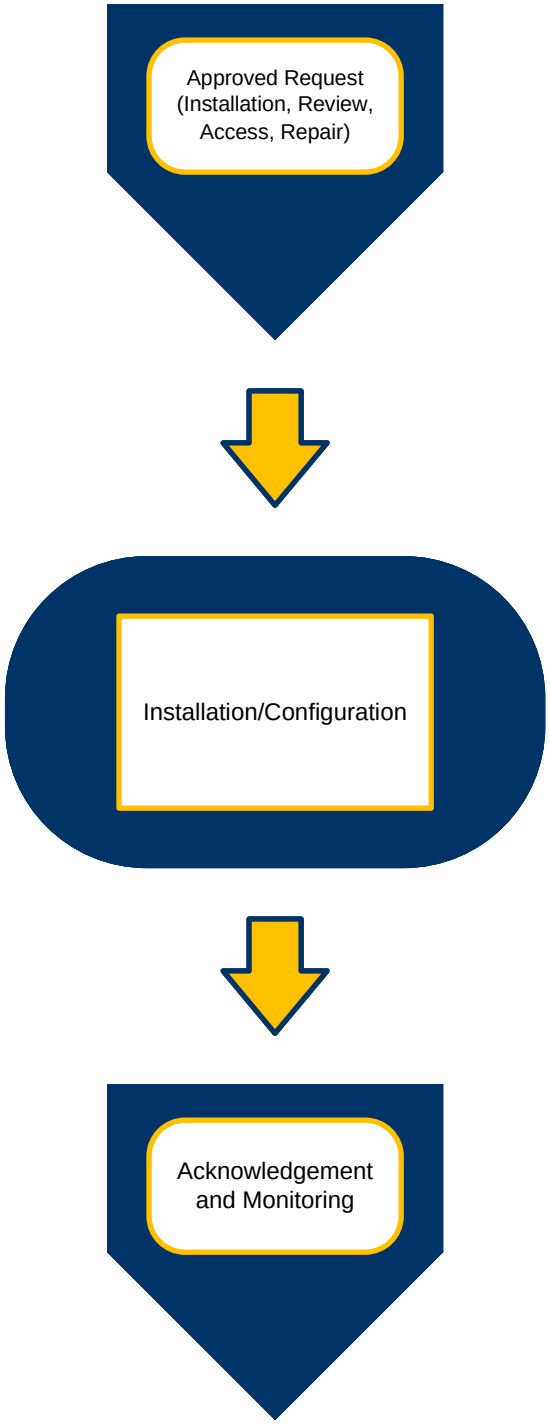

Approved Request (Installation, Review, Access, Repair)
Installation/Configuration
Acknowledgement and Monitoring

1.0. OBJECTIVE

1.1 The objective of this policy is to standardized the process related with the company's CCTV system and ensures that its sensitive information will be kept confidential as necessary.

2.0 SCOPE

2.1 This policy applies to CVM Finance Head Office, Branches and authorized employees that will access to the company's CCTV.

3.0. DEFINITION OF TERMS

3.1 CCTV – Closed Circuit Television, one of the security equipment that protects business establishments from unwanted events and monitor activities happening in the premise.

4.0 POLICY

4.1 INSTALLATION

4.1.1 Installation of CCTV equipment to Head Office and/or branch to safeguard and compliance
- 4.1.4.1 CCTV Equipment Configuration
  - 4.1.4.1.1 Camera configuration
  - 4.1.4.1.2 IP configuration
  - 4.1.4.1.3 DVR configuration
  - 4.1.4.1.4 Device registration to Hikvision administrative account
- 4.1.4.2 Camera Positioning
- 4.1.4.3 Cabling and Termination
- 4.1.4.4 Testing
- 4.1.4.5 Documentation

4.2 MONITORING

4.2.1 Daily monitoring of all CCTV equipment
- 4.2.1.1 ITG personnel from hardware team are assigned to monitor and check the CCTV equipment of all areas and head office.
- 4.2.1.2 Checking and monitoring considered the following activities
  - 4.1.1.2.3 Recording Status
  - 4.1.1.2.2 Online Status
- 4.2.1.3 Assigned ITG personnel(s) records any remarks found during the monitoring
- 4.2.1.4 ITG will be sending a monitoring report through email to Operation's Officers and Manager, and also includes recipients from other team that needs such updates including Audits and Managerial positions.

4.3 FOOTAGE REQUEST

4.3.1 Requests for footage from CCTV systems must be accompanied by accomplished CCTV Request Form to be submitted to ITG, and shall include the date, time, and location of the incident or event for which footage is requested.

4.3.2 Requests for footage from CCTV systems shall be approved by the team head of requesting employee.

4.3.3 The organization shall retain the right to deny any request for footage if the request is deemed to be improper, unreasonable, or in violation of applicable laws and regulations from both organization and/or Philippine Laws and Regulations.

4.3.4 ITG shall maintain a log of all requests for footage from CCTV systems, including the date and time of the request, the name of the individual making the request, the reason for the request, and the date and time the footage was released.

4.3.5 Footage from CCTV systems shall be released only in accordance with applicable laws and regulations, and shall not be edited, altered, or shared with anyone outside the organization without prior written authorization and/or request from government authority.
Yet, clause 4.3.4 can still be considered by ITG and/or CVM Finance and Credit Corporation whenever necessary.

4.4 ONLINE ACCESS AUTHORIZATION

4.4.1 Access to the CCTV System through online means shall be granted only to Authorized employees such as from ITG, Audit Officers, Operation's Area Officers, MANCOM, and/or other teams/employees that will be granted by the requesting team's Head and ITG's Team Head. However, all requesting personnel must accomplished and submit all the following documents to gain an online viewing access. Failed to complete the following documents, ITG has the authority to hold and/or deny the request of CCTV Online Viewing Access.
- 4.4.1.1 Online CCTV Viewing Access Form
- 4.4.1.2 CCTV Confidentiality Agreement

4.4.2 Granted personnel must be logged to ITG's monitoring which includes the information that are stated in accomplished Online CCTV Viewing Access Form

4.4.3 Access to the CCTV system through online means shall be immediately revoked when the authorized personnel need for access no longer exists or when an individual's employment relationship with the company is separated or terminated.

4.4.4 Authorized Employee/User who access the CCTV system through online means shall be held accountable for any unauthorized access or misuse of CCTV system data.

4.4.5 Authorized Employee/User who access the CCTV system through online means must strictly abide to the CCTV Confidentiality Agreement. Otherwise, violation shall be subject to sanction in accordance with the employee code of conduct

4.5 CONFIDENTIALITY

4.5.1 Sensitive information obtained from CCTV systems shall be considered confidential and shall not be disclosed to anyone outside the organization without prior written request accompanied by a document coming from government authority.

4.5.2 Sensitive information obtained from CCTV systems shall not be distributed in any online means such as social medias, streaming sites, cloud storage outside of official business purpose without the consent of CVM Finance and Credit Corporation.

4.5.3 Access to sensitive information obtained from CCTV systems shall be granted only to authorized CVM Finance and Credit Corporation employees who have submitted required documents.

4.5.4 All employees/users who have access to sensitive information obtained from CCTV systems shall be required to sign a non-disclosure agreement that will secure the proper use and handling of such information.

4.5.5 Sensitive information obtained from CCTV systems shall be stored and transmitted securely, and all reasonable measures shall be taken to prevent unauthorized access, use, or disclosure of such information.

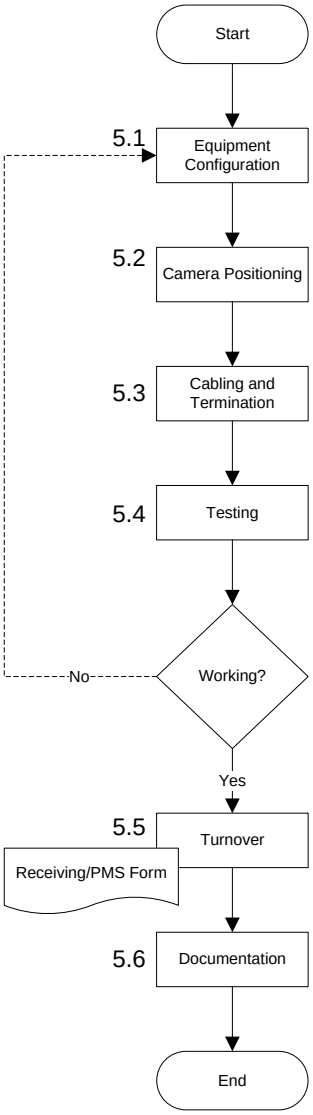
4.5.6 Any suspected unauthorized access, use, or disclosure of sensitive information obtained from CCTV systems shall be immediately reported to Information Technology Group for further actions.

4.5.7 Distribution of CCTV's data/information such as screenshots, footages, or video clips to other team/employees within the organization is strictly prohibited. Not unless, with the consented/approved by Information Technology Group.

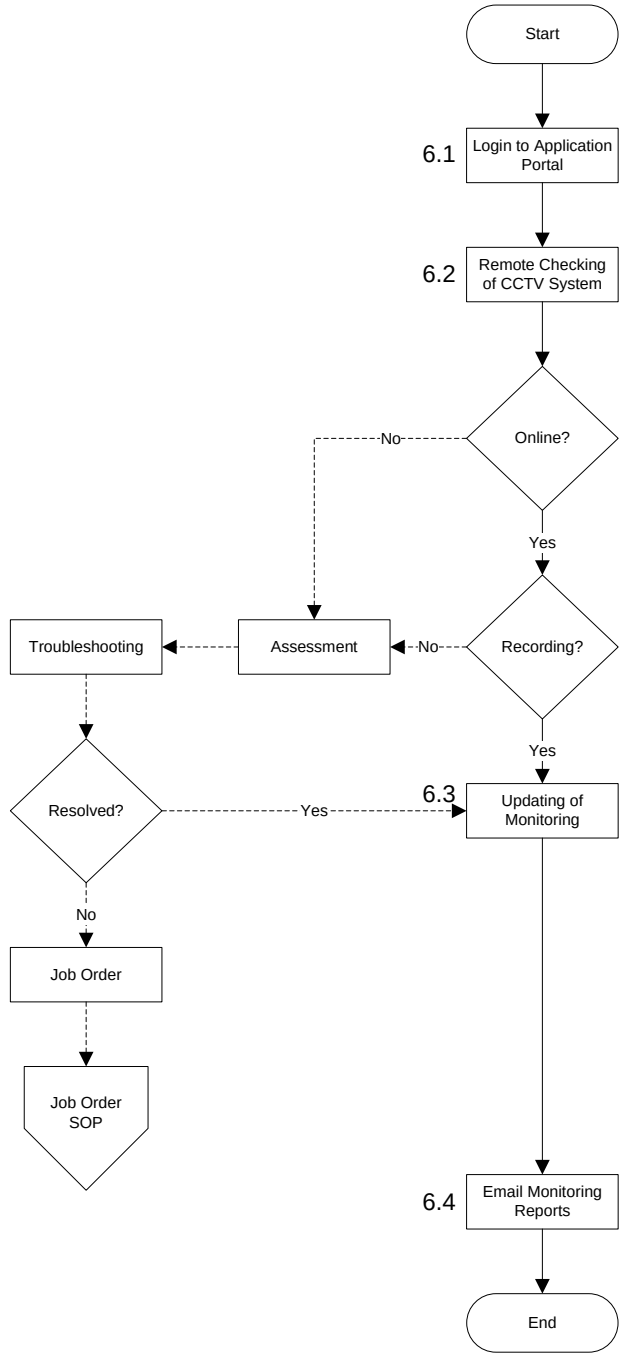
4.5.8 Data/Information obtained from CCTV System shall not be used in personal agenda(s)/interest that is unrelated to Official Business Purpose.

5.0 GUIDELINES

Responsibility	Process Flow	Guidelines
ITG Hardware	5.1 Equipment Configuration	**5.1 Equipment Configuration** 5.1.1 Configuration of the following devices and features. 5.1.1.1 Camera configuration 5.1.1.2 IP configuration 5.1.1.3 DVR/NVR configuration 5.1.1.4 Device registration to Hikvision administrative account
	5.2 Camera Positioning	**5.2 Camera Positioning** 5.2.1 ITG/Installer will position the camera accordingly and to whichever from the following list is applicable. 5.2.1.1 Vault Room 5.2.1.2 Releasing Area (Custodian) 5.2.1.3 Customer's Waiting Area 5.2.1.4 Entrance 5.2.1.5 Parking 5.2.1.6 Working Area
	5.3 Cabling and Termination	**5.3 Cabling Termination** 5.3.1 ITG/Installer will install and/terminate the wiring enclosed with flexible hose and/or PVC pipe, of whichever is applicable to protect and cover the lines from interference and pests. 5.3.2 Camera(s) must be mounted with Junction box to protect connectors. Yet, whenever applicable. 5.3.1 DVR/NVR must be enclosed inside a secure cabinet with lock. Yet, whenever application.
	5.4 Testing	**5.4 Testing** 5.4.1 Whenever all particulars are already mounted and installed, ITG will now test if configured and necessary setup is already completed. Else, it will be re-configured properly up to its working state prior proceeding to further steps.
	Working? (No / Yes)	**5.5 Turnover** 5.5.1 If the CCTV Installation is request by other Team/Officer, Receiving Form must be secured. Otherwise, Inventory monitoring must be updated for the proper generation of PMS report.
ITG Hardware/Requesting Team	5.5 Turnover Receiving/PMS Form	**5.6 Documentation** 5.5.1 MIS will now update inventory records 5.5.2 The developer must inform the concerning person and provide Satisfaction Survey Form.
	5.6 Documentation	

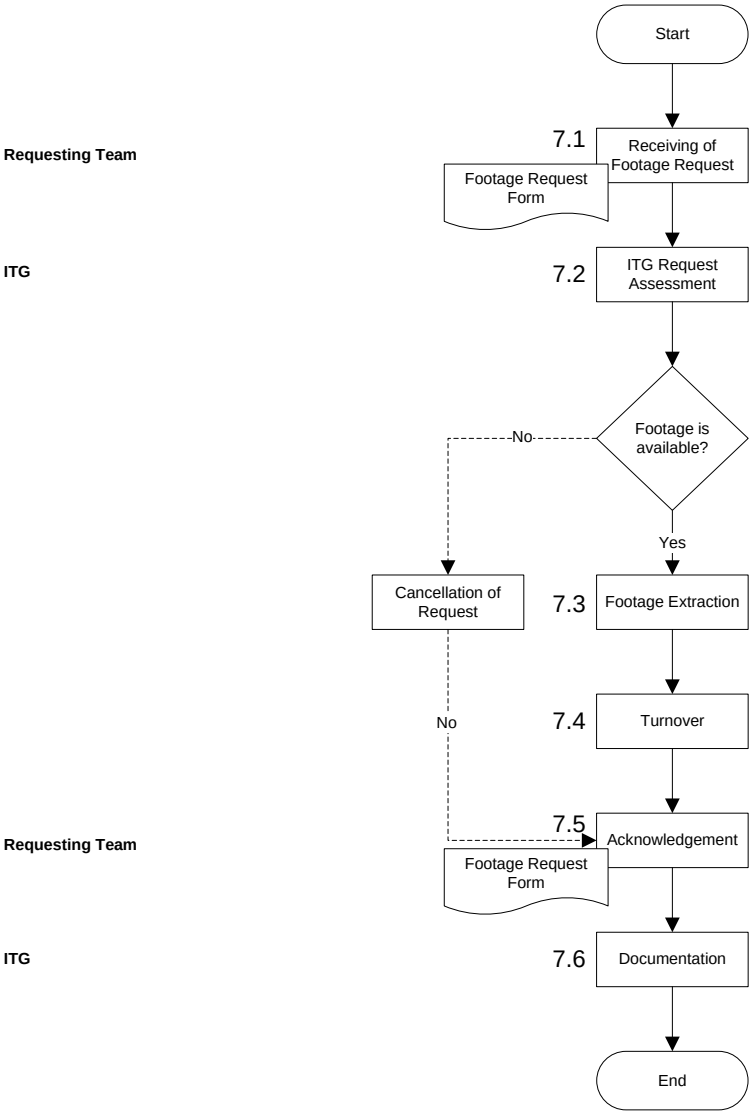


6.0 GUIDELINES

Responsibility	Process Flow	Guidelines
ITG Hardware		**6.1 Log-in to Application Portal** 6.1.1 Login to CCTV Online Viewing's Application Portal such as any of the following, or whichever is applicable. 6.1.1.1 Guarding Vision 6.1.1.2 Hik-Connect (latest) **6.2 Remote Checking of CCTV System** 6.2.1 ITG will now check the CCTV system of all offices through remote or online viewing. ITG monitors the status of said devices which includes Online, Recording status. 6.2.2 In event that the CCTV system is not online and/or not recording, ITG will isolate or assess the issue and provides further troubleshooting that can be done remotely. If the issue is not resolved, then it will further proceed to internal filling of Job Order, which can be referred to Job Order SOP. 6.2.3 Frequency of ITG's CCTV monitoring can be done twice a day during regular working days which it covers the AM and PM monitoring. However, Saturday only covers the AM monitoring. **6.3 Updating of Monitoring** 6.3.1 Regardless of its operational status and/or remote trouble-shooting result, ITG must update the monitoring in order to cascade an up to date monitoring remarks to concerned team. **6.4 Email Monitoring Reports** 6.4.1 ITG will send a Monitoring report via email which covers the monitoring results occurred within the day. 6.4.2 Recipients of this report may vary to teams that will be needing such update, and can secure the confidentiality of cascaded data like any of the following teams: 5.4.2.1 Audit Officers 5.4.2.2 MANCOM 5.4.2.3 ITG Officers 5.4.2.4 Operation's Area Officers 6.4.3 Reports can be sent by any personnel from ITG handling CCTV monitoring such as Area Its and/or Officers.

7.0 GUIDELINES

Responsibility | **Process Flow** | **Guidelines**



7.1 Receiving of Footage Request

7.1.1 ITG will receive signed and approved CCTV footage request from the requesting team.

7.1.2 Duly accomplished form consist of the following information that will be used further.

7.1.2.1 Date and time of for extraction

7.1.2.2 Incident summary

7.1.2.3 Other hints that will be helpful during the extraction

7.2 ITG Request Assessment

7.2.1 ITG will now assess the received CCTV footage request. If footage is not available, request will be cancelled that needs to be acknowledged by the requesting party. Otherwise, process will further proceed to footage extraction.

7.3 Footage Extraction

7.3.1 In extraction of footage, ITG can use any of the following means of storage to be used

7.3.1.1 USB flash drive

7.3.1.2 External hard drive

7.3.1.3 Cloud Storage such as Onedrive, Googledrive, etc.

7.4 Turnover

7.4.1 Once the needed CCTV footage has been retrieved, then ITG will turn over it to the requesting team while securing the acknowledgement of requesting party.

7.5 Acknowledgement

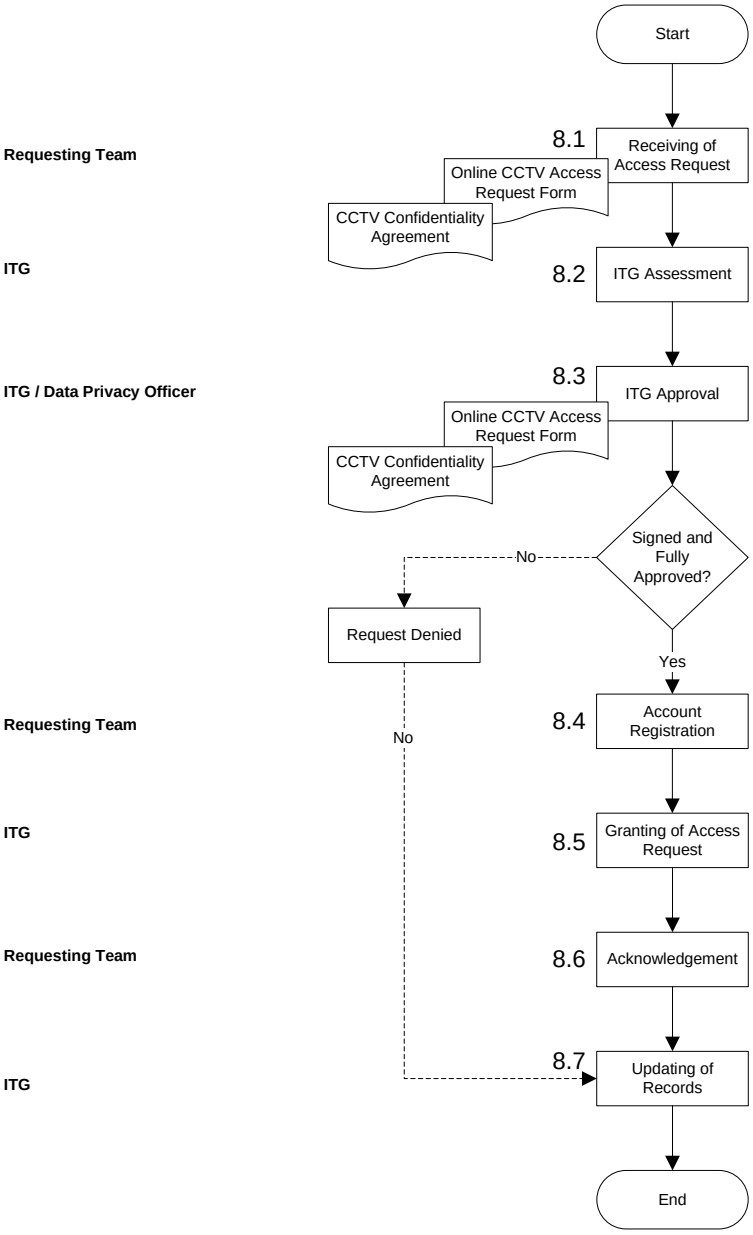
7.5.1 Upon acknowledgment of the received footage, the requesting party agreed to the confidentiality clauses mentioned under *clause number 4.5*

7.6 Documentation

7.6.1 ITG will update the monitoring

8.0 GUIDELINES

Responsibility | **Process Flow** | **Guidelines**



8.1 Receiving of Access Request

8.1.1 ITG will receive the following documents from requesting team.
- 8.1.1.1 Online CCTV Access Request Form
- 8.1.1.2 CCTV Confidentiality Agreement

8.1.2 Documents stated under clause number 8.1.1 must be fully approved by the requesting team's head. Otherwise, ITG has the authority to hold/deny the request.

8.2 ITG Assessment

8.2.1 ITG will assess the request if all the criteria are met ;
- 8.2.1.1 Reasonable request
- 8.2.1.2 Official business purpose
- 8.2.1.3 Approved by the requesting team's head

8.2.1 Failing to comply with all the criteria mentioned from clause number 8.2.1, ITG has the authority to hold/deny the request.

8.3 ITG Approval

8.3.1 Once all the needed documents are provided and all criteria mention from clause number 8.2.1 are met, documents are now proceeding to second level of approval from the ITG's Team Head and Data Privacy Officer.

8.3.2 Once request is approved by the ITG's Team Head and Data Privacy Officer, this can now proceed to further steps. Otherwise, request will be denied/cancelled in such event that request are disapproved.

8.4 Account Registration

8.4.1 Requesting party can now register or create an account through ITG's assistance.

8.4.2 Account registration must used an individual email. As using a team email is not allowed to ensure the confidentiality and accountability if any.

8.4.2 Requesting party must secure the created credential as he/she will held accountable for any indirect/direct violation that may cause.

8.5 Granting of Access Request

8.5.1 ITG will now authorized the Online Viewing Access to registered and validated account/email address.

8.6 Acknowledgement

8.6.1 Since, access had been granted, requesting party must acknowledged the submitted Online CCTV Access Request Form by affixing his/her signature as proof or evidence of completing such request.

8.7 Updating of Records

8.7.1 ITG will now update the monitoring.

9.0 FORMS

6.1 System Development Request Form – ITG-2019-F-007-C

10.0 AUTHORIZED SIGNATORIES

No.	FORM	SCOPE	SIGNATORIES
10.1	CCTV Footage Request Form	Requested by Recommending Approval Approved by Attended by Noted by Report Acknowledgement	Requesting Team Immediate Superior Team Head ITG ITG Senior Officer Requesting Employee
10.2	CCTV Online Access Request Form	Requested by Noted by Approved by Received by Recommending Approval Approved by Request Acknowledged by	Requesting Employee Immediate Superior Team Head ITG Representative ITG Senior Officer ITG Team Head Requesting Employee
10.3	CCTV Confidentiality Agreement	Company Represented by the President Company Represented by the Data Privacy Officer Employee Witnesses	Team Head/President Data Privacy Officer Requesting Employee Representatives from ITG

11.0 SANCTIONS : Non-compliance on this policy shall be subject to sanction in accordance with the employee code of conduct.

12.0 EFFECTIVITY : This policy will take effect on June 1, 2023

13.0 ACKNOWLEDGEMENT TO COMPLY AND IMPLEMENT

This is to acknowledge that we:

13.1 Reviewed the policies and procedure herein;
13.2 Agree with contents hereof; and
13.3 Commit to strictly implement these policies and procedures.

ELMER M. CATANGAY
Finance and Services
Team Head

MICHAEL B. FRANCISCO
Collection and Recovery
Group Head

DAISY JANE C. CERTEZA
Treasury and ROPOA
Group Head

LEA A. STA. MARIA
Control and Securities
Group Head

CATHERINE PACUAN
Operations Management
Group Head

ROVIELYN P. NATIVIDAD
Data Analytics and Virtual Verification
Team Head