Content

Title：	Guidelines for On-site Operation Management of the Fiscal Information Agency, Ministry of Finance Ch
Date：	2019.12.12
Legislative：	Established in the document number 1080004659 of the Fiscal Information Agency, Ministry of Finance,on December 12, 2019.
Content：	I. Purpose To strengthen the protection of financial and tax information and effectively manage the safety of on-site operations, these Guidelines have been established for compliance. II. Operational Zones On-site operations are divided into the following three zones: (1) Financial Data Research Center: As stipulated in Paragraph 2, Article 33 of the Tax Collection Act, it provides statistics or detailed data that cannot be directly identified as per. (2) Tax System Operation Monitoring Room: As stipulated in Subparagraphs 3 to 7, Paragraph 1, Article 33 of the Tax Collection Act,it provides tax data to staff appointed by various agencies(hereinafter referred to as external agency personnel) for review or to staff in charge of the tax information application system at the Fiscal Information Agency, Ministry of Finance (hereinafter referred to as the FIA) for system maintenance. (3) High-level Permission Command Operation Monitoring Room: Used by the FIA’s operating system administrators, network equipment administrators, or database administrators to maintain the tax information operation platform, network management devices, and database management services. III. Application Process 1. Financial Data Research Center (See “Application” part in Workflow Diagram 1) (1) Research institutions (organizations) applying to use the “Sampling Database” that the Ministry of Finance authorizes the FIA to open for research should follow the procedures in the “Guidelines for Using the Ministry of Finance’s Tax Sampling Database” of the FIA. (2) For those applying to use the “Non-Sampling Database” for research, the application process is as follows: a. Research institutions (organizations) should request the Ministry of Finance (hereinafter referred to as the MOF) in writing for permission to use tax data for research. b. If the institution (organization) or individual applying for research differs from the actual executing institution (organization) or individual, the person in charge of the research project should provide a letter of appointment and commitment letter, and a power of attorney (samples as in Appendixs 1-1 and 1-2). c. The person in charge of the research project should contact the system personnel of the business division of the FIA (primary contact window) with the approval letter from the MOF and related documents to set a meeting time. The person in charge of the research project is requested to attend the meeting to explain the research methodology, the the data to be utilized, including annual divisions, categorization, tax categories, files, fields, and expected extracted content. Both the representatives from the FIA and the responsible personnel from the relevant systems handling the required data shall be present. d. The person in charge of the system providing research data should assist and ensure that the principal investigator completes the “On-site Operation Data Application Form” (as in Appendix 2) and “On-site

Operation Data Entry Form" (as in Appendix 3). System personnel (primary contact window) of the business division, based on the aforementioned application forms and the approval letter from the MOF, should assess the resources and operation schedule that the FIA needs to provide prior to approving or denying access to the research data files.
2. Tax System Operation Monitoring Room (See "Application" part in Workflow Diagram 2)
(1) External agencies (organizations) should request the MOF in writing for approval to review tax data. Upon approval, personnel authorized to access the data should personally contact the business division of the FIA (primary contact window) with the approval letter, and specify the annual divisions, categorization, tax categories, files, fields, and expected extracted content for the data inquiry. The personnel from the business division of the FIA (primary contact window) should assist the authorized personnel in completing the "On-site Data Application Form" (as in Appendix 2). Based on the aforementioned application form and the approval letter from the MOF, the personnel from the business division of the FIA (primary contact window) will request approval in writing for providing access to the data files for inquiry.
(2) The application procedure for personnel of the FIA's tax information system applying for on-site operation system and data maintenance is:
a. For those applying electronically, use the "On-site Operation Management System (YST)" of the National Tax System Platform to apply for the "On-site Operation File Application Operation-YST100W" (screen as in Appendix 4-1) and the "On-site Operation DataTable Application Operation-YST110W" (screen as in Appendix 4-2).
b. For those applying with a paper form, fill out the "Tax System On-site Operation Application Form" (as in Appendix 6) to apply for on-site operation.
c. After the applicant acquires the signatures from the business division and management division, the management personnel of the monitoring room of the management division will arrange the time for on-site operation.
3. High-level Permission Command Operation Monitoring Room
(1) The application and management of system management and business processing personnel accounts with high-level permssion in the FIA are processed according to the "Management Procedures for High-level Permission Accounts of the Ministry of Finance and its Subordinate Agencies."
(2) When personnel in charge of the FIA's operating system administrators, network equipment administrators, or database administrators perform system maintenance and enter the High-level Permission Command Operation Monitoring Room for on-site operation, they need to fill out the "Access Control System Entry/Exit Change Application Form" (as in Appendix 7) to apply for authorization.
IV. Data Provision
1. Financial Data Research Center
(1) For research institutions (organizations) that apply to use the "Sampling Database" that the Ministry of Finance authorizes the FIA to make accessible for research according to the FIA's "Operating Guidelines for Using the Ministry of Finance's Tax Sample Database," the FIA will provide research data according to the filled requirements.
(2) For those applying to use the "Non-Sampling Database" for research, the research data will be processed and provided as follows:
a. If the data approved after application and import by the research institution (organization) needs to be scrambled and compared with tax data, the system personnel of the business division of the FIA (primary contact window) should provide "On-site Operation Data Import Form" (as in Appendix 3) and media data file to "System Design and Data Processing Division" to process the data and upload it to the tax host server. If the data does not need to be scrambled, the information will be provided to the Information and Communication Division to be downloaded on the Storage Area (D:) of the personal computer hard drive.
b. The planning and design of the data selection, and transcription of identifiable personal (or company) data fields (as in Appendix 8) (such as IDN, BAN, file number, Chinese name, address, phone number, tax registration number, etc.) for pseudonymization shall be conducted in

accordance with the "National Tax Host Data Scrambling Operation Procedure" (as in these Guideline's appendix). The "National Tax Host Data Transcription Application Form" (as in Appendix 9, format and example) shall be filled out and, along with the approval letters from the MOF and the FIA, upon electronic form approval, be sent to the data operations team personnel for data transcription operation.
c. After the data operations team produces the pseudonymized data file, they shall print the "Scrambled Text File Content (JUT120P1)" report (Appendix 10) and "Scrambled Text File Format (JUT120P2)" report for the business division's officer to verify. The business division officer must apply to enter the tax system operation monitoring room to perform data verification:
(a) Verify that the original data file is correctly produced: Check the names, formats, and content of all files (whether pseudonymized or not) provided to the research institution (organization).
(b) Verify that the pseudonymized data file is correctly produced: Check the name and format of the pseudonymized file. Compare the pseudonymized file data with the original data file data to ensure that the pseudonymized data cannot be directly identified.
d. The business division officer completes the "Research Institution (Organization) Data Verification Form" (as in Appendix 11, format and example), and after verification by another colleague, submits it for division head review.
e. After completing the "Research Institution (Organization) Data Verification Form" approval process, the business division officer scans and retains relevant data. Copies are sent to the data operations and monitoring room management personnel as evidence for subsequent internal audits.
f. Based on the "Research Institution (Organization) Data Verification Form," the data operations and monitoring room management personnel shall download data files from the host to the cloud server and provide them to the research institution (organization) via a virtual desktop for on-site operations. In cases of offline operations, the data files shall be downloaded to the Data Storage Area (D:) of the personal computer hard drive. The head of the research project of the research institution (organization) should set a password to lock the Data Storage Area (D:) to clearly define data security responsibilities.
2. Tax System Operation Monitoring Room
The FIA's tax information system personnel shall apply for on-site operations, and the data operations control personnel shall set the viewing permissions for the tax system host files or database tables according to the approved operation period, scope, and rights.
3. High-level Permission Command Operation Monitoring Room
This does not involve data access but only provides an environment for high-level permission commands for operating system administrators, network administrators, and database administrators to execute operating system and network device settings, problem diagnosis, and troubleshooting.
V. Operation Control
1. Financial Data Research Center (refer to Operation Flow Chart 1 "Execution")
(1) On-site operations are by appointment. Research institutions (organizations) must fill out the "On-site Operation Application Form" (see Appendix 12), attach the confidentiality agreement (see Appendix 13) specific to the research project, and after verification by the business division, submit it to the management division to schedule the operation time (office hours: 9:00–17:00).
(2) For the first entry and exit of the research institution (organization) personnel, they are accompanied to the access control personnel by the business division system personnel (primary contact window). The access control personnel will verify the identities of the project lead and participants and provide the necessary access control IC cards. Every entry and exit from the monitoring room requires filling out the "Financial Data Research Center On-site Operation Personnel Access Control Registration Form" (see Appendix 14). Access cards are to be provided daily when operations begin and swiped upon entry and exit; they should be returned at the end of the operation.

(3) To optimize resource allocation and allow different research institutions (organizations) to use the same personal computer at different times, the FIA will provide PCs. Each organization is assigned different computer accounts during the operation period and has its dedicated operational environment. For every on-site operation, the management provides a project-specific hard drive. The management installs and configures the hard drive and attaches a security seal. When the operator leaves, the hard drive is collected and locked in a dedicated metal cabinet.
(4) It is forbidden to bring mobile phones, cameras, laptops, PDAs, and other communication and storage devices. Eating and drinking are also not allowed. Any items brought should be locked in the dedicated metal cabinet.
2. Tax System Operation Monitoring Room (refer to Operation Flow Chart 2 "Execution")
(1) On-site operations are by appointment.
a. External agency personnel must fill out the "On-site Operation Application Form" (see Appendix 12), attach a confidentiality agreement (see Appendix 13), and after verification by the business division, submit it to the management division to arrange operation time.
b. The application center system leader arranges the operation time based on the duration specified in the electronic form (such as Appendixs 4-1, 4-2, 5-1, 5-2) or the paper application form (see Appendix 8).
(2) Every applicant for an application must present the approved application form (either paper or electronic) for reference. Operations begin with the "Tax Platform On-site Operation Personnel Access Control Registration Form" (see Appendix 15), collecting and swiping the access control IC card, which should be returned at the end of the operation. If there is an issue with the application system, an external vendor may accompany the application system leader.
(3) On-site operation applicants should operate on the designated PC and log in to the information operation platform using their employee number and password, following approved operations and privileges. Business division system personnel (primary contact window) should accompany external agency personnel throughout their work.
(4) Outside of regular working hours (daily off-hours and holidays), access control cards and the "Tax System Operation Monitoring Room Off-hour Card Loan Register" (see Appendix 16) are managed by the second-floor computer room staff until the next working day.
(5) It is forbidden to bring mobile phones, cameras, laptops, PDAs, and other communication and storage devices. Eating and drinking are also not allowed. Any items brought should be locked in the dedicated metal cabinet.
3. High-level Permission Command Operation Monitoring Room
(1) The FIA's operating system administrators, network equipment administrators, and database administrators enter the high-level permission command operation monitoring room by swiping their employee ID card. The access control system records the entry and exit times using the employee ID number.
(2) Colleagues in charge at the FIA, while setting up systems, diagnosing problems, troubleshooting, etc., can invite external vendors to assist. Operations should be conducted through a Virtual Desktop Infrastructure (VDI), and details should be logged in the "High-level Permission Command Operation Monitoring Room Computer Logbook" (see Appendix 17). Regular checks should be performed, and records stored after review.
(3) As per the "Ministry of Finance and Affiliated Agencies' High-level Permission Account Management Procedures," records of high-level permission account operations are managed.
a. For routine or periodic operations, the "High-level Permission Account Routine Operation Record Form" (see Appendix 18) should be filled out before the first operation.
b. For non-routine operations, the "High-level Permission Account Non-Routine Operation Record Form" (see Appendix 19) should be filled out after each operation.
VI. Equipment Management
1. To ensure the safety of the equipment, the FIA provides personal computer devices with basic control measures in place. These control measures include:

(1) The computer hard drive is divided into an operating system area (C:) and a data storage area (D:).
(2) The computer administrator account (Administrator) is managed by the FIA's equipment manager.
(3) The use of portable storage media, such as USB CD burners and flash drives, is restricted.
(4) The "Run" command is removed from the "Start" menu.
(5) "Network Neighbors" are hidden.
2. If a research institution (organization) needs to bring in their own personal computers or hardware devices, they must be non-removable hard drives and should have the computer hard drive divided into an operating system area (C:) and data storage area (D:) in advance. The person in charge of the research project (appointee) should fill out the "On-site Operation Information Equipment Entry Application" (as in Appendix 20), acquire approval by the business division, and have the equipment manager implement the aforementioned control measures.
3. If a research institution (organization) needs to install specified software (including non- suite software), it should be installed on the operating system area (C:). The official software licensing (copyright) documents should be inspected jointly by the business division's handler and the equipment manager. The licensing (copyright) documents are retained by the equipment manager. If there is a need to enable firewall operations, the "Fiscal Information Agency Firewall Security Management Guidelines" should be followed.
4. When a research institution (organization) takes out equipment, the project leader (appointee) should fill out the "On-site Operation Information Equipment Exit Application" (as in Appendix 21). The business division representative should then complete the "On-site Operation Information Equipment Exit Form" (as in Appendix 22). After obtaining approval from the division supervisor, it should be sent to the management division for processing. The access control personnel of the Financial Data Research Center will notify the equipment manager and inspection staff (cybersecurity and ethics official) based on the "Scheduled Exit Time." Inspection staff should first check whether the security seal on the equipment is intact, after which the equipment manager will unseal it. If a hard drive or other storage device in the equipment is taken out, data deletion should be carried out on-site according to the FIA's "Computer Equipment Management Operation Manual." When performing the data deletion, the "Computer Data Deletion Application (Confirmation Form)" (as in Appendix 23) should be filled out, recording the status of each deletion in the "Data Deletion Handling Status" column. Equipment can only be taken out after the data deletion is complete and confirmed by the inspection staff. When a research institution (organization) takes out equipment, the software installation licensing (copyright) documents retained by the equipment manager should be returned along with the equipment.
5. Equipment users should act with the diligence of a good manager regarding the software and hardware they use. They must not unilaterally make changes, record conversions, move, damage, or undertake any other actions that alter the current status of the equipment. If damage occurs, the FIA may seek compensation.
VII. Data Export and Deletion
1. Financial Data Research Center (refer to Workflow Diagram 1 "Data Export")
(1) After the operation is complete or during its duration, only the statistical results from the research should be exported, and individual taxpayer financial and tax information should not be taken out. The research institution (organization) should complete the "On-Site Operation Data Export Application" (see Appendix 24) after confirming the content of the final export data columns. It should then be signed off and approved by the business division handler.
(2) When exporting data, the business division handler must fill out the "On-Site Operation Data Export Form" (see Appendix 25). After being approved by both the business and management divisions, the management division, based on the "Export Time," informs the business division system personnel (primary contact window) and inspection personnel (cybersecurity and ethics official). They then review each piece of

exported data and, once confirmed accurate, the data operations team manager allows access to portable storage media. The business division system personnel (primary contact window) downloads the exported data and hands it over to the research institution (organization).
(3) After the conclusion of the research project, the business division system personnel (primary contact window) should inform the management division to carry out data deletion in accordance with the FIA's "Computer Equipment Management Procedure Manual." The equipment manager coordinates with the inspection personnel (cybersecurity and ethics official) to set a time for inspection. During this time, the equipment manager performs the data deletion and fills out the "Computer Data Delete Application (Confirmation Form)" (see Appendix 23), documenting each operation in the "Data Deletion Status" column and getting it confirmed and signed off by the inspection division.
2. Tax System Operation Monitoring Room (refer to Workflow Diagram 2 "Data Export")
(1) When external agency personnel exports data, upon confirming the final content of data columns to be exported, they should fill out the "On-Site Operation Data Export Application" (see Appendix 24). The business division system personnel (primary contact window) then assesses the necessity of the data and approves it.
(2) External agency personnel, when exporting data, should fill out the "On-Site Operation Data Export Form" (see Appendix 25). After being approved by both the business and management divisions, the management division, based on the "Export Time," informs the business division system personnel (primary contact window) and inspection personnel (cybersecurity and ethics official) to review each exported item. Once verified, the Information and Communication Division manager shall activate the business division handler's PC portable storage media access for downloading and assists in its deletion.
(3) The system personnel of the FIA's tax information system, or the system personnel of the business division (primary contact window), shall assist external agency personnel in accessing data use the national (local) tax platform "On-site Operation Management System (YST)" to apply for on-site operations, and concurrently apply to download the operation results file. Inside the monitoring room, system personnel uploads SQL using the national (local) tax platform "On-site Operation Data Table (data base) Application Operation" (as shown in Appendix 4-2, Appendix 5-1). They then select the "Data Download" for the national tax platform or "Investigation Export Download" for the local tax platform, and choose to download the operation results (including whether it is non-statistical data). After the operation is complete, for the national tax platform, use the "On-site Operation Database Query Result Download (Outside Monitoring Room)-YST611W" (as shown in Appendix 4-3) to query and select the specific order number, sequentially choosing functions "Generate File," "Apply for Download Approval," "Download File," and "Download Decryption Program." The "Generate File" function executes the uploaded SQL to produce the host-end operation result file. The "Apply for Download Approval" function sends the first twenty data contents (including the option to mark whether it is statistical data) of the operation result file to the electronic form for business division head for approval. After approval, select the "Download File" function. The "On-site Operation Management System (YST)" will then encrypt the operation results file with a password set by the system personnel and send it to the system personnel's mailbox. For the local tax platform, use the "On-site Operation Execution" option to "Database Query Result Download (YST204M)" for querying and downloading (as shown in Appendix 5-3).
(4) The FIA's Tax Information System personnel should complete the "Tax System On-Site Operation Application" (see Appendix 6) to request downloading of on- site operation result files. The "On-Site Operation Data Export Form" (see Appendix 24) should also be filled out. Once approved by the business division and management division, the Information and Communication Division's management personnel shall grant permission to use portable storage media for copying and exporting data.
(5) If the operation result file is a non-statistical data download case, the business division head should make a note during sign-off and should

remind the handler to report and cancel the oversight within 30 days from the data generation date.

VIII. Information Security Audit Procedures

1. Fiscal Data Research Center (see Operation Flowchart 1 “Audit”)

(1) The business division should audit and respond to the results based on the “Fiscal Data Research Center On-site Operation Personnel Entry and Exit Control Registration Form” (Appendix 14) transferred by the Information and Communication Division every two weeks.

(2) Information and Communication Division conducts self-audits:

a. Access control personnel conduct random daily inspections of the working environment and must ensure the security seals on computer equipment are intact at the end of the day.

b. Periodically designate personnel to check if the on-site operation staff matches the “Fiscal Data Research Center On-site Operation Personnel Entry and Exit Control Registration Form” (Appendix 14).

2. Tax System Operations Monitoring Room (see Operation Flowchart 2 “Audit”)

(1) Every two weeks, the Information and Communication Division prints the “National (Local) Tax System On-site Operation Management System Database Record Self-audit List” (Appendixs 26 & 27) and “National (Local) Tax System On-site Operation Management System Traditional File Record Self-audit List” (Appendixs 26 & 27). They send them in paper or electronic format to the relevant application divisions. The business divisions must self-audit these records and report the results to the supervising division, retaining them for three years for reference.

(2) Every two weeks, the Information and Communication Division prints the “National Tax System On-site Operation System Tax Data Export Record List” (Appendix 28) and “Local Tax System On-site Operation (YST) Application and Actual Download Record Table” (Appendix 29) and sends them to relevant application divisions for review. If the downloaded data is not statistical and the case handler fails to approve it within 30 days of data production, the business division should report to the FIA’s head. The review results are retained for three years for reference.

(3) Every two weeks, the Information and Communication Division conducts self-audits. The operations control personnel should match with access control personnel the “Tax Platform On-site Operation Personnel Entry and Exit Monitoring Room Control Registration Form” (Appendix 15) and the review results are retained for three years for reference.

(4) When using the “On-site Operation Management System (YST)” to apply for on-site operations, file names should be noted, including the results file application, and the various self-audit lists (Appendices 26, 27, 28, and 29). The business divisions must assign dedicated personnel to audit downloaded files and retain them, reporting the results to the division head and review results are retained for three years for reference.

3. High-level Permission Command Operation Monitoring Room

(1) According to the “Ministry of Finance and its Affiliated Agencies High-level Permission Account Management Procedure,” the high-level permission account management (recipient) division should have the “High-level Permission Account Routine Operation Record Table” and “High-level Permission Account Non-Routine Operation Record Table” sent bi-weekly to application divisions for self-audit.

(2) The Information and Communication Division conducts self-audits every two weeks, assigning dedicated personnel to review the “High-level Permission Command Operation Monitoring Room Computer Registration Book” (Appendix 17). After reporting the review results to the division head, they are retained for three years for reference.

(3) Based on the “Access Control System Entry and Exit Change Application Form” (Appendix 7), the management (recipient) division produces a list of approved entries into the High-level Permission Command Operation Monitoring Room every quarter. The list is sent to the application divisions for confirmation and retained for three years for reference.

IX. Fee Method

Fees are determined according to the “Ministry of Finance Fiscal Information Agency’s Tax Information Charging Standard.”

X. Suspension of Use Conditions for the Financial Data Research Center and Tax System Operations Monitoring Room

	If personnel exhibit any of the following behaviors, the FIA can unconditionally suspend their use of the Financial Data Research Center or Tax System Operations Monitoring Room. If damages are caused, compensation may be demanded: (1) Import, export, or transferring and recording data without application. (2) Eating, using cell phones, filming (recording) equipment, or using laptops (tablets) within the Financial Data Research Center or Tax System Operations Monitoring Room, especially if repeated after warning. (3) Unauthorized changes, movement, or damage to software or hardware equipment.
Attachments：	Workflow Diagram.pdf Attachment.pdf Appendices and Tables.pdf