**Annex B**

**Agreement**

This Acceptable Use of Assets Policy Agreement ("Agreement") is an agreement between the bank, and the undersigned “individual”. The term “individual” may refer to an employee, a contractor, a consultant, temporary personnel and other workers of the bank, including all personnel affiliated with third parties, having the privilege to access, use, possess, process, etc. bank assets such as information, technology, devices and system.

I have read, understand, and will abide by the Acceptable Use of Assets Policy of Metrobank. I further understand that any violation of this policy is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, disciplinary action may be taken, and/or the appropriate legal action may be initiated by Metrobank. If I am an employee, the unauthorized use of such assets outside the Bank or for personal gains, either during or after employment is strictly prohibited. If I am a consultant or working for a service provider, aside from the foregoing, then any violation of the policy will be immediately deemed a breach of our principal agreement and may cause the termination of our principal agreement.

This agreement shall be governed by Philippine laws. The parties agree that all disputes arising from this Agreement shall be settled by the Philippine courts and venue shall be the appropriate courts of Makati City.

Unit :ITG

Individual Name :Kevin Isaac Cortez

Position Title :Programmer Analyst

Signature :

Date signed : July 23, 2020

Agency Provider : SLI Consultancy

Kevin Isaac Cortez

Signature over printed name

**ACCEPTABLE USE OF ASSETS POLICY**

**General**

1. All users authorized to access the Bank’s information, information systems and information processing facilities must comply with the required user responsibilities to maintain effective access controls that prevent unauthorized access, compromise of information systems and processing facilities or theft of information.
2. All confidential bank information assets must not be shared with unauthorized personnel such as but not limited to: unauthorized bank personnel, family or household members, non-bank personnel, non-unit personnel, etc.
3. All covered individuals must only use bank assets (information, technology, devices, etc.) to the extent necessary to fulfill their business and/or job responsibilities through authorized activities in accordance with bank policies, standards and procedures.

Computing resources

* 1. Computing systems used to conduct business for the bank must use authorized and currently supported standard operating system, database, application software or programs installed.
  2. All workstations (PC, laptop, etc.) must be secured by locking the screen when unattended.
  3. Bank owned computers and electronic storage devices must not be used to store pornographic materials, hacking tools and other non-work related materials.

Using Public Computing Resources

* 1. Access of bank systems and information using a public computer (e.g. internet cafe computers, etc.) is not allowed.
  2. Connection must be encrypted when authorized to use a wireless and/or public network (e.g., internet).

Personally Owned Devices

* 1. All personally owned computing systems and devices, authorized to conduct bank activities must follow the requirements to secure them as if it is bank owned. These security requirements include but are not limited to the following:
* Anti-virus and Anti-spyware
* Personal Firewall
* Intrusion Prevention/Detection
* Latest patches/security patches are installed
* Stored data encryption
* Remote wipe
* Password security

Electronic Mail

* 1. The bank’s electronic mail system is granted primarily for business purposes. Any personal use must not interfere with normal business activities. Sending unsolicited email messages, including sending of “junk mail” or other advertising materials (including creating or forwarding chain letters or other pyramid schemes of any type) to individuals who did not request for such material is strictly prohibited.
  2. Use the bank’s electronic mail system when sending bank information. Confidential information should not be communicated via text message or instant messenger.
  3. Use of personal email accounts is not allowed unless authorized and information encrypted.

Transmission/Storage of Information

* 1. Use appropriate security when transmitting or storing bank information electronically by encrypting confidential information.

Kevin Isaac Cortez

Signature over printed name

Internet

* 1. All authorized users must only use the internet to the extent necessary to fulfill their business and/or job responsibilities. It should not be used for personal activities such as but not limited to: gambling, buying/selling/auctioning goods or services, accessing non-work related sites or engaging or encouraging unlawful, threatening, offensive, or obscene activities.

**Illegal or Harmful Use**

1. All covered individuals are prohibited from revealing, sharing or using any bank confidential or restricted information, trade secrets or any other material considered as bank information when engaged in blogging or participating in discussions in social networking sites, conferences, seminars and the like. This includes but is not limited to the job title, bank official activities, bank operating information, etc.
2. Infringement of intellectual property rights or other proprietary rights including, without limitation, material protected by copyright, trademark, patent, trade secret or other intellectual property right.
   1. Distributing, installing, copying or using pirated or other software products that are not appropriately licensed for the use of the bank is strictly prohibited.
   2. Unauthorized copying of copyrighted material including but not limited to, digitization, distribution and/or posting of photographs from magazines, books or other copyrighted sources, logos, copyrighted music, videos and the installation of any copyrighted software for which the bank or the end user does not have an active license is strictly prohibited.
3. Authorized users shall not use bank assets to harass, threaten or send materials to others that might be deemed inappropriate, derogatory, prejudicial, or offensive.

**Network Security and Integrity**

1. Introduction of malicious programs (i.e., malware, Trojans, spyware, virus, worms, etc.) into the network or server is prohibited and is subject to sanctions if found intentional.
2. The authorized enabled USB/CD/DVD port/drive must not be used to install/copy unauthorized programs/files such as games, music and video files, etc. to bank-owned laptops/PCs/servers, and must not be used to connect non-bank issued USB-based devices such as camera, PDA, printer, modem, external storage and the like.
3. Port scanning or security scanning is expressly prohibited unless prior notification and approval from the Information Security Division is secured.
4. Effecting security breaches or disruptions of network communication or system operations is not allowed.
   1. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access.

Kevin Isaac Cortez

Signature over printed name

* 1. “Disruption” includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.



1. Executing any form of network monitoring which will intercept data, unless this activity is part of the employee’s normal job/duty, is strictly prohibited.
2. Circumventing user authentication or security of any host, network or account is strictly prohibited.
3. Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable or deny service to a user’s terminal session, via any means, locally or via the Internet/Intranet/Extranet is strictly prohibited.

**Enforcement of Policy**

1. All covered individuals understand and agree that the bank reserves the right to enforce and monitor compliance and subject violators to disciplinary action.
2. Indirect or attempted breaches of this policy, and actual or attempted breaches by a third party on behalf of a company, customer, or user, may be considered breaches of this policy by such company, customer or user.