
   (2) Media file: Files stored in independent electronic media (e.g. discs, magnetic tapes, and diskettes).
2. Computer stored files
   (1) The space allocation of the storage media where computer stored files are stored shall include space for files used in official operation and test operation.
   (2) Access privilege shall be assigned to control access to data in computer stored files where necessary.
   (3) The number of backup copies, the cycle of backup, and recovery procedure for damage of computer stored files shall be specified based on the category and importance of files. Where they are not specified, at least one backup copy shall be made once a month.
   (4) After storing in an independent storage media, computer stored files are considered as medial files.
   (5) When it is necessary to replace computer hardware and software equipment for business needs, backup copies shall be made to prevent data loss.
3. Media files
   (1) The retention period of medial files shall be specified based on the category and importance of files.
   (2) For media files with a long retention period, two copies shall be made. One shall be retained in the datacenter of the Electronic Information Division, and another copy in an off-site location. All copes shall be properly retained and registered in a register for future reference. For backup media intended for temporary retention, retain the last two backup media on principle.
   (3) Storage media shall be labeled or clearly indicated on the appearance to facilitate identification.
   (4) The backup, borrowing, and return of medial files shall be registered for future reference.
   (5) Media files shall be stored in a well-maintained, suitable environment away from magnetic influence or dangerous objects. Access control shall apply to the place where media files are stored. Except for datacenter administrators and relevant officers, no unauthorized entry to the medial file storage site shall be allowed.
4. Management of computer stored files

   To facilitate resource sharing and the control of data access privilege, the files stored in the file server of this Company are partitioned as follows:

   (1) Financial holding data partition
      1) Data property: Financial holding data for common uses.
      2) Access authority: All employees of this Company.

3) Retention period: Permanent.

4) Management responsibility: Case officers of relevant business

(2) Division data partition

1) Data property: Divisional data

2) Access authority: The employees of each division can access the data of their division, whiles others are prohibited.

3) Retention period: Permanent.

4) Management responsibility: Each division shall assign one or two staff to manage its divisional data.

(3) Personal data partition

1) Data property: Temporary storage of personal work data.

2) Access authority: Individual users, no access by others.

3) Retention period: To be set at the employee's request and cancelled by the employee or his/her department after his/her resignation.

4) Management responsibility: To be managed by individual employees, and the maximum space may be limited where necessary.

(4) Project data partition

To ensure business data confidentiality and prevent project data from access by non-project team members, a project team may apply for creating a project folder ("Computer User Privilege Assignment and Change Application" (Form 7)) for data sharing and exchange among project team members (same or different departments).

1) Data property: Shared business data for project use.

2) Access authority: Project team members.

3) Retention period: To be set at the request of the project leader (or organizer) and to be canceled or retained after project completion.

4) Management responsibility: The project team leader (or organizer) or a member he/she assigns shall manage the project data.

5. Method(s) for naming files and directories

(1) The name of files and directories shall be concise and precise.

(2) The total length of a file or directory name shall not exceed 50 bytes.

6. Data backup

(1) System backup

1) Backup copies of system software shall be made once every two months.

2) No backup copy shall be made for system software irrecoverable with a recovery CD but needed re-installation with the installation CD.

(2) Data backup

1) Backup copies of data files shall be made once every two weeks.

2) For data requiring long-time retention, employees may request for making backup of a specific range of data with prior approval of their chiefs.

(3) Storage and management of backup data

1) Employees shall indicate the date and register each backup copy for management after completion.
2) Backup data shall be retained for a term of six months. Expired backup data shall be erased or destroyed in the company of a staff other than the case officer.
3) One latest copy of backup data shall be kept in the off-site retention site.
4) The backup, duplication, borrowing, return, erasure, and destruction of files in the disc shall be registered in the “Backup Disc Register”. Borrowing and return of such discs shall also be registered in the “Media File Borrowing and Return Registration” (Form 8).

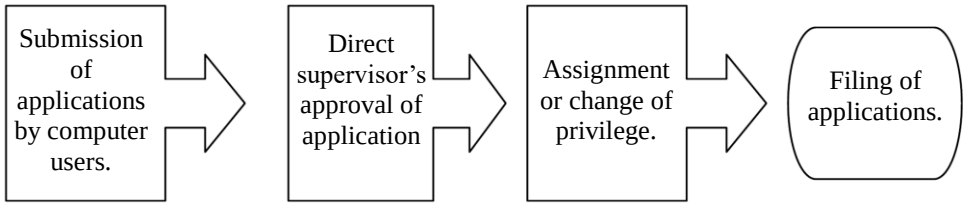
7. Scrap and destruction

Before scraping or destroying important computer products, applicants shall complete the Destruction Application Form (Form 9) and submit the form to the chief for approval before destroying by the case officer and chief together. The case officer and the chief shall remark the date and place of destruction in the application form. Participants shall sign in the form. Important computer products shall be specified in the register.

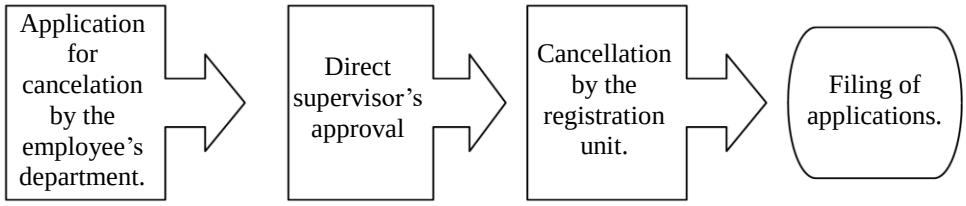
Chapter 7 User privilege management

To ensure the computer operation and data security, the “Computer User Privilege Assignment and Change Application Procedure” is established as follows:

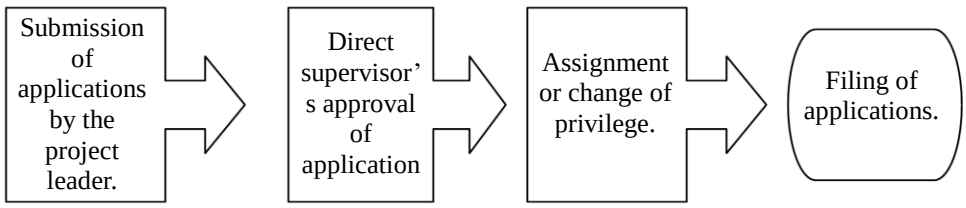
1. New employees or employees with a duty change shall complete the “Computer User Privilege Assignment and Change Application” (Form 7) to apply for new privilege according to the following procedures:
   (1) New employees or employees with a duty change shall complete the application form and submit it to the direct supervisor for approval before handing it over to the registration unit to assign or change the user’s computer privilege.
   (2) After the registration made according to the information contained in the approved application form, the registration unit shall submit the form to the department chief for review before filing.



2. Privilege for editing data of the department of an applicant (employees) shall be assigned, and a personal folder and editing privilege shall be created and assigned with the employee ID.
3. After the first-time login, employees must change their passwords before they can continue to use the departmental data. A password shall consist of six or more characters, including letters and non-letters.
4. A user account will be locked after five login failures. A user must ask the system administrator to unlock the account. The system administrator shall find out and verify the cause(s) of login failures before unlocking an account.
5. When an employee resigns (including retirement), his/her privilege will be canceled on the effective date of resignation. The department of that employee shall apply for privilege cancellation according to the following procedures:
   (1) When an employee resigns, the employee’s department (or the employee) must complete an application form and submit the form to the direct supervisor for approval before handing it over to the registration unit to cancel his/her privilege.
   (2) After cancelling the privilege of the applicant, the registration unit shall submit the application form to the department chief for review before filing the form.



6. The procedure for creating a project folder and the privilege of project team members are as follows. The project team shall complete the "Computer User Privilege Assignment and Change Application" (Form 7).
   (1) When a project team needs to create a project folder, it shall complete the application form and submit it to the direct supervisor for approval before handling it over to the registration unit to set or change the privilege of computer users.
   (2) After the registration made according to the information contained in the approved application form, the registration unit shall submit the form to the department chief for review before filing.



Chapter 8 Disaster recovery procedure

1. AP server disaster recovery (DR) procedure

The AP system of this Company consists of four hard drives using the IBM raid control card to provide raid 5 disk array functions. The system includes the personnel attendance system, accounting system, and consolidated statement system. Based on the server failure condition, the DR procedure includes:

(1) Hard drive damage recovery procedure: Retrieve data from the undamaged hard drives with the raid control card for system reconstruction.

(2) Recovery procedure for AP system damage: When an AP system is damaged, DR will only need to implement on the damaged AP system.

1) Re-installation of the damaged AP system (e.g. win2000 server, Lotus Notes server, and Oracle database).

2) Importing and recovering the latest system backup to recover the damaged system to the status at system backup.

3) Re-entry of the changed data after the last system backup.

2. File server DR procedure

The file server is equipped with both the AD server and Norton Antivirus parent server functions. Currently, the file/AD server is equipped with two hard drives (master and backup drives) with synchronous writing. In addition, a redundant server has been built. Based on the status of failure, the DR procedures of the file service are as follows:

(1) Recovery procedure for master drive damage: When one master drive is damaged, the backup drive can immediately work as the master drive to prevent data loss.

(2) Recovery procedure for File/AD Server damage:

1) Recovery procedure for domain privilege settings (AD service recovery)

The privilege settings of AD service users have been synchronized in the backup and master servers (synchronous data in both servers) in time of normalcy. When the master server is damaged, the backup server can go live immediately to become the AD server without human intervention.

2) Recovery procedure for server files (file service recovery)

a. Referring to the “Domain Privilege Settings Recovery Procedure”, the backup server will automatic activate and act as the AD server to recover AD services.

b. Copy the data in the master drive or backup drive to the backup server and set the privilege of relevant groups of all folders (financial holding data partition, division date partition, personal data partition, and so on) in the “data partitions” for users to process file data in relevant file servers over the intranet.

(3) Recovery procedure of the Norton Antivirus parent server

1) Re-installation of the Norton Antivirus server system (as parent server) in the backup server.

2) Re-installation Norton Antivirus in all computers within the domain and add this parent

server to accept the control of the backup server.

3. Exercise of DR procedures
   (1) The DR procedure shall be drilled once biannually.
   (2) The results of exercise and test shall be maintained in the record.

Section 3 Information Management of Subsidiaries

Chapter 1 Software management

1. Planning of AP systems
   (1) Business management personnel shall participate in AP system planning implemented with reference to the AP System Development SOP.
   (2) System capacity planning

   Personnel shall assess the capacity demand of AP systems to prevent capacity inadequacy from affecting normal system operation.
   (3) Security assessment before system goes live

   Personnel shall establish the SOP of the new AP system before official operation. Personnel shall also run relevant tests to verify if the new AP system complies with the existing security standard before the AP system goes live.
   (4) Redundancy planning

   Personnel shall plan the methods and run periodic tests to maintain business continuity after the system equipment is damaged or hangs.
   (5) When outsourcing the development of AP systems, personnel shall carefully assess their potential security risks and sign an information security agreement with developers to define their security management responsibility in the contract terms.
2. Development of AP systems
   (1) Personnel shall plan and establish SOPs for AP system development to ensure employees can correctly and securely use the computer and for the reference of the development, maintenance, test, and acceptance of systems.
   (2) AP system development SOPs shall be approved by supervisors when they are established and amended.
   (3) Separation of the development and implementation of systems

   While system development and tests may include software modification and computer resources sharing, to reduce potential risks, the development environment and implementation environment of systems shall be separated to minimize unintended tampering or unauthorized access of operating software or data.
3. Management of AP change
   (1) Personnel shall assess the operational risks of system change in advance.
   (2) A change of AP systems used in official operation shall be approved by supervisors prior to implementation.
   (3) A change of the AP systems used in official operation shall be reviewed by different personnel.
   (4) The previous version of the AP systems used in official operation shall be retained for reference for at least one year.

(5) Recovery procedures shall be considered for each change to ensure quick recovery of normal operation after a system anomaly.

4. Management of AP system problems
   (1) When a system problem occurs, personnel shall immediately report to supervisors, take corrective actions, and maintain relevant records for future reference.
   (2) A defined procedure for system problem reporting and relevant regulations shall be established.
5. Control of software duplication
   (1) Personnel shall abide by laws and regulations and contractual regulations regarding intellectual property rights while using software.
   (2) Unless otherwise being authorized, personnel shall not copy dedicated software to non-organizational IT equipment.
   (3) This Company shall inform employees of laws and regulations regarding intellectual property rights in writing, electronically, or by other means.
6. Prevention of computer viruses and malware
   (1) Personnel shall take preventive and protective actions to prevent and detect the intrusion of computer viruses and malware.
   (2) All departments and users shall abide by the software licensing regulations and the use of unlicensed software is strictly prohibited.
   (3) Personnel shall periodically update the computer virus prevention software used.
   (4) Personnel may install utilities to detect software tampering to detect if running codes are tampered with.
   (5) Personnel shall verify if media files of an unknown source and with uncertain contents are infected by computer viruses.

Chapter 2 Management of hardware and environment

1. Security management of equipment
   (1) Dedicated personnel shall be assigned to manage computer equipment to maintain equipment normal operation.
   (2) Maintenance and emergency repair measures shall be established for important computer equipment.
   (3) A log shall be established for each computer equipment and equipment shall be inventories periodically.
   (4) Protection of the point of equipment installation
      1) Access control shall be applied to protect the point of installation of important equipment to reduce dangers caused by environment insecurity and opportunities for unauthorized uses.
      2) No smoking and eating is allowed inside a datacenter and potentially flammable or explosive objects are strictly prohibited in a datacenter.
   (5) Power supply
      1) Important power switches in the computer operation area shall be equipped with measures to prevent unintended contacts in order to prevent power outages and other damage caused by abnormal power supply. Standby power supplies and uninterrupted power systems (UPSes) shall be considered where necessary.
      2) Power extension cords shall be used with cautions to prevent fire from overloading.
   (6) Equipment maintenance
      1) Equipment maintenance shall only be implemented by authorized maintenance personnel. Users shall confirm their identity in advance and escort them throughout the maintenance
      2) After repairing or maintaining computer equipment, records shall be maintained for future reference.
   (7) Security management of equipment placing in external space
      1) The same information security management and licensing regulations shall apply to computer equipment installed outside of this company to support business operations.
      2) Portable computers used by field personnel are subject to theft, loss or unauthorized use easily, access protection measures shall be implemented, and user units shall prepare a register to register their users.
   (8) Security measures for replacement and relocation of equipment

      Prior to replacement, confidential, sensitive data and licensed software contained in equipment with storage media shall be removed.
2. Environment management
   (1) Security of surrounding environments
      1) Personnel shall define the peripherals required security control and implement relevant security measures.

2) Personnel shall also define the perimeters of controlled areas.

3) Personnel shall place facilities supporting information services, such photocopiers and fax machines, in appropriate locations to reduce the risk of unauthorized access to the controlled areas and minimize the opportunities for the compromise and leakage of sensitive data.

4) For the security purpose and prevention of potential improper actions, unauthorized personnel working alone in the office shall be controlled.

5) When information service is outsourced, equipment under self-management shall be placed in a specific area and separated from the equipment of information service providers.

6) IT support personnel or maintenance personnel shall enter a controlled area only when requested or authorized, and their activities in the controlled area shall be limited (e.g. access to sensitive data) and supervised.

(2) Personnel access control

1) Access control measures shall be implemented for all controlled areas to ensure access is granted only to authorized personnel.

2) Visitors can access the controlled area only with authorization. Their entry and exist times shall be registered in a logbook.

3) The right to access to controlled areas shall be cancelled immediately when employees resign.

(3) Security management of datacenters

1) Datacenters shall be equipped with good physical security measures. The potential of natural disasters, such as a fire, a flood, or a quake, and man-induced disasters, and the potential threats from nearby space shall be considered when selecting the location of datacenters.

2) Dangerous and flammable objects shall be stored in a safe location far away from the datacenter.

3) Backup media shall be stored off-site to prevent damage while a datacenter is damaged.

4) Security detection and prevention equipment shall be installed and inspected periodically.

(4) Monitoring of computer operating environments

The computer operating environment shall be under surveillance at all times to maintain normal computer operation.

(5) Management of information assets

Personnel shall not carry computer equipment, data or software out of the office without prior permission.

Chapter 3 Network management

1. Planning and management of network security
   (1) Network security planning
      1) Control mechanisms for computer network security shall be established to ensure the security of data transmitted over the network, protect network connections, and prevent unauthorized access.
      2) Network security management shall be strengthened for trans-organizational computer network systems.
      3) Security protection measures shall be adopted when transmitting sensitive information via public networks to protect the integrity and confidentiality of data transmitted via public networks and the operating systems connected.
      4) The IT department of each subsidiary shall plan, construct, and manage the subsidiary portal.
      5) Prior application and permission shall be made and obtained before connecting a host or network equipment of an external network to the intranet. The internal network security regulations and connection procedures shall be strictly followed.
   (2) Security protection of the web server
      1) Prior written applications shall be made to apply for initiating a web service. Web services shall go live on the corporate website only after obtaining an approval.
      2) In addition to the adopting the same security controls as operating systems, the web server for official operation and storing important data shall be equipped with the identity authentication and privilege control mechanism to prevent illegal users from logging in to the server to steal from and damage the server.
   (3) Firewall management
      1) Firewalls shall be established between the intranet and the internet for segregation and protection.
      2) The firewall system and control mechanisms shall be appropriately adjusted with reference to the change of web services or network equipment in order to deal with various types of new internet attacks.
      3) Records of firewall settings shall be maintained.
   (4) Establishment of network security protection systems
      1) To strengthen network security protection, virus prevention measures shall be adopted. Antivirus prevention software with complete functions shall be carefully selected and maintained and updated periodically.
      2) For the purpose of early alert and post hoc tracking and detection of an intrusion and attack in progress, an intrusion detection system (IDS) shall be constructed where necessary, periodic vulnerability scan and assessment or penetration test shall be implemented, and appropriate defensive measures shall be adopted.
   (5) Management of network information

1) Personnel shall not store confidential and sensitive data or documents in information systems open to the public.
2) Personnel shall prevent the illegal use of the files containing the personal data of customer applications or registrations when storing them.

(6) Redundancy of network equipment and system backups

1) To maintain the continuous and normal operation of the corporate network, backup network equipment shall be prepared.
2) Hardware network equipment shall be equipped with the UPS to prevent unexpected power failures.
3) System backup of all network servers shall be made periodically.

2. Network security audit

(1) Records of the settings of important network equipment shall be maintained.

(2) Alarm systems shall be equipped where necessary to alert network administrators of specific network security events with warming signals in order to take effective preventive actions to minimize network security events.

(3) Personnel shall immediately report network instruction behaviors involving threats to theft, damage or illegal acts for management.

3. Management of network access

(1) Management of network use

1) Personnel shall abide by relevant regulations and the scope of authorization while using any computer resources over the network.
2) Personnel shall not transmit information violating the copyright law and relevant laws and regulations over the network.

(2) Identification of user identity

A remote user identification mechanism shall be established for public networks for use by non-organizational users or linking to the corporate network from an extranet to reduce the risk of unauthorized system access.

(3) Segregation of networks

A network system can be separated into different domains for different users and different computer systems to minimize security risks.

(4) Control of network connections

For the purpose of system security, the scope of web services for cross-organizational network systems shall be limited.

(5) Security control of web services

When using public or private networks, the potential risks of respective web services shall be assessed.

Chapter 4 Management of internet applications

1. The designated department of each subsidiary shall plan, implement and management the portal its corporate website. Where there are special business needs, the chief of the requesting department shall apply for establishing an independent website for the department and relevant management rules.
2. Mechanisms for network security management shall be established based on the protocols and linking architecture used to protect the security, integrity, and confidentiality of networks.
3. Segregation measures shall be adopted for information systems opened for external connections shall be to prevent direct entry into the information systems or databases for data access from an external connection.
4. Appropriate protective measures shall be implemented for transmitting sensitive information across subsidiaries over the internet to ensure data privacy.
5. No data and documents containing confidential and sensitive information and the privacy of a person shall not be published on the website without the prior permission of the party concerned.
6. Security protection measures shall be adopted for websites storing personal information or files to prevent the theft and illegal use of personal privacy data.
7. Backup equipment shall be prepared for all major network equipment used on the network system.
8. Procedures and required actions for handling network intrusion shall be established.

Chapter 5 Management of community security

1. Rules for email use shall be specified.
2. Mechanisms for email security management shall be established to reduce the potential operational and security risks brought by emails.
3. Personnel shall not send classified documents and data and documents and data of higher security levels by email. Where sending sensitive information by email is required, personnel shall encrypt it before sending.
4. Personnel shall not open emails of unknown origins to prevent malicious files from activation to damage the network system.
5. Where subsidiaries transmit data via a dedicated line (e.g. closed network system), they shall encrypt them based on the security level of data in accordance with relevant security regulations.

Chapter 6 Management of data and documents

1. Protection of personal information

   Personnel shall carefully process and protect personal information in accordance with the "**Personal Information Protection Act**".

2. Classification of information security levels

   For information security classification, subsidiaries may classify data into confidential, sensitive, and general information based on their nature or the characteristics of information operation. Subsidiaries shall indicate confidential and sensitive information.

3. Data backup
   (1) Appropriate and adequate backup facilities shall be prepared to periodically make backup copies of data and software for redundancy to **quickly** recover normal operation after a disaster or storage media failure.
   (2) At least one data backup copy shall be stored off-site to prevent potential damage brought by the disaster at the major operational venue.
   (3) The backup of important data shall maintain three generations of data.
   (4) Backup data shall be tested periodically to ensure their usability.

4. Management of computer media
   (1) Regulations for computer media management shall be established to reduce potential security risks.
   (2) Computer media containing important data shall be stored in a controlled area and assessed only by authorized personnel.
   (3) When computer media storing confidential and sensitive information are not used anymore, erase all the contents stored inside or destroy the storage media.

5. Security management of media inter
   (1) In principle, data transmission via media exchange shall be achieved by direct file transfer. Where transmission via physical media is required by special operational needs, the security of transfer of the physical media shall be ensured.
   (2) Access to the data for media exchange shall be controlled by privilege to ensure unauthorized personnel cannot access data in relevant files.
   (3) Mechanisms for user privilege control shall be established in subsidiaries with a media data exchange area to ensure unauthorized personnel cannot access data in relevant files.
   (4) A user unit shall change the access privilege of any personnel immediately after their transfer or resignation.

6. Protection of data and files
   (1) Protection of files
      1) Important data and files shall be securely stored to prevent loss, damage, forgery or tampering.
      2) Files after the regulatory retention time can be deleted or destroyed in accordance with

relevant regulations. However, their potential impact on computer operation shall be considered in advance.

(2) Protection of testing data

1) Testing data shall be protected and controlled. Avoid using real databases containing personal information in the test. Where real data should be used in a test, remove all data valid for identifying any person in advance.

2) When using real data in a test, access control measures for actual operational systems shall also apply to the testing system.

3) After running a test with real data, real data shall be removed from the testing system immediately.

7. Security management of outsourced data processing

When outsourcing the processing of computer documents and data, a financial institution shall carefully select service providers with adequate security management capacity and confirm that outsourced service is one of the legally approved business item of the service provider. **Apart from** signing a service agreement with the service provider, **periodic inspections shall be implemented to verify the performance of the service provider; when allowing the service provider to collect, process or use personal information, a financial institution shall appropriately supervise the service provider in accordance with Article 8 of the Enforcement Rules for the Personal Information Protection Act**. A service agreement shall contain at least the following items:

(1) A description of the items and contents of service.

(2) The laws and regulations (including the Banking Act, Money Laundering Control Act, the Personal Information Protection Act, and other laws and regulations) applicable to financial institutions with which the service provider shall comply.

(3) The service provider shall an internal control mechanism and regularly and irregularly conduct internal audits. The service provider shall immediately notify the financial institution for inability to, difficulty in, or uncertainty of performing the service.

(4) A financial institution may terminate the service agreement with a prior notice where necessary (including under the order of the competent authorities).

(5) The service provider shall provide the data and reports related to the service at the request of the Financial Supervisory Commission, the Central Bank, the audit unit of the financial holding company, and the inspection agency they assign and accept the financial inspection performed by the financial institution. A service provider shall not perform the service items in the name of the financial institution.

(6) The non-disclosure obligations of the service provider and its employees.

(7) The service provider shall accept the inspection and audit implemented by the financial institution.

(8) A service provider shall not re-outsource the service or assign the service agreement to another party, unless otherwise approved by the financial institution.

(9) Penalties for breaching the service agreement by the service provider.

8. Document management

(1) For system development or maintenance, the processes of system development or maintenance shall be documented and updated after a change.

(2) Prior to filing, documented and updated processes of system development or maintenance shall be submitted to the responsible person of system development or maintenance for approval.

(3) A filename shall be assigned to each document and a register shall be established to register the filename of documents. Documents shall be stored by category and personnel shall be assign to keep custody of documents. A register shall be established to register the borrowing and retrieval of documents.

(4) Documents containing confidential or sensitive information shall be disposed of carefully, such as destruction or shredded by a paper shredder.

(5) System documents including system workflow, operation workflow, data structure, and authorization procedures shall be protected appropriately to prevent improper use.

Chapter 7 Management of personnel using information

1. Non-disclosure responsibility of personnel using information

   Employees using information systems shall abide by the non-disclosure responsibility specified in relevant laws and regulations and sign the non-disclosure agreement (NDA).

2. Division of labor for information operation

   The responsibility for security management and implementation of key information business shall be separated, and relevant personnel shall be requested to abide by the non-disclosure responsibility. A check and balance mechanism shall be established where necessary.

3. Education and training of information security for users

   Education and training of information security shall be arranged for employees for them to understand the importance of information security in order to improve their awareness of information security and urge them to follow the information security regulations.

4. Access management of users

   (1) User registration management

      1) Procedures for user registration management shall be established for information systems used by many people.

      2) When the duty of a user is adjusted or a user resigns (retires), his/her system access privilege shall be canceled with two workdays after receiving the notice of his/her status change.

      3) Unused user IDs and passwords shall be checked and cancelled periodically.

   (2) Management of user passwords

      1) A system for user password management shall be established.

      2) After the first-time login, users shall change the password before they can continue to use the information system.

      3) Passwords shall be changed periodically.

   (3) Review and assessment of system access privilege

      For effective control data and system access, user access privileges shall be reviewed and assessed periodically.

Chapter 8 Emergency response and management

1. Report of information security events
   (1) Procedures and channels for official reporting of information security events shall be established, and the actions and measures to be taken after reporting shall be defined.
   (2) After detecting an information security event or a probable information security event (including system security loopholes, threats, system vulnerabilities, and functional anomalies), employees shall report the event according to the reporting procedures and channels to quickly notify the responsible unit and personnel to take action.
   (3) Employees and the external personnel with in information security agreement with this Company shall be clearly informed of the response and reporting procedures of different types of information security events for them to understand relevant handling procedures.
2. Report of information security vulnerabilities
   (1) Employees shall pay attention of the internal security vulnerabilities of and potential threats to the information system or information service facilities and report to the direct business supervisor or the system service provider.
   (2) Professionals shall handle system security vulnerabilities and system users shall not modify them by themselves.
3. An emergency event handling team may be established to handle an emergency event in order to take appropriate measures when an emergency event occurs.
4. Emergency handling procedures for handling the damage or theft of confidential data shall be established based on the possibility and scenario of events to strengthen the response ability of relevant personnel.
5. The backup media files of business shall be stored off-site at planned intervals. A record covering a summary of contents, data date, and storage location of the backup media shall be maintained and submitted to the supervisor for approval prior to filing and retention. In addition, items, such as manuals, magnetic tapes, forms, and paper, required for disaster recovery shall be prepared at an appropriate venue to prepare for the need of system recovery after a disaster.
6. Emergency response and disaster protection training or exercises shall be organized every year, and records of the training or exercise results shall be maintained.

Chapter 9 Planning for information system continuity

1. Procedures for information system continuity planning shall be established and an information system continuity plan shall be established in consideration of cost efficiency.
2. When planning information system continuity, potential threats of man-induced or accidental factors to the continuity of important business shall be analyzed and reduced to ensure the continuity of important business after an incident, facility failure or damage of the information system.
3. Responsible units or personnel shall be assigned for the emergency response, manual preparations, and system recovery in the information system continuity plan.
4. Periodic tests and exercises shall be arranged for the information system continuity plan to ensure the effectiveness of the plan and for relevant personnel to actually understand the latest status of the plan.
5. The information system continuity plan shall be updated with reference to the business, organization, and personnel adjustment and change in order to demonstrate the investment efficiency of the plant and ensure its effectiveness.

Section 4 Addenda

1. These Regulations and its amendments shall be implemented after obtaining the approval of the president.
2. These Regulations were established on 22 September 2003
   (Originally the “First Financial Holding Co., Ltd. Directions for Information Management”)
3. The first amendment was made on 3 March 2004.
4. The second amendment was made on 9 September 2004.
   (Renamed “First Financial Holding Co., Ltd. & Subsidiaries Information Management Regulations”).
5. **The third amendment was made on 14 December 2012.**

Form 1 Application System User Privilege Assignment and Change Application

Form 2 AP System/Program Change Application

Form 3 Computer File Data Change Application

Form 4 Computer Equipment Maintenance Record

Form 5 Web Content Posting Application

Form 6 Internet Account Application

Form 7 Computer User Privilege Assignment and Change Application

Form 8 Media File Borrowing and Return Registration

Form 9 Important Computer Item Destruction Application