China Development Financial Holding Corporation Security and Maintenance Plan for the Protection of Personal Data Files and Guidelines for Disposing Personal Data Following Business Termination

Drafted by: Compliance Dept.
Date of First Version: December 27, 2013
Date of Latest Version: December 10, 2020

Chapter 1 General Provisions

Article 1 The Plan and Guidelines are established in accordance with the "Regulations Governing the Security and Maintenance of Personal Data Files of Non-government Agencies Designated by the Financial Supervisory Commission" and CDF's Personal Data Protection and Management Policy.

Article 2 The terms used in the Plan and Guidelines denote the following meanings:

1. "Data Subject" refers to an individual whose personal data is collected, processed, or used.
2. "Personal Data Security Incident" refers to an incident reported internally or externally, depending on the cause and effect of its occurrence, which involves the theft, alteration, destruction, loss, leakage of personal data or other infringement on the rights and interests of a Data Subject.
3. "Serious Personal Data Security Incident" refers to the occurrence of a personal data security incident that will jeopardize the normal operation of CDF or the rights and interests of a large mass of Data Subjects.
4. "Unit in Charge of Incident" refers to a unit which is responsible for the causes of Personal Data Security Incidents.
5. "Special Personal Data" refers to data pertaining to an individual's medical records, healthcare, genetics, sex life, physical examination, and criminal records as prescribed in Article 6, Paragraph 1 of the Personal Data Protection Act.

Article 3 The scope of personal data management includes the collection, processing and use of personal data involved in the execution of business, projects, and internal administration by all employees and third-party partners of CDF.

Article 4 The goals of CDF's personal data management are as follows:

1. Set up a proper personal data protection system in accordance with relevant laws and regulations and the requirements of the authority in charge to ensure the proper management of personal data;
2. Implement the operating procedures for the collection, processing, and use of personal data to prevent personal data from being stolen, altered, damaged, destroyed, disclosed or used unreasonably; and
3. Fulfill the duty of care as a good administrator to build the data subjects' trust and safeguard their rights and interests.

Chapter 2 Personal Data Protection and Management Organization

Article 5 The following shall be reported to the President for approval: review and supervision of CDF's personal data protection and management system, cross-department coordination and cooperation, integration and application of various resources, and deliberations and promotion of other matters in relation to personal data protection and management.

Article 6 CDF shall set up a personal data protection task force (the "Task Force"), which shall constitute the representative of each department. The Task Force is responsible for evaluating, planning, and implementing CDF's personal data protection and management system and related work, coordinating each department's effort, and handling matters in relation to personal data protection and management as prescribed in the Plan and Guidelines.

As the business unit of the Task Force, Compliance Dept. is responsible for convening and presiding over the Task Force meetings and synthesizing the matters that the Task Force takes charge of in the preceding paragraph.

The members of the Task Force representing the departments are the contacts of the departments for matters in relation to personal data protection and management. In addition to raising concerns and proposing in the Task Force meetings, the members are responsible for following up the progress of personal data protection and management in the departments.

Chapter 3 Scope of Personal Data

Article 7 For the purpose of personal data management, the information security department may check on personal data in the personal computers at each department and hand over the results to the members of the Task Force representing the departments. Each department shall identify business processes in relation to personal data and check on personal data, so as to define the scope of personal data.

Article 8 The scope of personal data shall be defined according to the following procedures:

1. Each department shall identify relevant business processes containing personal data and fill in the "Personal Data Process Checklist" (Attachment 1) based on the results of identification; and
2. Each department shall check on files containing personal data based on the "Personal Data Process Checklist" and fill in the "Personal Data Checklist" (Attachment 2).

Each department shall assign appropriate personnel to fill in the "Personal Data Process Checklist" and the "Personal Data Checklist," which shall be submitted to the Task Force upon approval of the head of the department.

Article 9 Each department shall compile and maintain the "Personal Data Process Checklist" and the "Personal Data Checklist" and submit the same to the Task Force on a regular basis.

In case of the addition, revocation, or modification of business processes or personal data files (e.g., adjustment of business processes or personal data files or change in administrators), each department shall update the "Personal

Data Process Checklist" and the "Personal Data Checklist" and submit the same to the Task Force in a timely manner.

Article 10 CDF shall identify business processes and check on personal data at least once every year according to the frequency of risk assessment prescribed in Chapter 4.
In case of changes in the organization or operating procedures, major changes in personal data files, or the occurrence of Serious Personal Data Security Incidents, the Task Force may make a plan for identifying business processes and checking on personal data within the certain scope and have it executed by relevant departments.

Chapter 4 Personal Data Risk Assessment and Management

Article 11 After defining the scope of personal data, each department shall conduct a risk assessment at least once every year.

Article 12 The risk assessment referred to in the preceding article shall be conducted according to the following procedures:

1. After identifying the business processes, each department shall further identify the potential risk of personal data security incidents and fill in the "List of Risk Scenarios" (Attachment 3). Each department shall also conduct the legality analysis and the process impact analysis respectively based on the aforesaid business processes and fill in the "Legality Analysis Form" (Attachment 4) and the "Personal Data Process Impact Analysis Form" (Attachment 5); and
2. After completing the process impact analysis, each department shall conduct a risk assessment, where the "Personal Data Process Risk Assessment Form" (Attachment 6) is used to calculate the risk value of each business process, and shall make the "Plan for Handling Personal Data Management Risks" (Attachment 7) accordingly.

Each department shall assign appropriate personnel to fill in the aforesaid "List of Risk Scenarios," "Legality Analysis Form," "Personal Data Process Impact Analysis Form," "Personal Data Process Risk Assessment Form," and "Plan for Handling Personal Data Management Risks," which shall be submitted to the Task Force upon approval of the head of the department.

Article 13 The Task Force shall prioritize the risks based on the "Personal Data Process Risk Assessment Form" completed by each department, and shall assess the acceptable risks based on the impact intensity, risk value, and acceptable costs and distributable resources.
The business unit of the Task Force shall assign personnel to prepare the "Self-assessment Report on Personal Data Management Risks" based on the results of the assessment. The said report shall be submitted to the Task Force for deliberations and then reported to the President for approval.

Article 14 In case of changes in the organization or operating procedures, major changes in personal data files, or the occurrence of Serious Personal Data Security Incidents, the Task Force may make a plan for assessing the risks of personal

data within the certain scope and have it executed by relevant departments.

Article 15 The operating procedures for the risk assessment prescribed in this chapter are detailed in the "Description of Procedures for Personal Data Risk Assessment and Handling" (Attachment 8).

Chapter 5 Notification, Handling, and Prevention of Personal Data Security Incidents

Article 16 When finding any suspicious Personal Data Security Incident, each department's personnel shall immediately report to the member of the Task Force representing the department, who is responsible for determining whether the reported case is truly a Personal Data Security Incident. If the reported case is truly a Personal Data Security Incident, the department shall take appropriate emergency measures immediately and fill in the "Personal Data Security Incident Notification" (Attachment 10) and submit the same to Compliance Dept. Upon receiving the notification, Compliance Dept. shall convene a meeting of the Task Force to identify the Unit in Charge of Incident, and shall cooperate to take emergency measures.

If the Personal Data Security Incident constitutes a serious contingency, it shall be handled in accordance with the "Guidelines for Handling Material Contingencies."

Article 17 Units in Charge of Incident and relevant departments shall take appropriate emergency measures for Personal Data Security Incidents according to the instructions and depending on the nature of the incidents. All analyses and records of the incidents handled shall be retained.

The Task Force shall cooperate to clarify the causes and effects of the incidents, and shall coordinate relevant departments' efforts to keep the incidents under control, so as to reduce possible losses arising therefrom.

The emergency measures referred to in the preceding two paragraphs may include, but are not limited to, the following:

1. Interrupt the path of breach or leakage;
2. Initiate the backup procedures or alternatives;
3. Conduct a preliminary analysis of the causes of the accidents;
4. Assess the type and quantity of personal data breached;
5. Check the functions of protection and monitoring equipment;
6. Record the incidents;
7. Retain relevant evidence before the completion of internal investigations;
8. Initiate solutions or recovery plans;
9. Notify other units that hold the same data;
10. Seek professional assistance or on-site troubleshooting.
11. Refer those involving criminal responsibility to the prosecutors for authentication or investigation; and
12. Publish internal notices, press releases, and website announcements and notify the Data Subjects or the authority in charge.

Article 18 Personal Data Security

After clarifying the incidents, the Units in Charge of Incident shall consult the business unit of the Task Force and report to the President for approval before

notifying the Data Subjects of the facts that their personal data have been breached, the emergency measures taken by CDF, and a consultation hotline in an appropriate manner.

The notification referred to in the preceding paragraph may be given verbally, in writing, by telephone, SMS, email, or fax, or electronically, or in other ways sufficient to make the Data Subjects aware or known, provided that relevant records shall be kept. If such notification costs a lot, it may be given publicly through the Internet, press releases or other appropriate means.

Article 19 The business unit of the Task Force shall compile the complete material and evidence of the Personal Data Security Incidents and follow up how such incidents are handled, and shall report to the President depending on the seriousness of such incidents. Serious Personal Data Security Incidents, if any, shall be reported to the authority in charge immediately.

Article 20 After a Personal Data Security Incident is cleared, the business unit of the Task Force may convene a post-review meeting of relevant departments or personnel as needed to analyze the cause of the incident and deliberate on relevant corrective and preventive measures. Such measures shall be taken upon approval of the President to prevent a recurrence of the incident or the occurrence of a potential incident.

In case of a Serious Personal Data Security Incident, the corrective and preventive measures referred to in Paragraph 1 shall be diagnosed and examined by experts who work impartially and independently and hold accepted certificates.

Chapter 6 Internal Procedures for Collecting, Processing, and Using Personal Data

Article 21 Each department shall collect, process, and use personal data necessary for the performance of business duties in compliance with the following principles:

1. The collection, processing, and use of personal data shall be carried out in a way that respects the Data Subject's rights and interest;
2. The collection, processing, and use of personal data shall be carried out in an honest and good-faith manner without intentionally concealing it from the Data Subject;
3. The collection, processing, and use of personal data shall not exceed the necessary scope of specific purposes;
4. The collection, processing, and use of personal data shall have legitimate and reasonable connections with the purposes of collection; and
5. The collection, processing, and use of personal data shall be based on the minimum data fields within the necessary scope of specific purposes.

Article 22 Each department shall comply with relevant laws and regulations when collecting, processing or using Special Personal Data due to special needs.

Article 23 In accordance with Article 8, Paragraph 1 of the Personal Data Protection Act, each department is obligated to inform the Data Subjects when collecting their personal data directly. However, the obligation to inform may be waived under any of the circumstances prescribed in Article 8, Paragraph 2 of the Personal Data Protection Act.

The notification referred to in the preceding paragraph may be given verbally, in writing, by telephone, SMS, email, or fax, or electronically, or in other ways sufficient to make the Data Subjects aware or known, provided that relevant materials shall be retained for future review.

If the Data Subjects do not have a capacity to make juridical acts, have a limited capacity to make juridical acts, or are subject to an order of commencement of assistance, the notification shall be given to their legal representatives, guardians, or assistants.

Article 24 CDF shall, before processing or using the collected personal data which are not provided by the Data Subjects, inform the Data Subjects of the source of data and other matters specified in Article 8, Paragraph 1, Subparagraphs 1 to 5 of the Personal Data Protection Act. However, the obligation to inform may be waived under any of the circumstances prescribed in Article 9, Paragraph 2 of the Personal Data Protection Act.

Article 25 Except for Special Personal Data, the collection or processing of personal data shall be for specific purposes and on one of the following bases:

1. Where it is expressly required by law;
2. Where there is a contractual or quasi-contractual relationship between CDF and the Data Subjects, and proper security measures have been adopted to ensure the security of the personal data;
3. Where the personal data have been disclosed to the public by the Data Subjects or have been made public lawfully;
4. Where consent has been given by the Data Subjects;
5. Where it is necessary for furthering public interest;
6. Where the personal data are obtained from publicly available sources unless the Data Subjects have an overriding interest in prohibiting the processing or use of such personal data; or
7. Where the rights and interests of the Data Subjects will not be infringed upon.

CDF shall, on its own initiative or upon the request of the Data Subjects, erase or cease processing or using the personal data when it becomes aware of, or upon being notified by the Data Subjects, that the processing or use of the personal data should be prohibited pursuant to the proviso to Subparagraph 6 of the preceding paragraph.

Article 26 The use of personal data for another purpose shall be only on any of the following bases:

1. Where it is expressly required by law;
2. Where it is necessary for furthering public interest;
3. Where it is to prevent harm on life, body, freedom, or property of the Data Subject;
4. Where it is to prevent material harm on the rights and interests of others;

5. Where consent has been given by the Data Subject; or
6. Where it is for the Data Subject's rights and interests.

Article 27 CDF shall abide by the following principles when using personal data for marketing purposes:

1. Upon the Data Subject's objection to such use, CDF shall cease using the Data Subject's personal data for marketing; and
2. When using the Data Subject’s personal data for marketing purposes for the first time, CDF shall provide the Data Subject the ways to object to such use, and CDF shall pay for the fees therefrom.

Article 28 CDF shall establish, and implement accordingly, relevant procedures for the Data Subjects to exercise their rights regarding to their personal data

Article 29 Each department shall verify personal data in detail when performing business duties. If the copies of the credentials are retained according to law, each department shall record the purpose and scope of restricted use to prevent the credentials of the Data Subjects from illegal use.

In the event of a dispute regarding the accuracy of the personal data, each department shall, on its own initiative or upon the request of the Data Subject, cease processing or using the personal data, unless the processing or use is either necessary for the performance of an official or business duty, or has been agreed to by the Data Subject in writing, and the dispute has been recorded.

Where a request is made by a Data Subject to each department pursuant to Article 11 of the Personal Data Protection Act, each department shall determine whether to accept or reject such a request within thirty (30) days; the deadline may be extended by up to thirty (30) days if necessary, and the Data Subject shall be notified in writing of the reason for the extension.

Each department shall, on its own initiative, notify the external units when finding that it has provided incorrect or non-up-to-date personal data to the external units in order to protect the rights and interests of the Data Subjects from the use of such incorrect data.

Article 30 Personal data shall be retained for a period of time as required by law or prescribed in the relevant regulations of CDF. If no laws or relevant regulations of CDF are available, the unit in charge of data retention may set another appropriate time limit based on the necessity and reasonableness of the performance of business duties, or delete or stop processing or using the personal data per Data Subject's request.

If there are reasons to extend the period of retention due to business needs (e.g., subsequent audits, comparison or certification), the unit in charge of data retention shall give full consideration to the cost of retention and take security and maintenance measures for data retained.

After the termination of business, relevant records of the processing of personal data or the deletion or destruction of data shall be kept.

Article 31 CDF shall comply with the following regulations to ensure that personal data are transferred outside the country (border) with an appropriate level of protection:

1. CDF shall check whether the country (region) receiving the personal data is restricted by the central authority in charge of relevant business from transferring personal data across the country (border), and shall process the data in accordance with the restrictions issued by the central authority in charge of relevant business; and
2. When disclosing personal data to a third party outside the country (border) or entrusting personal data outside the country (border), CDF shall request the entrusted unit to comply with the relevant provisions of the Personal Data Protection Act.

Article 32 CDF shall comply with the following regulations when disclosing personal data to an external third party:

1. CDF shall disclose personal data to an external third party in the manner prescribed by law or after obtaining the written consent of the Data Subject except for circumstances where notification may be waived in accordance with the law;
2. CDF shall ensure that only the minimal content of the personal data is disclosed to an external third party;
3. CDF shall have control over the transfer of personal data to a third party in accordance with the existing internal regulations pertaining to personal data management;
4. All records of the transfer of personal data to any third parties shall be kept for at least five (5) years; and
5. If personal data are transferred by mail, they shall be processed as confidential letters in accordance with CDF's relevant documentation regulations.

If the third party referred to in the preceding paragraph is a government agency (e.g., administrative agency or judicial agency) or another agency concerned, a written original inquiry such as an official letter or inquiry form of an external agency shall be provided. In case of an urgent inquiry under a special circumstance, the head of the agency receiving the inquiry or a person designated by the head in writing may first transfer the personal data by telephone or fax. Upon confirmation, the personal data shall be transferred per the third party's request.

Except as required by law, CDF shall, before transferring or copying personal data to a third party due to business needs, confirm that the third party has signed a contract or quasi-contract with CDF that specifies the rights and obligations of both parties and can be used as the basis for transferring or copying the personal data.

Article 33 CDF shall comply with the following regulations when entrusting the collection, processing, or use of personal data to a third party:

1. CDF shall understand and review the existing security controls of the entrusted unit as needed before signing a contract with it;
2. CDF shall confirm that the content of the contract meets the requirements of relevant laws and regulations;

3. CDF shall supervise the entrusted unit in aspects including but not limited to the following:
   (1) CDF shall identify the intended scope, classification, specific purpose and period of personal data collected, processed, or used;
   (2) CDF shall confirm that the entrusted unit takes proper security and maintenance measures in accordance with the Personal Data Protection Act;
   (3) CDF shall determine whether the entrusted unit is eligible to entrust another third party. If the entrusted unit is eligible to entrust another third party, it is required to have the third party agree in the service entrustment contract to be at least under the same obligation to protect the personal data as the entrusted unit;
   (4) The entrusted unit or any of its employees shall notify CDF when violating the Personal Data Protection Act or the terms of the service entrustment contract, and shall take appropriate corrective measures;
   (5) CDF may conduct the audits of the entrusted unit's personal data management within the scope of the contract whenever necessary;
   (6) The contract shall specify the methods of compensation/damages to or reconciliation/negotiation with the Data Subjects and CDF for reasons attributable to the entrusted unit;
   (7) CDF shall supervise the additional directives given to the entrusted unit, if any; and
   (8) When the entrustment relationship is terminated or rescinded, CDF shall request the entrusted unit to return the media storing the personal data and delete or destroy the personal data stored at the entrusted unit.
4. If the service entrustment contract contains personal data (e.g., a non-disclosure agreement), the retention period of the written contractual data shall be consistent with the retention period of the personal data;
5. The entrusted unit shall conduct appropriate training for its executive personnel when processing a large amount of personal data or sensitive personal data; and
6. CDF shall periodically confirm the progress of the entrusted unit and record the results of such confirmation.

Chapter 7 Personnel Management

Article 34 To safeguard the retained personal data, CDF shall set the limits of authority and appropriate controls as required in the performance of business duties to manage personnel who have access to the personal data.

Article 35 The personnel hired or employed by CDF shall sign, accept, and comply with all the terms and conditions pertaining to personal data protection in the employment contract or labor contract (including a confidentiality agreement), and shall comply with the personal data protection provisions and responsibilities set out in the rules and regulations at the department level.

Article 36 Prior to personnel transfer or separation, the head of the department shall ensure that

the personnel have returned related personal data files and records in their custody and that their access to related files and records has been revoked; the personnel shall also give a written promise that they will continue complying with the relevant provisions of the Personal Data Protection Act after the transfer or separation.

Chapter 8 Personal Data Security Management

Article 37 CDF shall take the confidentiality, risk, and sensitivity of personal data into account when storing and processing the personal data, and shall manage the personal data in an appropriate manner (including but not limited to transmission, printing, destruction, and access control).

Article 38 Each department shall take appropriate controls for computer equipment used to collect, process, and use personal data, including floppy disks, USB ports, and CD-ROM drives.

Article 39 The IT department shall conduct backup verification on a regular basis to confirm the readability of backup data and the availability of storage media.

Article 40 CDF shall publish the "Privacy Policy" on its public website in an accessible manner. The Privacy Policy shall contain relevant consultation channels and expressly stipulate the rights of users on the website.

Article 41 If the content of CDF's public website involves the collection, processing, and use of personal data, personal data shall be collected, processed, and used by the business management unit only after it is countersigned by Compliance Dept.

Article 42 CDF shall grant access to personal data for a minimum required in the performance of business duties and work.

Article 43 For a system containing personal data, its user access administrator shall ask the head of each department to check on the appropriateness of personnel's authority on a regular basis.

Article 44 The IT department shall ensure that each system keeps an appropriate record of access to personal data based on the need of each unit, and shall adopt appropriate protection.

Article 45 CDF shall take the following information security measures for the e-commerce system provided:

1. User authentication and protection;
2. Hidden codes for personal data;
3. Data encryption in transit via the Internet;
4. Software verification and validation in the development, launch, and maintenance of application systems;
5. Access control and monitoring measures for personal data files and databases;
6. Countermeasures for network intrusion; and
7. Monitoring and response mechanism to illegal or abnormal use.

Periodical drills and reviews shall be carried out for the measures referred to in Subparagraphs 6 and 7 of the preceding paragraph.

Chapter 9 Awareness Promotion and Training

Article 46 Persons in charge of the daily operation's compliance with the personal data management policy shall understand thoroughly personal data protection laws and practices and be able to put them into practice, and shall obtain information pertaining to personal data management in a timely manner.
All personnel of CDF shall be aware of their own responsibility for the protection of personal data, and shall protect and process personal data according to the appropriate procedures.

Article 47 CDF shall conduct awareness promotion and training on personal data protection for its personnel (including external personnel who are stationed at CDF and responsible for the collection, processing, or use of personal data).
The awareness promotion and training referred to in the preceding paragraph may be conducted in various forms such as meetings, electronic propaganda, written propaganda, or events.

Chapter 10 Equipment Security Management

Article 48 CDF shall establish controls for the relevant units in charge to manage the hosts, computer equipment, and other media that store or transmit personal data files.

Article 49 Each department shall manage equipment used to process or store personal data in accordance with CDF's "Directions for Computer Operation Security," "Instructions for Server and Personal Computer Management," and "Directions for Network Management."

Chapter 11 Retention of Personal Data User Records, Data Traceability, and Evidence

Article 50 Each department shall retain the following personal data user records, data traceability, and evidence within the necessary scope in ways in proportion to the intended purposes of personal data protection:

1. Records of delivery and transmission of personal data;
2. Records of confirmation and correction of personal data;
3. Records of a Data Subject's exercise of their rights;
4. Records of deletion and destruction of personal data;
5. Records of access to personal data through a system;
6. Records of backup and recovery tests;
7. Records of addition, change, and deletion of personnel's authority;
8. Records of violation of personnel's authority;
9. Records of actions taken in response to Personal Data Security Incidents;
10. Records of periodical checks on the information systems containing personal data;
11. Records of training; and
12. Records of relevant audits and corrective procedures.

Unless otherwise provided by law or CDF, the aforesaid records shall be kept for at least five (5) years.

Article 51 Personnel shall be duly authorized to use personal data, whether in a system or on hard copy, and shall maintain the correctness of the personal data.

Article 52 The Task Force shall collect the complete evidence of Personal Data Security Incidents and review and analyze the causes of the incidents, and shall coordinate relevant departments' efforts to take corrective and preventive measures, so as to avoid the recurrence of the incidents or prevent the occurrence of potential incidents.

Chapter 12 Audit Mechanisms for Personal Data Security

Article 53 CDF shall incorporate personal data into internal control and internal audit systems. Relevant procedures, methods, and frequency of the audits are outlined in the "Regulations for Audit Operations."
The audit department shall draw up an audit form in accordance with laws and regulations, relevant regulations of CDF, and external standards and conduct relevant audits using the audit form.

Article 54 CDF shall incorporate personal data protection into the compliance self-evaluation, and shall conduct regular evaluations to ensure compliance with relevant laws and regulations.

Chapter 13 Continuous Improvement in Personal Data Security and Maintenance

Article 55 Each department shall take and continuously improve personal data security and maintenance measures in accordance with the Plan and Guidelines.

Article 56 Based on the results of the "Self-assessment Report on Personal Data Management Risks," the Task Force shall review and revise the Plan and Guidelines in a timely manner. The Task Force shall also plan on the corrective and preventive measures for any violations of laws and regulations found.

Article 57 The business unit of the Task Force shall conduct an evaluation at least once every year using the "Personal Data Management System Matrix" (Attachment 9). The results of the evaluation are used as a reference for improvement in the personal data management system.

Chapter 14 Supplementary Provisions

Article 58 Unspecified matters in the Plan and Guidelines shall be governed by relevant laws and regulations and the requirements of the authority in charge.

Article 59 The Plan and Guidelines, and any amendments thereafter, shall take effect on the date of promulgation upon approval of the President.