DIRECTIVE ON INFORMATION TECHNOLOGY SECURITY FOR BANK PERSONNEL

June 14, 2018

A. Overriding Objective

1.1 This Directive establishes the rules and instructions for Bank Personnel with respect to Information Technology (IT) security of the Asian Infrastructure Investment Bank to protect AIIB against IT security threats, including the risk of espionage, to reduce the risks associated with such threats and to ensure the availability of effective and uncompromised IT systems across the Bank's administrative and operational functions.

1.2 The exercise and interpretation of this Directive shall seek to give effect to this overriding objective.

B. Related Provisions

This Directive relates to provisions of the Code of Conduct for Bank Personnel regarding IT security, namely:

> **15. Use of Bank Property, Services and Facilities.** Bank Personnel shall protect and preserve Bank property and assets and use such resources as efficiently as possible, guarding against waste and abuse, and protecting workplace health and safety. Bank Personnel may not use Bank services, supplies and facilities, except as permitted under the relevant Bank policy, and may not request other Bank Personnel members to carry out private tasks for themselves or their family.
>
> **16. Use of Bank Computer Systems, Devices and Internet Access.** Bank Personnel may use the Bank's computer systems, electronic devices and Internet access for personal use only if such use:
>
> - Does not interfere or conflict with the duties of Bank Personnel;
> - Is consistent with respect for laws under paragraph 18 below; and
> - Does not adversely reflect upon the integrity, public image or interests of the Bank.

C. General Principles

3.1 While protecting IT security, AIIB is committed to encouraging and maintaining an open and collaborative IT environment in which Bank Personnel can work efficiently and communicate freely.

3.2 Necessary IT security technical controls will be implemented to facilitate the efficient and appropriate implementation of this Directive.

D. Definitions

4.1 **Authentication Information:** Credentials used to prove an External Party or Bank Personnel is who they claim to be before accessing any IT Facilities, including via use of a password, passcode, digital certification, fingerprint, or similar.

4.2 **Bank Personnel:** As defined in the Code of Conduct for Bank Personnel.

4.3 **Business Unit:** As defined in the Directive on Business Continuity.

4.4 **BYOD**: Bring Your Own Device, a term that describes situations where Bank Personnel use their personally owned device such as phones, tablets, or laptops to access AIIB's information and applications.

4.5 **External Party:** Any entity, including any individual that may be working for an entity, that is not Bank Personnel.

4.6 **IT Facilities**: All hardware and software, including but not limited to networks, servers, applications, switches, cabling, computers, smartphones, tablets, storage media and devices (fixed, portable or removable) owned, leased, hired or licensed by or to AIIB.

4.7 **Malware**: A computer program that is maliciously placed onto a computer with the intent of compromising the privacy, accuracy, or reliability of the computer's data, applications, or operating system, such as a virus, worm, Trojan horse, or other code-based malicious entity.

4.8 **Remote Access**: The capability that allows a user to access AIIB's resources without being physically present on AIIB's premises.

4.9 **Restricted Data:** Data that contains information which is defined as Restricted Information under the Directive that establishes the Bank's security of information classification system.

4.10 **Shared ID**: A user identity used by more than one individual.

E. Computing and Storage Devices Use

5.1 Computing and storage devices include but are not limited to desktop computers, laptops, smartphones, tablets, printers, copy machines, optical media and removable storage devices.

5.2 When available, Bank Personnel shall only use AIIB-issued devices to conduct AIIB's functions. If a BYOD device needs to be used, Bank Personnel shall use the BYOD solution provided by AIIB to protect AIIB's information stored in the device. Whilst BYOD devices may belong to Bank Personnel, AIIB shall own all of AIIB's information and AIIB's applications residing in these devices.

5.3 Upon termination of employment with AIIB and when otherwise requested to do so, Bank Personnel shall return to the IT Division AIIB-issued devices. Whenever a device is no longer needed, Bank Personnel shall return it to the IT Division.

5.4 Bank Personnel shall secure all AIIB-issued and BYOD devices by using the standard screen lock function on these whenever they leave the device unattended.

5.5 When using removable storage media, including optical media and USB flash drives, Bank Personnel shall use encryption for files that contain Restricted Data.

5.6 Bank Personnel shall delete Restricted Data from their devices when the data is no longer required by them for official Bank purposes.

5.7 Bank Personnel shall not attempt to disassemble or modify the hardware of any IT Facilities. Bank Personnel shall not attempt to bypass, disable or diminish the effectiveness of the system or software of any IT Facilities.

5.8 Outside of AIIB Headquarters, Bank Personnel shall not leave any IT Facilities unattended without physical anti-theft measures, such as using a laptop security cable, placing them in a locked desk drawer, filing cabinet, safe or locked room.

F. Software Use and Malware Defense

6.1 When downloading software or any app onto AIIB's IT Facilities, Bank Personnel shall not knowingly download any pirated, corrupted or malicious software or app.

6.2 Bank Personnel shall comply with all applicable software licensing agreements and copyright restrictions.

6.3 Malware defense software installed by AIIB shall be activated at all times and shall not be tampered with, removed, suspended, disabled or functionally minimized by Bank Personnel.

6.4 Bank Personnel shall not attempt to change the security configuration of any IT Facilities. Bank Personnel shall enable security patches to update on a frequent basis.

6.5 Bank Personnel shall not use any removeable storage device, including USB flash drives, on AIIB IT Facilities if that device has previously been used on any other facility, including any BYOD device.

G. Network Use and Email Use

7.1 Only Bank Personnel authorized by the Manager, IT Division may monitor or test AIIB's network and systems. Bank Personnel who are not so authorized shall not try to attack, bypass or undermine AIIB's network and systems.

7.2 Bank Personnel shall not knowingly use AIIB's IT Facilities to visit any websites that would reflect adversely upon the integrity, public image or interests of AIIB, such as websites involving pornography, gambling, drug abuse and trafficking.

7.3 Bank Personnel shall not create any wireless network that connects to AIIB's network, and shall not modify wireless devices on AIIB's infrastructure, either technically or physically.

7.4 Bank Personnel shall choose the specified network category when connecting to AIIB's network, and shall not connect any unauthorized devices to AIIB's network.

7.5 When communicating or sharing Restricted Data over any network, Bank Personnel shall only use systems and tools that have been approved by the Manager, IT Division or the Vice President and Chief Administrative Officer (VP & CAO), and shall use encryption to protect the security of such data.

7.6 When accessing critical information or applications of AIIB from an external network, Bank Personnel shall use the Remote Access solution provided by AIIB.

7.7 Bank Personnel shall not create or provide any services over the Internet within AIIB's network without the prior approval of the Manager, IT Division.

7.8 Bank Personnel shall be vigilant to risks associated with email, including malware distribution, spam and social engineering.

7.9 Bank Personnel shall conduct AIIB-related functions over the AIIB email system and no other email. Bank Personnel may only use the AIIB's email system for personal use in an incidental manner and to an extent compatible with their official duties.

H. User Identification and Authentication

8.1 Bank Personnel shall use their unique user identification (user ID) provided by AIIB to access AIIB's IT Facilities. They shall not use user IDs and Authentication Information of other Bank Personnel, and shall not use any Shared ID.

8.2 Upon termination of employment with AIIB, user IDs and Authentication Information of Bank Personnel shall be disabled or removed by the IT Division.

8.3 Bank Personnel shall protect their user IDs and Authentication Information, and shall not share their Authentication Information with anyone.

8.4 Bank Personnel shall not circumvent or attempt to circumvent AIIB's authentication measures on any IT Facilities.

8.5 Bank Personnel shall create and protect passwords consistent with the password requirements specified in Administrative Guidance.

I. Rules for External Parties

9.1 External Parties who need to use AIIB's IT Facilities shall also comply with the rules of this Directive and its underlying Administrative Guidance through their incorporation by reference into their respective contracts.

9.2 External Parties shall not enable or facilitate access to AIIB's IT Facilities and Restricted Data, by any entity or body, including commercial, political, or state organizations of any country.

J. IT Security Incident Reporting

10.1 Bank Personnel shall report without unnecessary delay any observed or suspected IT security risks and incidents to the IT Division, and proactively provide reasonable assistance in incident-handling activities.

K. Roles and Responsibilities

11.1 **Bank Personnel** shall 1) not enable or facilitate access to AIIB's IT Facilities and Restricted Data, by any entity or body, including commercial, political, or state organizations of any country.
2) not knowingly be involved in any activity that may undermine, circumvent or breach the IT security of AIIB, 3) comply with this Directive and follow any related Administrative

Guidance, and 4) complete IT security trainings as required by AIIB.

11.2 **The Information Technology Division** shall 1) design and implement management measures and technical controls for IT security, 2) coordinate IT security incident handling activities and provide technical solutions, and 3) develop and implement IT security education and training programs.

L. Misconduct

A breach by Bank Personnel of the terms of this Directive may amount to misconduct under the Code of Conduct for Bank Personnel.

M. Implementation

The VP & CAO shall oversee this Directive and introduce any related Administrative Guidance and ensure their efficient and accurate implementation.

N. Authority

The VP & CAO shall make all final decisions regarding the application of this Directive.

*****