# First Financial Holding Co., Ltd. Work from Home Guidelines

Established on 4/17/2020

**The 1st amendment was made on September 9, 2020**

**The 2nd amendment was made on May 20, 2021**

**The 3rd amendment was made on June 21, 2021**

I. Purpose

The Guidelines are established to provide guidance for the initiation of working from home, ensure the employees' health, and maintain the regular operations of the Company's command system in the event of epidemics or major disasters.

**II. In response to diseases or major disasters, the group shift pattern is as follows:**

**(I) Divide the employees into groups according to the actual situation. Only one group of employees shall be in the office at a time, and the rest of the groups shall work from home, sharing the office space and reducing the number and frequency of attendance in the office through shifts to lower the impact of disasters or pandemic and the risk of infection. The principle of personnel working from home is to not involve the Company's core systems and accounting affairs.**

**(II) For the list of personnel groups, personnel above the department head level shall be assigned by the President; other personnel shall be assigned by the respective department heads and shall be reported to the Administration Management Department and be approved by the President before the start of the shift work mechanism. After the shift work mechanism is activated, personnel in each group are not allowed to work across groups, and they are not allowed to contact and meet during or after work to reduce the risk of infection; furthermore, in order to facilitate immediate response, the head of the department may adjust the list of working-from-home personnel based on the development of the pandemic and business conditions, and notify the Administration Management Department.**

III. Work Management

(I) The Department and direct supervisors shall fully communicate with employees working from home on the list of to-do items and completion deadline. The employees shall use VPN accounts to connect to the Company's VPN system and log into the Company's personal computer to execute the original business approval procedures. Matters that cannot be completed in the system shall be reported via e-mail and confirmed by telephone. Related records shall be retained for future

confirmation.

(II) Employees working from home shall actively communicate and confirm with the direct supervisor on targets for business operations and execution for working from home. They shall fill out the "Work Log" (Attachment 1) and report the business operation conditions. Employees shall maintain communication during office hours and ensure that communication channels (e.g., home telephone, mobile phone, or instant communication software) remain open in order to maintain control over the progress of work. The direct supervisor must confirm that the employees understand the supervisor's expectations and requirements, and review whether the contents recorded in the "Work Log" meet business procedures in internal and external regulations. The direct supervisor shall use system resources for inspections and auditing and regularly collect information on the employees' physical conditions and work progress which shall be recorded for future inspections.

IV. Attendance Management

(I) The office hours of employees working from home shall be processed in accordance with the Company's "Employee Attendance Management Guidelines". Such employees shall report to the supervisor when reporting for work and signing off from work and register the time in the "Work Log". They may not go outside during office hours.

(II) As a principle, employees working from home should not work overtime. Where necessary, they must apply for the unit supervisor's approval to work over time in the employee attendance system (EasyFlow) and record the number of overtime work in the "Work Log". The records shall be used as the basis for obtaining remuneration for overtime work.

V. Safety and Health Management

(I) Employees working from home shall adopt self-health management measures. They shall take their temperatures once in the morning and again in the evening during office hours, record results in the "Temperature and Health Status Records Table" (Attachment 2), and regularly report to their respective departments. They must wash their hands often and pay attention to respiratory health and cough etiquette.

(II) They must avoid visiting public spaces during non-office hours and postpone all medical treatment or inspections that are not urgent. If they must go outside, they must wear surgical masks at all times. Employees who have respiratory symptoms such as a fever, cough, runny nose, or those that feel ill shall wear surgical masks carefully and seek medical attention as quickly as possible. They may not use public transportation. When seeking medical attention, employees must actively provide

information on the people they have been in contact with, their travel history, exposure due to professional practices, and whether the people they live with exhibit similar symptoms. After returning home, they shall also wear masks and avoid going outside. They shall also keep a distance of at least 1 meter when talking with others. If an employee seeks medical attention and the hospital arranges a test, the employee must stay at home and may not go outside before receiving the test results. Where the employee is confirmed to have a disease, the unit supervisor shall immediately report to the Risk Management Department and the Administration Management Department.

VI. Information Security Management

(I) Employees that are assigned to work from home shall be given VPN accounts by the Information Technology Department. The default setting of the VPN account is "Disable" and the "Enable" status is activated after the work from home status is initiated.

(II) Computer equipment used for working from home must be equipped anti-virus software and the employees must pay attention to the safety of the network environment. Employees are prohibited from using connected equipment and networks in public areas (e.g., Internet cafes, coffee shops, or other open public spaces) to log into the VPN system.

(III) When using the VPN connection, files cannot be uploaded or downloaded to the computer used for working from home. Where the employee needs such files due to business requirements, the information must be stored in the file server for remote operations and processing. Where businesses operations cannot be completed and information must be mailed to the employee for processing onsite, the mailing shall be processed in accordance with the Company's "E-Mail Management Guidelines ". All data mailed shall be scanned for personal data. Mail containing personal data or encrypted mail shall only be released with the approval of the supervisor.

(IV) Where the employee working from home temporarily leaves work or ends operations, they should immediately log out from the Company's personal computer and sign off from the VPN system. The employee should not allow the computer to idle on standby.

(V) The Company's Work Log management system shall produce the users' operation report for the previous day every day (including login and access to file servers). The system shall mail the report to the user for confirmation before review by the supervisor to confirm that the use of the system was conducted by the specific employee.

(VI) When an employee working from home uses the VPN for remote access to a personal computer at the office, the following protective measures must be added:

1. The access-control list (ACL) configuration allows each user to connect to only his/her own computer desktop after logging in. Connections to all other IPs and services are prohibited.
2. The firewall configuration only allows the Company's VPN equipment to connect to the office personal computer of the employee working from home.
3. The Company's Remote Desktop Protocol (RDP) shall be activated based on the list of employees working from home and the user accounts shall be added to the server's Remote Desktop Users Group.
4. The remote VPN connection time for working from home is 08:30 a.m. to 08:00 p.m.

VII. Business Data and Personal Data Protection

(I) Employees working from home must sign the "Confidentiality Agreement for Working from Home" (Attachment 3) before initiating working from home and submit it to the Administration Management Department for recordkeeping.

(II) As a principle, the business data and personal data (including printed and digital data) under the management of an employee working from home may not be taken out of the Company. Where usage outside the Company is required, the department supervisor's approval must be obtained and the management personnel shall retrieve the data and deliver them to the employee working from home. A record book shall be established for management. Data brought out of the Company shall be stored in locked drawers or file cabinets. The keys must be securely stored and contact by individuals that are not employees of the Company must be avoided to prevent data leaks. Such data shall be used in accordance with the Company's file processing guidelines and personal data management regulations. Related regulations shall also apply to physical data printed at the home office or e-mails sent from the home office. After the end of the work from home period, the data shall be compared with the record books to ensure that all data are brought back to the Company.

VIII. Matters not addressed in the Regulations shall be governed by FFHC's other relevant regulations.

IX. These Guidelines are promulgated following the approval of the President; the same applies in the event of amendments.