DIRECTIVE ON SECURITY AND SAFETY

Asian Infrastructure Investment Bank

April 28, 2020

Contents

PART 1: INTRODUCTION 3
PART 2: ACCOUNTABILITY 7
PART 3: APPLICABILITY 13
PART 4: TERMS OF REFERENCE OF FOCAL POINTS 15
PART 5: SECURITY OF BANK PREMISES 17
PART 6: SECURITY OF SPECIAL EVENTS 19
PART 7: TRAVEL SECURITY 23
PART 8: SECURITY AWARENESS 27
PART 9: SECURITY TRAINING 29
PART 10: SECURITY RISK MANAGEMENT 31
PART 11: FIRE SAFETY 37
PART 12: HOSTAGE INCIDENT MANAGEMENT 41
PART 13: SECURITY CRISIS MANAGEMENT 45
PART 14: SECURITY COMPLIANCE 49
PART 15: ARREST AND DETENTION 51
PART 16: SECURITY OF BANK ACTIVITIES 55
PART 17: HOST NATION RELATIONS 57
PART 18: ARMED PROTECTION 59

Parts 1 – 7 originally approved on April 5, 2018

Parts 8 – 17 originally approved on August 23, 2018

Part 18 approved on June 3, 2019

Amendments to Parts 1, 2, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 approved on April 28, 2020

Note: Color print required for page 35

[Intentionally blank]

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 1: INTRODUCTION

A. OVERRIDING OBJECTIVE

1.1 This Directive establishes rules and processes to ensure that safety, security and emergency response are undertaken by the Bank in a manner that supports the (a) continuity of operations and safeguards the reputation of the Bank, and (b) wellbeing of individuals while on the premises of the Bank, attending events arranged or hosted by the Bank, or while traveling on behalf of the Bank.

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

B. GENERAL PRINCIPLES

2.1 The lives of individuals are of paramount importance.

2.2 In supplementing the natural obligation of states to maintain order and protect persons and property within their jurisdiction, the Bank is responsible to implement a system to determine acceptable security and safety risk to Bank Personnel and all others at, or visiting, the Bank, or while traveling on behalf of the Bank; to provide adequate and sustainable resources to manage the risk to persons, assets, premises and operations; and, to develop and implement an appropriate security and safety legal framework towards this end.

C. NORMATIVE REFERENCE

3.1 The primary standard for the development of security and safety guidance in the Bank shall be the international standards ISO 31000 of 2009 Risk Management – Principles and Guidelines, and ISO 22300 of 2012 Societal Security – Terminology, and related standards.

D. STRUCTURE OF THE DIRECTIVE

4.1 This Directive is comprised of this introduction and other Parts (as listed in Appendix A). Each Part addresses a specific security or safety topic. Each Part, when read in conjunction with this Introduction and Part 2 (Accountability), carries the authority of a Directive. Parts shall be added to the Directive over time.

E. DEFINITIONS

5.1 “Bank Personnel” means as defined in the Code of Conduct for Bank Personnel”.

5.2 Key terms relating to security and safety are distinguished from each other as follows:

5.2.1 **“**Security” means management of risk to protect persons, assets and operations from the consequences of threats.

5.2.2 **"**Safety**"** means management of risk to protect persons, assets and operations from the consequences of hazards and technical failures.

5.2.3 **"**Threat**"** means a potential cause of harm initiated by deliberate and malicious actions.

5.2.4 **"**Hazard**"** means a potential cause of harm resulting from non-malicious actions or natural events. A hazard can involve a deliberate action but with no intent to harm.

5.2.5 **"**Risk**"** (in the context of safety and security) means the likelihood of a harmful event occurring and the impact of the event if it were to occur.

5.3 Definitions for other terms related to security and safety are within the relevant Parts of this Directive.

F. MISCONDUCT

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

G. IMPLEMENTATION

7.1 The Vice President and Chief Administration Officer (VP & CAO) shall oversee this Directive and introduce any related Administrative Guidance and ensure their efficient and accurate implementation.

H. AUTHORITY

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

*****

APPENDIX A

CONTENTS OF THE DIRECTIVE ON SECURITY AND SAFETY

Part	Topic
1	Introduction
2	Accountability
3	Applicability
4	Terms of Reference of Focal Points
5	Security of Bank Premises
6	Security of Special Events
7	Travel Security (includes aviation security arrangements)
8	Security Awareness
9	Security Training
10	Security Risk Management
11	Fire Safety
12	Hostage Incident Management
13	Security Crisis Management
14	Security Compliance
15	Arrest and Detention
16	Security of Bank Activities
17	Host Nation Relations (relevant to Security)
18	Armed Protection

[Intentionally blank]

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 2: ACCOUNTABILITY

A. OBJECTIVE OF THIS PART

1.1 This Part establishes the framework of accountability for security and safety in order to ensure that the protection of individuals, assets, premises and operations is addressed on every level of management within the Bank.

B. GENERAL PRINCIPLE

2.1 While the Bank accepts responsibility and accountability for security and safety management, fatalities and casualties may occur despite appropriate efforts and the implementation of measures to reduce to an acceptable level the risks to individuals and the Bank's assets, premises and operations.

C. DEFINITIONS

3.1 “Accountability” means the obligation of a member of Bank Personnel to be responsible, and to be held accountable, for the security and safety of other Bank Personnel and the assets and operations of the Bank.

3.2 “Business Unit” means a Vice-Presidency, Department or Division of the Bank, or discrete subcomponent thereof, as such term is defined in the Directive on Business Continuity.

D. OVERALL RESPONSIBILITY FOR SECURITY AND SAFETY

4.1 As stated in the Directive on Security and Safety (Part 1: Introduction), “in supplementing the natural obligation of states to maintain order and protect persons and property within their jurisdiction, the Bank is responsible to implement a system to determine acceptable security and safety risk to Bank Personnel and all others at, or visiting, the Bank, or while traveling on behalf of the Bank; to provide adequate and sustainable resources to manage the risk, as well as the risk to persons, assets, premises and operations; and, to develop and implement an appropriate security and safety legal framework towards this end”. This Part specifies the responsibilities and accountabilities of Bank Personnel for such implementation.

4.2 Besides this responsibility of the Bank, in the case of Bank premises in China, the Government of the People’s Republic of China holds a specific responsibility under Article 7 of the Headquarters Agreement between the Government and the Bank to “exercise due diligence to protect the Premises of the Bank against any intrusion or damage and to prevent any disturbance of the peace of the Bank or impairment of its dignity”.

E. INTERNAL RESPONSIBILITIES FOR SECURITY AND SAFETY

5.1 **The President**. Under Article 29, Paragraph 4, of the Articles of Agreement, the "President shall be the legal representative of the Bank. He shall be chief of staff of the Bank and shall conduct, under the direction of the Board of Directors, the current business of the Bank". The President is thus accountable to the Board of Directors for the proper running and administration of the Bank and shall include, in the context of this framework, the overall security and safety of the Bank.

5.2 **Vice President and Chief Administration Officer (VP & CAO)**. The VP & CAO reports, and is accountable, to the President. The President delegates to the VP & CAO the authority to make executive decisions relevant to the direction and control of the overall security and safety of individuals, assets, premises and operations of the Bank at headquarters and field locations. The VP & CAO represents the President on all security and safety-related matters. See Appendix A for more detailed responsibilities.

5.3 **Vice Presidents (VPs), the General Counsel, the Chief Risk Officer, the Chief Financial Officer and all Managing Directors (MDs), Directors General (DGs), Heads of Department and Officers that Report Directly to the President**. VPs, the General Counsel, the Chief Risk Officer, the Chief Financial Officer and all MDs, DGs, Heads of Department and Officers reporting directly to the President, shall be responsible and accountable to the President for ensuring that the overriding objective of security and safety within the Bank, namely to ensure that security and safety is undertaken by the Bank in a manner that ensures continuity of operations and safeguards the reputation of the Bank, while ensuring the wellbeing of individuals, is met within their respective Business Units. See Appendix A for more detailed responsibilities.

5.4 **Director General of the Facilities and Administration Services Department (DG FAS)**. At the discretion of the VP & CAO, specific decision-making authority as indicated in the various Parts to this Directive may be delegated to the DG FAS. Overall accountability for security and safety will continue to reside with the VP & CAO as indicated in Section 5.2.

5.5 **Officer Responsible for the Management of Security and Safety**. The officer to whom the responsibility for the management of security and safety is delegated by VP & CAO, and who reports to DG FAS, shall be responsible for the daily management of security and safety in and away from premises of the Bank; development of guidance for approval according to the Internal Legal Framework of the Bank; training of Bank Personnel and other relevant individuals in security and safety; and the provision of security and safety advice to management, other Bank Personnel and other relevant individuals. See Appendix A for more detailed responsibilities.

5.6 **Internal Security and Safety Focal Point Network**. Focal Points appointed by managers to represent their Business Units on the internal security and safety focal point network of the Bank shall be responsible for coordinating the Business Unit's input to the development of security and safety guidance in the Bank. See Appendix A for more detailed responsibilities.

5.7 **Security and Safety Personnel of the Bank**. Security and safety personnel of the Bank at whatever level or seniority shall be responsible and accountable for all matters pertaining to security and safety entrusted to them. These personnel are the first line of protection for Bank Personnel and other relevant individuals and shall ensure that the

responsibilities of the Bank with respect to security and safety are effectively and efficiently administered in the day-to-day security management activities of the Bank. See Appendix A for more detailed responsibilities.

5.8 **Bank Personnel**. Bank Personnel, regardless of their grade or level, shall abide by all security and safety Directives, Administrative Guidance, plans, procedures, instructions and security measures of the Bank. Bank Personnel shall also apply sound judgement to ensure that where specific guidance or instructions are absent, their actions or inaction does not compromise the security of the Bank, their own security and safety, and that of others. Security and safety is a shared responsibility beginning with all Bank Personnel. See Appendix A for more detailed responsibilities.

5.9 **Other Persons**. Any individual, other than Bank Personnel, with a direct contractual relationship with the Bank shall abide by all security and safety Directives, Administrative Guidance, plans, procedures, instructions and security measures of the Bank to the extent their contract with the Bank so requires. Failure to comply with such contractual obligations may result in contract termination by the Bank.

F. DETAILED ROLES AND RESPONSIBILITIES

6.1 The detailed roles and responsibilities indicated in Appendix A may be supplemented by additional responsibilities and tasks in the terms of reference and work plans of the incumbents.

*****

APPENDIX A

DETAILED ROLES AND RESPONSIBILITIES

A. BANK PERSONNEL

1.1 The responsibilities of Bank Personnel shall include:

1.1.1 Strict adherence to all security and safety Directives, Administrative Guidance, plans, procedures, instructions and security measures of the Bank.
1.1.2 Reporting of any breaches in security, suspicious activity, or safety violations and incidents observed by them promptly to security and safety officers.
1.1.3 Obtaining security clearance prior to traveling.
1.1.4 Attending security briefings when instructed.
1.1.5 Comporting themselves in a manner which will not endanger their security and safety, or that of others.
1.1.6 Attending and successfully completing required security and safety training relevant to their level and role.
1.1.7 Remaining alert and aware of their environment to detect any looming security or safety threats or hazards, and to take appropriate action which could include informing the relevant security and safety authority of the Bank.

B. ADDITIONAL RESPONSIBILITIES PER ROLE

2.1 **President**. Has overall responsibility and accountability for the security and safety of Bank Personnel, and the assets, premises and operations of the Bank at headquarters and field locations.

2.2 **The Vice President and Chief Administration Officer (VP & CAO)**. The responsibilities of the VP & CAO shall include:

2.2.1 Developing security guidance, practices and procedures for the Bank.
2.2.2 Coordinating with the Business Units of the Bank to ensure support for the implementation of, and compliance with, security and safety rules and procedures.
2.2.3 Preparing reports for the Executive Committee on all security and safety-related matters.
2.2.4 Advising the President and members of the Executive Committee on all matters related to security and safety of the Bank.
2.2.5 Further delegating the responsibility for the management of security and safety as required.
2.2.6 Directing the Bank's response to crisis as required.
2.2.7 Establishing, maintaining and furthering professional relationships in the field of security and safety with other international organizations, private companies or relevant professional associations.

2.3 **Vice Presidents (VPs), the General Counsel, the Chief Risk Officer, the Chief Financial Officer and all Managing Directors (MDs), Directors General (DGs), Heads of Department and Officers that Report Directly to the President**. The responsibilities of VPs,

the General Counsel, the Chief Risk Officer, the Chief Financial Officer and all MDs, DGs, Heads of Department and Officers reporting directly to the President, shall include:

2.3.1 Ensuring that security and safety considerations are included in the planning for any new operational or business initiative.
2.3.2 Supporting the development of a security and safety culture within their Business Unit that is consistent with this Directive.
2.3.3 Appointing a Focal Point to the security and safety focal point network of the Bank and supporting this person in the discharge of their duties.

2.4 **Director General of the Facilities and Administration Services Department (DG FAS)**. The responsibilities of DG FAS shall include:

2.4.1 Taking decisions regarding security and safety as delegated in the various Parts to this Directive by the VP & CAO.
2.4.2 Overseeing the functions and work of the officer responsible for the management of security and safety.

2.5 **Officer Responsible for the Management of Security and Safety**. The responsibilities of the officer responsible for the management of security and safety in the Bank shall include:

2.5.1 Advising the VP & CAO (directly or via the management chain as determined by the VP & CAO) on security and safety matters, and keeping the VP & CAO updated on security and safety management issues.
2.5.2 Liaising with local security authorities where applicable.
2.5.3 Assuring the security and safety of visitors to the Bank, including dignitaries.
2.5.4 Leading, directing and coordinating the work of the internal Security and Safety Focal Point Network.
2.5.5 Managing the security unit at headquarters, including all matters related to the management of security and safety personnel, operations, and logistics of the unit.
2.5.6 Managing security and safety systems and equipment of the Bank.
2.5.7 Managing the security and safety functions specified in the incumbent's terms of reference at headquarters and where applicable in the field, and for travel.
2.5.8 Overseeing the implementation of the Directive on Security and Safety and its associated Parts.
2.5.9 Drafting, and seeking approval for, security and safety procedures required to implement the Directive on Security and Safety, and any resultant Administrative Guidance.
2.5.10 Providing security and safety advice to any Business Unit in the Bank requiring such support.
2.5.11 Conducting security and safety risk assessments where necessary and designing appropriate prevention and mitigation measures.
2.5.12 Developing and delivering security and safety training programmes, or identifying suitable external vendors, to ensure that all Bank Personnel, individuals recognized by the Human Resources Department as dependants of Bank staff members if applicable, and other relevant individuals are adequately trained on security and safety related matters, including awareness.
2.5.13 Managing and directing the work of a 24-hour emergency control centre.

2.5.14 Assisting with the planning and security management of conferences and events of the Bank, at, and away from, headquarters.

2.5.15 Disseminating information, advisories and educational materials regarding security and safety matters.

2.5.16 If a security warden system is deemed necessary, maintaining up to date warden lists of Bank Personnel and individuals recognized by the Human Resources Department as dependants of Bank staff members if relevant. Appointing and coordinating the work of wardens.

2.5.17 Monitoring and reporting on compliance with security and safety rules, practices and procedures.

2.5.18 Acting as the Bank's representative in establishing professional relationships in the field of security and safety with other international organizations, private companies or relevant professional associations as delegated by the VP CAO pursuant to Section 2.2.7, and maintaining and furthering relationships already established.

2.6 **Internal Security and Safety Focal Point Network**. The responsibilities of the security and safety Focal Points of the Business Units shall include:

2.6.1 Ensuring that their Business Unit's interests are taken into consideration in the development of security and safety guidance.

2.6.2 Keeping their Business Units appraised of all new developments in security and safety.

2.6.3 Attending all meetings of the network personally, or represented by their alternate Focal Point, and providing required inputs and feedback on time and complete.

2.7 **Security and Safety Personnel of the Bank**. The responsibilities of Security and Safety personnel of the Bank shall include:

2.7.1 Performing all security and safety functions assigned to them efficiently and effectively.

2.7.2 Reporting any breaches in security, suspicious activity, or safety violations and incidents promptly.

2.7.3 Taking charge of any security or safety incident scene until further instructions are received.

2.7.4 Ensuring the protection of the Bank's assets and premises, and the security and safety of individuals while on the premises of the Bank, attending events arranged or hosted by the Bank, or while traveling on behalf of the Bank.

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 3: APPLICABILITY

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules for determining the categories of persons that benefit from the security and safety management system and arrangements of the Bank.

B. GENERAL PRINCIPLES

2.1 The applicability of security and safety arrangements extends to any location where business or operations of the Bank are conducted.

2.2 No distinction is made in this Part between those Bank Personnel that are globally and locally recruited.

C. DEFINITION

3.1 “Bank Personnel” means as defined in the Code of Conduct for Bank Personnel.

D. APPLICABILITY

4.1 Security and Safety Directives, Administrative Guidance, procedures, standards, instructions, measures and other arrangements of the Bank shall benefit individuals while on the premises of the Bank, attending events arranged or hosted by the Bank, or while traveling on behalf of the Bank, including but not limited to:

4.1.1 Bank Personnel.

4.1.2 Experts performing missions for the Bank.

4.1.3 Individuals on secondment to the Bank.

4.1.4 Interns to the Bank.

4.1.5 Any other individuals in direct contractual relationships with the Bank, other than Bank Personnel.

4.1.6 Members of the International Advisory Panel.

4.1.7 Individuals recognized by the Human Resources Department as dependants of Bank staff members.

4.1.8 Visitors.

*****

[Intentionally blank]

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 4: TERMS OF REFERENCE OF FOCAL POINTS

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules and processes to ensure that arrangements for security, safety and Business Continuity at the Bank are effectively consulted, and to facilitate joint development of common guidance for these topics.

B. GENERAL PRINCIPLES

2.1 Management on all levels shall be accountable for security, safety and Business Continuity and need therefore, to be represented in the development of guidance for these topics.

2.2 The development of guidance on all levels for security, safety and Business Continuity shall be undertaken in an inclusive and representative manner.

C. DEFINITIONS

3.1 “Focal Point” means anyone appointed by a manager or supervisor to represent the relevant Business Unit on all matters relating to security, safety and Business Continuity.

8.2 “Business Continuity” is as defined in the Directive on Business Continuity as the capability of the Bank to continue delivery of services or operations at acceptable predefined levels following a disruption.
3.2 .

3.3 “Business Unit” means a Vice-Presidency, Department or Division of the Bank, or discrete subcomponent thereof, as such term is defined in the Directive on Business Continuity.

D. APPOINTMENT OF FOCAL POINTS

4.1 A network of Focal Points representing individual Business Units shall be utilized to achieve the objective of this Part. By default a single network covering security, safety and Business Continuity shall be established, or at the discretion of the Director General of the Facilities and Administration Services Department (DG FAS) separate networks may be established for security and safety on the one hand, and Business Continuity on the other. Vice Presidents, the General Counsel, the Chief Risk Officer, the Chief Financial Officer and all Managing Directors, Directors General, Heads of Department and Officers that report directly to the President, shall each appoint at least one Focal Point, and at least one alternate, to represent their Business Units in accordance with this Part.

4.2 Focal Points should have broad knowledge of the work of the Business Units and the ability to make meaningful contributions to joint discussions and products.

4.3 Focal Points shall serve until a replacement has been appointed.

E. DUTIES AND RESPONSIBILITIES

5.1 Duties and responsibilities of Focal Points shall include, but not be limited to:

5.1.1 Attendance of all Focal Point meetings, either personally or by the designated alternate, or both.

5.1.2 Accurately reflect the point of view and needs of their Business Units on the topics of security, safety and Business Continuity.

5.1.3 Keep their Business Unit apprised of all developments with regard to these topics.

5.1.4 Act as interface for their Business Unit with FAS with regard to these topics.

5.1.5 Complete assigned tasks according to schedules as determined by the coordinating officer(s).

5.1.6 Inform the coordinating officer(s) of any changes to the Focal Point(s) of their Business Unit and arrange with the head of their respective Business Unit for a replacement Focal Point(s) should the incumbent(s) no longer be available.

F. COORDINATION OF THE FOCAL POINT NETWORK(S)

6.1 DG FAS shall appoint an officer(s) to coordinate the Focal Point network(s). Either one officer shall be appointed for the security and safety topic, and one for the Business Continuity topic, or a single officer for both.

6.2 The coordinating officer(s) shall be responsible for coordinating all activities of the network(s) to include determination of an appropriate name for the network(s), development of an online presence for the network(s), arrangement of meetings, setting of meeting schedules, setting of agendas, determination of work plans, collation of inputs from the Business Units, maintaining of records, and reporting to DG FAS on all matters pertaining to the network(s).

*****

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 5: SECURITY OF BANK PREMISES

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules and processes for determining the measures, arrangements and basic principles for security, and where relevant, safety, of Bank Premises.

B. GENERAL PRINCIPLES

2.1 As stated in the Directive on Security and Safety, Part 2, "in the case of Bank premises in China, the Government of the People's Republic of China holds a specific responsibility under Article 7 of the Headquarters Agreement between the Government and the Bank to exercise due diligence to protect the Premises of the Bank against any intrusion or damage and to prevent any disturbance of the peace of the Bank or impairment if its dignity".

2.2 The Bank is responsible for the security and safety of all persons while at Bank Premises.

2.3 This Part only covers the security aspects of premises management, including fire safety and not occupational safety or health matters, nor safety aspects relating to premises design, construction, technical assessment, refurbishment and management, related to the risk inherent in natural hazards.

C. DEFINITIONS

3.1 "Bank Premises" means all physical locations owned or leased by the Bank, or otherwise provided to the Bank by a Member, for the exclusive use of the Bank and where Bank Personnel are physically present, and the premises are used in furtherance of the Bank's functions. This definition is without prejudice to the same term as used in the Articles of Agreement.

3.2 "Exclusive use" means both where the Bank occupies the entire premises, or the portion occupied by the Bank where Premises are shared.

D. ARRANGEMENTS FOR SECURITY OF BANK PREMISES

4.1 Security of Bank Premises shall be grounded on the implementation of the following:

4.1.1 Implementation of a **Security Risk Management (SRM) approach** as specified in the Directive on Security and Safety, Part 10, to determine appropriate situation-specific security procedures and measures for premises security and safety. Security and safety personnel of the Bank shall work in close collaboration with host Government, facilities managers and other relevant parties in the application of the SRM process.

4.1.2 Implementation of an **integrated systems approach** to design and management that focuses on the total system, rather than on the individual components of the system. This shall be done to ensure that the physical, procedural, technical and human aspects of security are integrated, creating self-reinforcing protection of Bank Premises. The integrated systems approach shall also be coordinated with areas of responsibility of the host Government outside of Bank Premises.

4.1.3 Application of the **"Four Ds"** (Deter, Detect, Delay and Deny) concept of security design through which potential perpetrators will be deterred from attempting to attack Bank Premises; detected, if they should still choose to do so; delayed in achieving their objective so that reaction elements can be mobilized to counter the attack; and, denied access by ensuring effective protection measures.

4.1.4 Application of **concentric layers** of security to ensure that Bank Premises are protected with sufficient diversity and redundancy so that the strength of one particular component offsets the weakness of another. Components of the security system shall be designed in a sufficient number of layers to make it more difficult to defeat the whole system. All Bank Premises shall require at least two physical layers of security between Bank Personnel or valuable assets on the one hand, and the external areas (the areas beyond direct Bank control) on the other, including a system to only allow authorized persons, vehicles and other items to cross these layers. Security and safety personnel of the Bank shall coordinate the application of this concept with the host government to ensure that security of the areas outside of Bank Premises form part of the total security plan.

E. IDENTIFICATION AND SCREENING

5.1 Positive identity verification of persons entering Bank Premises shall be performed by security and safety personnel of the Bank, and may include the use of biometric systems, facial recognition and other means, including questioning.

5.2 Security screening of persons, bags and goods shall be performed by security and safety personnel of the Bank and may include physical screening through the use of X-Ray, metal detection or biological and chemical detection systems, as well as visual inspection and frisking, or a combination of these methods.

F. ACCESS BY EXTERNAL SECURITY PERSONNEL

6.1 Armed or unarmed security personnel of any government shall only be permitted to enter Bank Premises in accordance with Article 6(2) of the Headquarters Agreement.

6.2 Armed or unarmed personnel of private security service providers shall not be permitted to enter Bank Premises unless the service provider is providing the service pursuant to a contract it has with the Bank.

*****

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 6: SECURITY OF SPECIAL EVENTS

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules and processes for determining the measures and arrangements for security of Special Events arranged by the Bank.

B. GENERAL PRINCIPLES

2.1 Special Events arranged by the Bank fall under the overall security and safety responsibilities of the Bank, notwithstanding the natural obligation of the Host Government to maintain order and protect persons in whose jurisdiction the event is being held.

2.2 The detailed responsibilities of parties with regard to security and safety shall be agreed in advance of the Special Event through a Memorandum of Understanding (MOU), or similar instrument, and operationalized through a jointly agreed security plan.

2.3 Where the Bank is co-hosting a Special Event, the Bank shall endeavour to apply the spirit of this Part during joint planning.

2.4 This Part does not apply to events in which the Bank participates but has no Hosting role. In those cases, normal security measures for Bank Personnel shall apply.

C. DEFINITIONS

3.1 "Special Event" means any event, conference or meeting arranged, sponsored or organized by the Bank that meets both of the following criteria:

3.1.1 Participants include (a) Bank Personnel, a member or alternate member of the Board of Governors, a member or alternate member of the Board of Directors, a representative of an AIIB member and (b) a third party.

3.1.2 The Bank has concluded, or intends to conclude, a legal agreement of any nature with the Host Government where the Special Event is to take place.

3.2 "Location" means the place where the Special Event will occur within any country.

3.3 "Convener" means the Business Unit, as such term is defined in the Directive on Business Continuity, which hosts or arranges the Special Event.

D. PLANNING FOR SPECIAL EVENTS

4.1 The Convener shall notify the Director General of the Facilities and Administration Services Department (DG FAS) of the need for security support once the preferred Location and dates for a Special Event have been determined. DG FAS shall assign a Security Focal

Point (SFP) who shall act as liaison with the Convener for the planning phase and, if necessary, for support during the Special Event itself. The SFP shall coordinate the Bank's security requirements with the Convener, Host Government, or third parties.

4.2 The Convener shall ensure that all applicable security-related legal documents and agreements are established with the relevant Government authority at the Location and request the appointment of a security liaison officer from the relevant Host Government.

4.3 The Bank may opt to request security advisory support from third parties such as other Multilateral Development Banks (MDBs), or any other party. This shall be coordinated by DG FAS.

4.4 The Convener shall be responsible for all costs associated with security not covered by the Host Government at the Location, including travel costs for the assigned SFP.

4.5 To the extent that a Business Unit hosts a Special Event but has not succeeded in concluding an agreement with a Host Government, this Part 6 shall not apply and the assigned SFP shall be responsible for all security arrangements in collaboration with the Business Unit. The Business Unit shall remain responsible for all security costs.

E. RISK ASSESSMENT

5.1 The assigned SFP shall complete a security risk assessment for the proposed Special Event and venue, either independently, or in collaboration with the Host Government, and make recommendations on the security risk management measures needed to bring the residual security risks to the Special Event to acceptable levels. Even if undertaken independently, the security risk assessment shall be coordinated with the Host Government.

5.2 Special Events shall only be held when the risk assessment indicates that risks associated with the planned Location and dates can be mitigated to acceptable levels.

5.3 The security plan shall include measures to mitigate risks to acceptable levels for the venue itself and any other Location to be used during the Special Event; accommodation of delegates; access control; travel and transportation to and from the venue; visitor management; and, screening of workers, deliveries and the media.

F. ROLES AND RESPONSIBILITIES

6.1 **The Convener**. Shall be responsible for:

6.1.1 Arranging any required legal agreements and documents with respect to security arrangements with the Host Government;

6.1.2 arranging with the Host Government for the appointment of a liaison officer to work with the Bank's assigned SFP for the Special Event; and

6.1.3 covering all security costs associated with the Special Event that are not covered by the Host Government, including travel costs of the assigned SFP.

6.2 **DG FAS**. Shall be responsible for:

6.2.1 Security coordination of the Special Event from the Bank's side in collaboration with the representative of the Convener, the Host Government, or third parties. To this end, DG FAS shall assign a SFP to support the Convener for security coordination of the Special Event.

6.2.2 Requesting security advisory support from any third party if required.

6.3 **Security Focal Point for the Special Event (SFP)**. Shall be responsible for:

6.3.1 Coordinating all security related matters with the Convener, the Host Government security liaison officer, internal or outsourced security personnel of the Bank, and third parties.

6.3.2 Developing, in collaboration with the Host Government, the security risk assessment for the Special Event.

6.3.3 Developing, in collaboration with the Host Government, the security plan including measures to minimise risk.

6.3.4 Accompanying the representative of the Convener on any preliminary scoping missions, and to the Special Event itself.

6.3.5 Preparing a security debrief report on conclusion of the Special Event, indicating lessons learned and identifying possible best practice.

*****

[Intentionally blank]

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 7: TRAVEL SECURITY

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules and processes for determining the measures and arrangements for travel security applicable to individuals traveling in their official capacity on behalf of the Bank (Travelers).

B. GENERAL PRINCIPLES

2.1 Travel Security Clearance shall be required for all Official Travel with the exception of Official Travel when the mission destination is Beijing. However, during times when Beijing itself is subject to security or safety restrictions or risks, including medical risks, Travel Security Clearance shall be required for Official Travel to Beijing. This exception shall be handled on a case-by-case basis and may involve security administrative arrangements different from the established travel administration arrangements in place.

2.2 Where travel is undertaken with, or under the leadership of, implementing partners or other parties, security measures and arrangements shall not be less stringent than those normally applicable to Travelers for the same location.

2.3 This Directive does not apply to medical evacuation, or private travel. Bank Personnel are encouraged to apply basic security awareness and good judgement when undertaking private travel.

2.4 At the discretion of the Vice President and Chief Administration Officer (VP & CAO), the decision-making authority for exceptions and emergency decisions relating to this Part, with the exception of Section 5.1.3, may be delegated to the Director General of the Facilities and Administration Department (DG FAS).

C. DEFINITIONS

3.1 “Official Travel (OT)” means travel on behalf of the Bank approved in accordance with the Directive on Official Travel.

3.2 “Traveler” means as defined in the Directive on Official Travel.

3.3 “Travel Security Clearance (TSC)” means the security approval process for OT through which permission for the travel to a specific destination is granted from the point of view of security only, and does not imply authority to undertake the mission involved in the travel. Permission to undertake the mission itself shall be obtained from the Traveler’s Travel Approving Authority (TAA) in accordance with the Directive on Official Travel.

3.4 “Security Measures” means any security prevention or mitigation measures and arrangements specified for a specific destination, circumstance, purpose or time frame.

3.5 “Donated Flights” means flights provided at no financial cost to the Bank, including the use of publicly-owned (i.e. State, government, military) or privately-owned (i.e. corporate, personal) aircraft.

3.6 “High Risk” means a level of security Risk that the Bank may apply to a given jurisdiction in accordance with the Directive on Security and Safety (Part 10: Security Risk Management).

D. GENERIC SECURITY MEASURES FOR TRAVEL

4.1 Travelers shall obtain a TSC for the specific destination before committing Bank funds for tickets or other travel costs. This provision shall not apply for OT when the mission destination is Beijing except as provided in Section 2.1.

4.2 DG FAS shall ensure that all OT is registered with the service provider(s) contracted to manage travel medical and security matters on behalf of the Bank.

4.3 Travelers shall ensure that they are familiar with the security advisories in place for the destination as provided by (a) the officer responsible for overseeing travel security at FAS, and (b) any third-party provider contracted by the Bank for this purpose.

4.4 Travelers shall complete the required training as specified in the Directive on Security and Safety (Part 9: Security Training) prior to the granting of TSC.

4.5 Travelers shall adhere to all Security Measures that have been specified for the destination or event to which the Traveler is traveling, irrespective of whether these Security Measures have been set by the Bank, or arranged or coordinated with third parties.

E. ADDITIONAL MEASURES FOR AIR TRAVEL

5.1 The officer responsible for overseeing travel security at FAS shall be responsible for the provision of air travel-related security advice. In addition, the VP & CAO or their delegated authority shall implement a process whereby air carriers are certified for use by the Bank and shall formalize this process in Administrative Guidance. The officer responsible for overseeing travel security at FAS shall employ this process to certify air carriers according to one of the classifications below:

5.1.1 **Unrestricted Use**: Air carriers classified for Unrestricted Use may be used for OT with no restrictions.

5.1.2 **Conditional Use**: Air carriers classified for Conditional Use shall only be used for OT when an Unrestricted Use air carrier is unavailable. Decisions on the use of these air carriers shall be taken on a case-by-case basis in accordance with Administrative Guidance.

5.1.3 **Restricted Use**: Where OT is urgent and no Unrestricted Use or Conditional Use air carrier is available, the following may be used in exceptional cases: (a) air carriers classified for Restricted Use, and (b) chartered flights by non-commercial air carriers. In these cases, a risk assessment shall be undertaken by the officer responsible for overseeing travel security at FAS, utilizing information and data

obtained from any available sources, including other multilateral development banks. Final decisions on the use of these air carriers shall be taken by the VP & CAO based on this risk assessment.

5.2 Restrictions on the use of air carriers may be waived during crisis situations or emergencies at the discretion of the VP & CAO or their delegated authority.

5.3 **Donated Flights**. VP & CAO or their delegated authority shall approve the use of donated flights. These officers shall determine if a risk assessment, to be undertaken by the officer responsible for overseeing travel security at FAS, is required.

F. TRAVEL SECURITY CLEARANCE

6.1 **Requirement for Travel Security Clearance**. TSC procedures shall:

6.1.1 Ensure that all OT is undertaken within an environment of acceptable risk;

6.1.2 Provide important security information to Travelers, and,

6.1.3 Assist with locating all Travelers that are registered with the service provider(s) contracted to manage travel, medical and security matters on behalf of the Bank, in order to provide them with security information and advice in the event of a crisis or emergency at the location to which they have traveled, or in extreme cases, to assist with their rescue or evacuation.

6.2 TSC shall be required irrespective of the mode of transport being utilized for OT.

6.3 TSC shall be required for all Travelers. Application for a single TSC for all Travelers in a group may be submitted if deemed more convenient by persons arranging OT.

6.4 **Granting of Travel Security Clearance**. TSC, for an individual or a group, shall be granted on condition that the officer responsible for overseeing travel security at FAS has assessed that the travel can be undertaken in an environment of acceptable security risk. That assessment may include the implementation of additional security measures to be arranged either by FAS or the Traveler.

6.5 If the security situation deteriorates after clearance has been granted, the Traveler shall be advised by the officer responsible for overseeing travel security in FAS whether the clearance will be rescinded, if travel can take place as initially authorized or if travel will now only be authorized if certain, additional security measures are implemented.

6.6 Where a Traveler disagrees with an assessment of risk, the assessment shall be escalated to DG FAS for consideration. If the decision of DG FAS is not acceptable to the Traveler, the VP & CAO shall take the final decision.

6.7 Travel Approving Authorities authorizing missions to jurisdictions assessed as High Risk shall carefully consider the criticality of such missions as travel to these areas may be hazardous to Travelers.

6.8 Where a Traveler will travel to a destination assessed as High Risk, restrictions may be placed on the selection of accommodation at the destination. The VP & CAO shall

implement a process for the clearing of accommodation based on security considerations. Travelers shall only make use of accommodation cleared for OT use under these circumstances. The rules in this paragraph prevail over more general rules on accommodation that are present in the Directive on Official Travel.

6.9 The Traveler shall provide to the officer responsible for overseeing travel security at FAS a valid certificate of completion of the training required for the destination, as specified in the Directive on Security and Safety (Part 9: Security Training). TSC shall not be granted unless the Traveler, and all Travelers in a group, have provided proof of completion of the training.

G. TRAVEL TICKETING

7.1 The Travel Contractor shall only issue travel tickets on receipt of a valid TSC for an individual or a group, except when the mission destination is Beijing.

7.2 The Travel Contractor shall make reservations only on Unrestricted Use air carriers unless authorization for travel on Conditional Use or Restricted Use carriers has been approved in accordance with this Part.

H. GROUP TRAVEL OF SENIOR PERSONNEL

8.1 Bank Personnel arranging travel of the President, Members of the Executive Committee, Managing Directors and Directors General, shall endeavor to avoid all members travelling on the same aircraft, ship, train, bus or other means of transport. As a general rule, no more than two-thirds of any such senior group shall travel on the same aircraft, ship, train, bus or other mode of transport. Where this is deemed not possible or feasible, the VP & CAO or their delegated authority shall take the final decision. In doing so, the VP & CAO or their delegated authority shall apply sound judgement, which, at their request, may be supported by a risk assessment provided by the officer responsible for travel security at FAS.

I. ROLES AND RESPONSIBILITIES

9.1 **VP & CAO**. The VP & CAO shall authorise flights on Restricted Use air carriers, and for donated flights; waive restrictions during crisis situations or emergencies; issue Administrative Guidance on the booking of flights, issuance of travel tickets, and the TSC process; take final decisions on TSC where the denial of clearance is disputed by a Traveler after an initial decision by DG FAS; and, where required, take final decisions on the number of senior staff permitted to travel on the same aircraft, ship, train, bus or other means of transport. These responsibilities, with the exception of Section 5.1.3, may be delegated in accordance with Section 2.4.

9.2 **DG FAS**. DG FAS shall authorize the use of Conditional Use air carriers and take decisions on TSC where the denial of clearance is disputed by a Traveler.

9.3 **Officer Responsible for Overseeing Travel Security**. The officer responsible for overseeing travel security shall advise the VP & CAO, DG FAS, and the Travel Contractor on the Air and Travel Security Directive in general; provide a list of Extreme Risk and High Risk jurisdictions; classify air carriers; issue TSC; and undertake risk assessments as required.

*****

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 8: SECURITY AWARENESS

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules and processes for ensuring that personal and corporate security is enhanced through the development of a general attitude and culture of security awareness.

B. GENERAL PRINCIPLES

2.1 Sound security is the product not only of good security management and guidance, but also of individual contributions at every level in the Bank.

2.2 Corporate and personal security culture and attitude, enhanced with knowledge and information on the security threat environment, can be described as security awareness and provides protection, even in the absence of formal security measures and arrangements.

C. MEASURES TO ENHANCE SECURITY AWARENESS

3.1 The Vice President and Chief Administration Officer (VP & CAO) shall develop and implement a program of mandatory security training designed to enhance the security awareness and knowledge of all Bank Personnel, as such term is defined in the Code of Conduct for Bank Personnel. This responsibility shall be planned and managed by the officer responsible for the management of security and safety as delegated in the Directive on Security and Safety (Part 2: Accountability).

3.2 The officer responsible for the management of security and safety shall periodically issue bulletins or advisories and arrange briefings on security topics to impart knowledge and create security awareness and understanding of security issues amongst Bank Personnel and others required to receive such information.

3.3 The officer responsible for the management of security and safety shall ensure that all Travelers, as defined in the Directive on Security and Safety (Part 7: Travel Security), are provided with security briefing materials relating to any destination to which they are traveling. This officer shall also make arrangements that in the event that a security incident occurs at, or near, any such destination, Travelers are provided with security advisories in a timely manner.

3.4 The officer responsible for the management of security and safety shall ensure that a dedicated page for security is maintained on the Bank's intranet and shall regularly provide materials to enhance security awareness through this means.

3.5 The officer responsible for the management of security and safety shall enhance Bank-wide security contact through the maintenance of the Focal Point network defined in the

Directive on Security and Safety (Part 2: Framework of Accountability and Part 4: Terms of Reference of Focal Points).

*****

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 9: SECURITY TRAINING

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules and processes for security training in the Bank.

B. GENERAL PRINCIPLES

2.1 Training is a fundamental requirement to address the security culture of the Bank through enhancing security awareness as described in the Directive on Security and Safety (Part 8: Security Awareness) and thereby contribute to the protection of Bank Personnel, as such term is defined in the Code of Conduct for Bank Personnel, and of the Bank itself.

2.2 Security training provides Bank Personnel with the ability to make sound decisions in the absence of direct security guidance or instructions, and in doing so select appropriate courses of action to protect themselves, others, and the Bank.

2.3 Security training is a cost-effective measure to lower risks and to provide Bank Personnel with the means to fulfil their security responsibilities under the Directive on Security and Safety (Part 2: Accountability).

C. TARGET GROUPS FOR TRAINING

3.1 Security training shall be developed to enhance skills and knowledge of:

3.1.1 Security and safety personnel as such term is used in the Directive on Security and Safety (Part 2: Accountability);

3.1.2 Security Focal Points as such term is used in the Directive on Security and Safety (Part 2: Accountability);

3.1.3 Bank Personnel;

3.1.4 Recognized dependants of Bank staff members where appropriate, understanding that participating in such training is voluntary; and

3.1.5 Other persons, including members of the Board of Directors, who may benefit from this training.

3.2 Security training applicable to their role shall be mandatory for Bank Personnel, experts performing missions for the Bank, individuals on secondment to the Bank, interns to the Bank, and any other individuals, other than Bank Personnel, in direct contractual relationships with the Bank.

D. SECURITY TRAINING TOPICS

4.1 The officer responsible for the management of security and safety shall select applicable security training topics and determine which topics are mandatory for persons fulfilling different roles and functions and shall determine the frequency of refresher training required by these persons.

4.2 Topics shall include, but may not be limited to, provisions for general security awareness, travel security, security requirements for high risk locations, and specific security threats and risks as appropriate.

E. METHOD OF DELIVERY

5.1 The officer responsible for the management of security and safety shall determine the appropriate methods of delivery of security training programs, including the option of outsourcing such programs.

*****

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 10: SECURITY RISK MANAGEMENT

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules and processes with respect to Security Risk Management (SRM) for all activities in furtherance of the Bank's purpose and functions at any location where such activities take place.

1.2 This Part does not apply to Information Technology security.

B. GENERAL PRINCIPLES

2.1 The purpose of SRM is to enable activities in furtherance of the Bank's purpose and functions notwithstanding the presence of Threats, as defined in the Directive on Security and Safety (Part 1: Introduction) within the operating environment of such activities.

2.2 While SRM cannot eliminate Risk, as such term is defined in the Directive on Security and Safety (Part 1: Introduction), it facilitates valid, context-specific, and timely management decisions to ensure that activities are conducted within an acceptable level of Risk.

C. DEFINITIONS

3.1 "Acceptable Risk" means that, after careful analysis, the potential benefits to be achieved by an activity outweigh the assessed Projected or Residual Risk to individuals, assets or activities.

3.2 "Impact" means a rating of the assessed potential harm that an event would have if it were to occur.

3.3 "Likelihood" means a rating of the assessed potential for a harmful event to occur.

3.4 "Present Risk" means the Risk currently assessed based on the identified Threats, taking existing security measures and procedures into consideration.

3.5 "Projected Risk" means the expected Risk if recommended security measures and procedures were to be in place.

3.6 "Residual Risk" means the Risk remaining after approved security measures and procedures have been implemented.

3.7 "Risk Rating" means a rating of the Risk based on an assessment of the Likelihood and Impact of the event occurring, as further specified in Appendix A.

3.8 "Security Risk Assessment" (SRA) means the methodology whereby security Risk is assessed through the identification of Threats, determination of Vulnerability, and the

assessment of the Likelihood and Impact of the Threat. While an SRA is primarily aimed at assessing Risk associated with Threats, the same methodology can be applied to assessing the Risk associated with Hazards, as such term is defined in the Directive on Security and Safety (Part 1: Introduction), and for the purposes of Business Continuity planning.

3.9 "Security Risk Management" (SRM) means the systematic determination and implementation of timely and effective approaches for managing Risk.

3.10 "Vulnerability" means a weakness in the security profile of the Bank that can allow a Threat to cause harm.

D. SRM MODEL

4.1 The Vice President and Chief Administration Officer (VP & CAO) shall put in place an SRM model to enable Bank activities to be performed notwithstanding the presence of Risk.

4.2 The systematic application of the SRM model shall empower the user to (i) identify potential Threats to a given activity, (ii) assess the Likelihood of such Threats affecting the activity and their potential Impact, (iii) determine the level of Present Risk, (iv) identify an appropriate security response to enable the activity to take place within acceptable levels of Projected and Residual Risk, and (v) provide advice on the implementation of such a response.

4.3 The SRM process shall address Risk through one, or a combination, of the following key strategies: controlling, avoiding, transferring and accepting Risk.

4.3.1 Where possible, Risk shall be avoided by altering the location or timing of an activity.

4.3.2 If feasible, Risk shall be controlled through prevention measures (lowering the Likelihood) and mitigation measures (lowering the Impact).

4.3.3 If not possible to control or avoid Risk, it shall be transferred by the use of implementing partners thereby removing individuals covered by this Part from the effects of the Risk.

4.3.4 If not possible to control, avoid or transfer Risk, a decision in accordance with Section G shall be required to determine if the Risk is acceptable or not.

4.4 The VP & CAO shall put in place a methodology to implement the SRM model.

E. RESPONSIBILITY FOR SRM

5.1 Specific responsibility to apply the SRM model, and the SRA process in order to assess the level of Risk involved with an activity shall reside with the officer responsible for the management of security and safety.

5.2 All individuals planning an activity under the Directive on Security and Safety (Part 6: Security of Special Events or Part 16: Security of Bank Activities), or any operational activity where there is a reasonable expectation of Risk, or where actual Risk is identified, shall consult

with the officer responsible for the management of security and safety who shall apply the SRM model.

F. CRITICALITY OF ACTIVITIES

6.1 The SRA process determines a Risk Rating and does not assess the importance of implementing an activity in furtherance of the Bank's purpose and functions. The VP & CAO, and the officer responsible for the management of security and safety, shall not be responsible for determining the criticality of any such activity. Such responsibility resides with the Bank Personnel approving the implementation of a given activity.

6.2 Risk Ratings of High, Very High and Unacceptable (or "Extreme" when referring to travel Risk) reflect at least a reasonable probability that Travelers may sustain non-life threatening, severe or critical injuries or may be killed in the implementation of a given activity. Therefore, an individual approving the implementation of a given activity shall carefully consider the potential benefits of the activity under such conditions versus the potential negative impact on those implementing the activity.

G. DECISION-MAKING FOR RISK ACCEPTANCE

7.1 In reaching a decision to accept Risk, the following shall apply:

7.1.1 No unnecessary Risk shall be accepted.

7.1.2 All reasonable steps shall have been taken to prevent or mitigate the Risk.

7.1.3 The decision to proceed with an activity where the Projected or Residual Risk is assessed as Unacceptable shall be taken by the President. In an emergency situation where the President is unavailable to take the decision to accept the Risk, this decision shall be taken by the VP & CAO. In the absence of the VP & CAO, the decision shall be taken by any other Vice President.

7.1.4 The decision to proceed with an activity where the Projected or Residual Risk is assessed as lower than Unacceptable shall be taken jointly by the individual authorizing the activity for which the Risk has been assessed and the officer responsible for the management of security and safety. This officer shall determine the prevention and mitigating measures required for the activity to proceed and the individual responsible to authorize the activity shall acknowledge this assessment and determine if the benefits of the activity outweigh the Risk according to Section F. The officer responsible for the management of security and safety shall implement a mechanism to facilitate this joint decision making.

7.1.5 The VP & CAO shall determine under what circumstances the process described in section 7.1.4 may be waived or delegated, or may delegate the responsibility to determine these circumstances to the officer responsible for the management of security and safety.

7.1.6 In situations where a Traveler applying for Travel Security Clearance in accordance with the Directive on Security and Safety (Part 7: Travel Security)

appeals an assessment of Risk by the officer responsible for overseeing travel security at FAS as Unacceptable, the appeal mechanism specified in Part 7 shall not apply, and only the President shall take the decision to authorize the travel or not.

*****

Appendix A

Security Risk Rating Matrix

(following the United Nations Security Management System risk rating scale)

Risk Matrix		Impact				
		Negligible	Minor	Moderate	Severe	Critical
LIKELIHOOD	Very Likely	Low	Medium	High	Very High	Unacceptable
	Likely	Low	Medium	High	High	Very High
	Moderately Likely	Low	Low	Medium	High	High
	Unlikely	Low	Low	Low	Medium	Medium
	Very Unlikely	Low	Low	Low	Low	Low

LIKELIHOOD DESCRIPTORS:

Very Likely: Is considered imminent or has a very high probability of occurring.

Likely: Has a high probability of occurring.

Moderately Likely: Has a reasonable probability of occurring.

Unlikely: Has a reasonable probability of NOT occurring.

Very Unlikely: Is considered unrealistic or to have a high probability of NOT occurring.

IMPACT DESCRIPTORS:

Critical: Death and critical injuries to personnel; cessation of program activities; major or total loss

Severe: Severe injuries to personnel; severe program disruptions; significant damage and/or loss

Moderate: Non-life-threatening injuries/high stress to personnel; program delays; some loss of

Minor: Some minor injuries and/or stress to personnel; limited program delays; minor damage

Negligible: No injuries to personnel; no measurable program delays; no measurable damage

Note: For the **purposes of travel security only,** and to align Risk Ratings with advisories issued by the Bank's outsourced medical and security service provider contracted at the time of promulgation of this Part, the Risk Rating of "Very High" in the matrix is synonymous with the service provider's Risk Rating of "Extreme". "Unacceptable" in the matrix above has no equivalent in the assessments undertaken by the service provider as the service provider does not assess any risk as more serious than "Extreme". This note will only remain relevant while the circumstances for which it has been included as a note to Appendix A exists.

[Intentionally blank]

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 11: FIRE SAFETY

A. OBJECTIVE OF THIS PART

1.1 This Part establishes internal rules and processes for Fire Safety in the Bank, and augments any applicable Fire Safety legislation, codes, regulations or rules set by Host Nation authorities, as defined in the Directive on Security and Safety (Part 17: Host Nation Relations), or those set by building management authorities of Bank Premises as defined in the Directive on Security and Safety (Part 5: Security of Bank Premises).

B. GENERAL PRINCIPLES

2.1 Fire is a preventable hazard, and compliance to simple safety measures will serve to minimise the risk to persons, assets and Bank Premises.

2.2 Fire Safety strategy comprises both prevention measures to minimise the risk of fire, and mitigation measures to protect persons, assets and Bank Premises.

2.3 The Bank shall respect Fire Safety laws, codes and regulations of the Host Nation.

C. DEFINITIONS

3.1 “Bank Premises” is as defined in the Directive on Security and Safety (Part 5: Security of Bank Premises).

3.2 “Business Unit” is as defined in the Directive on Business Continuity.

3.3 “Fire Safety” means the set of practices intended to reduce the destruction or damage caused by fire. Fire Safety measures include those that are intended to prevent ignition of an uncontrolled fire, and those that are used to limit the development and effects of a fire after it starts.

3.4 “Fire Safety Violation” means an act or omission that compromises, or may compromise, Fire Safety.

3.5 “Warden” means a layperson who has volunteered to act for their Business Unit or floor, as the case may be, as the fire focal point under the direction of the officer responsible for the management of security and safety. In the absence of volunteers, This officer shall appoint Wardens as specified in the Directive on Security and Safety (Part 2: Accountability).

D. RESPONSIBILITIES

4.1 The primary responsible party for fire prevention and suppression at Bank Premises remains the owner of the building in which the Bank Premises are housed, if applicable, and their appointed building management company. The secondary responsible party shall be any

company hired by the Bank to manage the Bank's exclusive use areas within a building if applicable. Neither of these entities are governed by this Part. The tertiary responsible party shall be the Bank.

4.2 **Individuals**. Individuals to whom the Directive on Security and Safety (Part 2: Accountability) applies shall abide by all Fire Safety rules and measures adopted for Bank Premises by building and facility managers, the officer responsible for the management of security and safety, and, the Building Facilities Management (BFM) Unit of the Facilities and Administration Services Department (FAS).

4.3 **Officer Responsible for the management of Security and Safety**. This officer shall:

4.3.1 Ensure that outsourced and internal security and safety personnel are trained in their roles related to fire prevention and firefighting.

4.3.2 Ensure that measures are in place to report a fire or fire hazard.

4.3.3 Ensure that persons listed in the Directive on Security and Safety (Part 3: Applicability) working at Bank Premises are trained in immediate actions in the event of a fire.

4.3.4 Appoint and direct Wardens in their role and maintain an up to date list of Wardens.

4.3.5 Take charge during a Fire Safety crisis to ensure that all persons in the Bank Premises are guided as to their actions which could involve evacuating the building.

4.3.6 Determine what Fire Safety training is required and arrange for the training to be delivered to the relevant recipients as indicated in the Directive on Security and Safety (Part 2: Accountability).

4.4 **Wardens**. Wardens shall execute the tasks assigned to them by the officer responsible for the management of security and safety. Wardens shall:

4.4.1 Sound the alarm in the event of fire observed by them or reported to them by a colleague.

4.4.2 Marshal colleagues and guide them according to the fire plan.

4.4.3 Report to the officer responsible for the management of security and safety any actual or potential Fire Safety Violation observed by them or reported to them.

4.4.4 Ensure that any Fire Safety equipment entrusted to them is kept serviceable and easily accessible.

4.4.5 Report any planned prolonged absence from the work place due to leave, illness, mission away from headquarters or any other reason to the officer responsible for the management of security and safety.

4.5 **Building Facilities Management Unit (BFM) of FAS**. The senior officer of the BFM shall:

4.5.1 Appoint a staff member to oversee, as the Bank's representative, Fire Safety matters at the headquarters.

4.5.2 Ensure that the building management company, if applicable, maintains all fire prevention and suppression equipment and installations at the standard required by the Beijing Municipal Government.

4.5.3 Coordinate all Fire Safety matters with the officer responsible for the management of security and safety.

4.5.4 Act as the Bank's fire prevention and suppression expert in support of the officer responsible for the management of security and safety.

4.5.5 Resolve any reported actual or potential Fire Safety Violation reported by the officer responsible for the management of security and safety or other person.

4.5.6 Assist with training, or organizing of training, of the Wardens.

E. REPORTING

5.1 Any individuals to whom the Directive on Security and Safety (Part 2: Accountability) applies who observes an actual or potential Fire Safety Hazard shall report such in a timely manner to any Warden, the officer responsible for the management of security and safety or any security personnel and take actions according to the fire plan.

5.2 The officer responsible for the management of security and safety shall report to the Director General of the Facilities and Administration Services Department (DG FAS) on a quarterly basis any reports received of Fire Safety Violations and actions taken with respect to plans or processes to prevent recurrence.

F. TRAINING AND FIRE DRILLS

6.1 Individuals to whom the Directive on Security and Safety (Part 2: Accountability) applies shall participate fully in fire training and drills applicable to them.

6.2 The hosts of visitors, to include maintenance and service contractors, to Bank Premises shall be responsible to ensure that such visitors participate in fire drills should these take place while the visitors are present. If unwilling to do so, the host responsible shall request such visitors to leave the Bank Premises.

*****

[Intentionally blank]

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 12: HOSTAGE INCIDENT MANAGEMENT

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules for managing Hostage-Taking of those individuals listed in Section 4.1 of the Directive on Security and Safety (Part 3: Applicability).

B. GENERAL PRINCIPLES

2.1 The applicability of Hostage Incident Management (HIM) extends to any location where activities of the Bank are conducted.

2.2 The management of Hostage-Taking, kidnapping and abduction is addressed under the single term, HIM.

C. DEFINITIONS

3.1 "Hostage-Taking" is defined in the International Convention Against the Taking of Hostages of 17 December 1979 as the seizure or detention and threat to kill, to injure or to continue to detain another person (hereinafter referred to as the "Hostage") in order to compel a third party, namely, a State, an international intergovernmental organization, a natural or juridical person, or a group of persons, to do or to abstain from doing any act as an explicit or implicit condition for the release of the hostage. This definition is accepted for Bank use and is deemed to include kidnapping and abduction.

3.2 "Hostage-Taker" means the individual or group responsible for Hostage-Taking, or who participates as an accomplice.

3.3 "Ransom" means money or other consideration demanded for the release of a Hostage.

D. LEGAL FRAMEWORK

4.1 This Part draws on the 1979 International Convention against the Taking of Hostages which, amongst other matters, provides that Hostage-Taking is an offence of grave concern to the international community, that any person committing an offence of Hostage-Taking shall either be prosecuted or extradited, and that States shall make such offences punishable by appropriate penalties which take into account the grave nature of these offences; and on United Nations Security Council resolution 579 (1985) by which the Council unequivocally condemned Hostage-Taking, called for the immediate release of all Hostages wherever and by whomever they were being held, and affirmed the obligation of all States in whose territory Hostages were held to urgently take all appropriate measures to secure their safe release and to prevent the commission of acts of Hostage-Taking in the future.

E. GENERAL RULE

5.1 The Bank shall neither pay Ransom nor make any substantial concessions to Hostage-Takers to secure the release of Hostages, nor shall it intervene with the State concerned to make concessions in exchange for Hostages, because this would encourage potential Hostage-Taking, and thus, increase the danger that other individuals covered by this Part might face in the future.

5.2 Should individuals covered by this Part be taken Hostage, the Bank shall make every effort to secure their speedy and safe release, notwithstanding the legal imperative of States as described in Section D. To achieve this goal, the Bank may establish contacts or start dialogue with the Hostage-Takers if it is determined that this would promote the speedy and safe release of the Hostages or engage a third party to do so on behalf of the Bank. Such contacts or dialogue shall be aimed at trying to convince the Hostage-Takers of the inhumanity, illegality and futility of their actions as a means of attaining their objectives.

5.3 The Bank shall always assist individuals covered by this Part who fall victim to Hostage-Taking as a result of their official duties and will assist where possible in cases where the incident is not as a result of their official duties.

F. PREVENTION AND RESILIENCE

6.1 It is accepted that Hostage-Taking can occur anywhere, however the likelihood of such events is greater in locations assessed as High Risk. The Vice President and Chief Administration Officer (VP & CAO) shall, through the officer responsible for the management of security and safety, develop and maintain the following measures in an attempt to prevent individuals covered by this Part falling victim to Hostage-Taking, and in the event that this still occurs, to build resilience of potential Hostages:

6.1.1 Ensuring that the Travel Security Clearance (TSC) process as specified in the Directive on Security and Safety (Part 7: Travel Security) is enforced for all travel to locations assessed as High Risk or higher.

6.1.2 Issuing of guidance for Hostages to enhance their chance of survival.

6.1.3 Development of a process to record proof of life questions for travelers to locations assessed as High Risk.

6.1.4 Development of a training program for Hostage incident prevention and survival either as a separate topic, or within other training modules.

G. HOSTAGE INCIDENT MANAGEMENT

7.1 The VP & CAO shall, through the officer responsible for the management of security and safety, develop HIM guidance to guide management actions at the Bank should persons included in section 1.1 fall victim to Hostage-Taking. This guidance may specify specific responses for the unique circumstances related to kidnapping and abduction where relevant.

7.2 The guidance shall include, but may not be limited to, specific arrangements, to be planned and managed by departments of the Bank, as follows:

7.2.1 Establishment of a HIM team and crisis management arrangements.

7.2.2 Specific actions to be taken and avoided by the HIM and crisis management teams.

7.2.3 Host Nation, as defined in the Directive on Security and Safety (Part 17: Host Nation Relations) liaison and coordination guidelines.

7.2.4 Liaison with third party specialist HIM vendors, and coordination of their activities.

7.2.5 Media and communication guidelines.

7.2.6 Family support including stress counselling for families of the Hostage(s).

7.2.7 Reception plan on release.

7.2.8 Post-incident stress counselling for the Hostage(s).

7.2.9 Insurance arrangements for the management of the Hostage incident itself.

7.2.10 Post-incident debrief of the Hostage(s) and reports.

7.3 The VP & CAO shall coordinate the Bank's response to Hostage-Taking, but all substantive decisions shall be taken by the President.

7.4 The VP & CAO shall identify specialist vendors of HIM services and where necessary, engage such vendors when a Hostage-Taking occurs, or on a stand-by or retainer basis.

7.5 Post-incident reports shall indicate if the Hostage incident resulted from, or was exacerbated by, actions or omissions in the observance of Bank security Directives, instructions, advisories, guidelines or rules.

*****

[Intentionally blank]

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 13: SECURITY CRISIS MANAGEMENT

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules and processes for the management of security Crises to ensure that individuals, the Bank's assets and Bank Premises, as such term is defined in the Directive on Security and Safety (Part 5: Security of Bank Premises), are protected during such Crises and that normal operations resume at the earliest opportunity.

1.2 This Part shall apply at headquarters and at any location where Special Events or Bank Activities, as such terms are defined in the Directive on Security and Safety (Part 6: Security of Special Events and Part 16: Security of Bank Activities respectively), take place, or in support of a security Crisis experienced at any field location where the Bank operates.

B. GENERAL PRINCIPLES

2.1 Business disruptions for which the Directive on Business Continuity applies will be handled according to that Directive. Should a business disruption involve risk to life, or significant damage to the Bank's assets or Bank Premises, the management of the situation may be escalated to the level of a Crisis at the discretion of the Crisis Manager.

2.2 This Part only addresses security Crisis, however the Crisis management architecture and processes mandated by this Part can be applied to any form of Crisis.

C. DEFINITION

3.1 "Crisis", to imply a security crisis for the purposes of this Part, means a situation created by an incident, or the potential for such incident, threatening to inflict harm on individuals or significant damage to, or loss of, the Bank's assets or Bank Premises.

3.2 "Crisis Manager (CM)" means the person appointed to lead and direct the Bank's response to Crisis.

3.3 "Crisis Management Team (CMT)" means a standing body for the management of Crisis under the leadership and direction of the CM, activated when required.

3.4 "Crisis Coordinator (CC)" means the person appointed to coordinate the activities of the CMT under the direction of the CM.

D. CRISIS MANAGEMENT TEAM

4.1 The CM shall be the Vice President and Chief Administration Officer (VP & CAO). In situations where the VP & CAO is unavailable, the President shall assign any other member of Senior Management to this role. In the case of a crisis situation where none of the Senior

Management team are available, and in the absence of a decision by the President, the most senior officer at the location shall assume the duties of a CM.

4.2 The CC shall be the officer responsible for the management of security and safety.

4.3 The CMT shall comprise the following officers and Business Units, as such term is defined in the Directive on Business Continuity:

4.3.1 The CM.

4.3.2 Office of the President.

4.3.3 VP and Corporate Secretary.

4.3.4 VPs Investment Operations (as applicable to the crisis at the discretion of the CM).

4.3.5 VP Policy and Strategy.

4.3.6 The General Counsel (OGC).

4.3.7 The Chief Risk Officer (RMD).

4.3.8 The Chief Financial Officer (CFO).

4.3.9 Communications Department (COM).

4.3.10 Facilities and Administration Services Department (FAS).

4.3.11 Human Resources Department (HRD).

4.3.12 The officer responsible for the management of security and safety (the CC).

4.4 The officers and heads of Business Units referenced in Section 4.3 shall be the primary member of the CMT and, with the exception of the CM, shall appoint an alternate member. In the absence of these pre-designated members, the Business Units shall be represented by the most senior officer in that Business Unit at the time of the Crisis.

4.5 The CM shall co-opt any additional members as required.

4.6 The CC shall provide technical advice related to security and safety as well as secretarial services to the CMT once activated.

E. ACCOUNTABILITY AND ROLES

5.1 The CMT is accountable to the President to coordinate the Bank's internal and external responses in the event of a Crisis.

5.2 The decision to declare a Crisis shall be taken by the President or in the absence of the President, the CM.

5.3 Upon the declaration of a Crisis, the CMT shall be activated.

5.4 The CM shall direct the CC to coordinate the implementation of the decisions of the CMT.

5.5 During a Crisis, the CM shall keep the President informed on developments as regularly as practically possible.

F. CRISIS SCENARIOS AND PLANS

6.1 The CC shall lead the work required to develop possible Crisis scenarios for headquarters and for specific Special Events and Bank Activities away from headquarters at the time of planning for those activities.

6.2 To facilitate prompt reaction in a Crisis, members of the CMT shall ensure that their respective Business Unit Business Continuity Plans as laid down in the Directive on Business Continuity are up-to-date and readily available on a permanent basis.

6.3 The CM shall determine if detailed Crisis management plans are required for all, or some, identified scenarios. Arrangements shall include, but not limited to, the following elements to form a Crisis plan for the scenario being addressed:

6.3.1 Security management and coordination plan.

6.3.2 Legal support plan.

6.3.3 Communications plan.

6.3.4 Human resources plan.

6.3.5 Logistics support plan for facilities, travel and administration.

6.3.6 Actions to be taken by Bank Personnel as such term is defined in the Code of Conduct for Bank Personnel.

6.4 The CC shall lead the work required to develop plans for scenarios as directed by the CM.

G. CRISIS MANAGEMENT CENTRE

7.1 At headquarters the Crisis Management Center (CMC) shall be the meeting room used by the Executive Committee unless an alternate CMC is selected by the CM.

7.2 Away from headquarters, a suitable venue shall be found by the CC and approved by the CM. This shall be determined at the time of arrival at the location of the Special Event or Bank Activity.

H. RESPONSE AND ACTIVATION

8.1 Once a Crisis is declared by the President in accordance with Section 5.2, the CM shall activate the CMT and set forth actions, including but not limited to the following:

8.1.1 gather all available information on the Crisis;

8.1.2 assess the severity of the situation;

8.1.3 advise the President of the situation;

8.1.4 determine whether the response will follow an existing plan or guide the development of a plan;

8.1.5 task CMT members; and,

8.1.6 communicate the situation to Bank Personnel while ensuring that the message reaches all other relevant individuals, including visitors.

8.2 The CM, advised by the CMT, and with technical input from the CC, shall classify the Crisis according to a code signifying the level of severity of the actual or potential incident:

8.2.1 **Code Red**: Involves the potential to inflict grave harm including all incidents where casualties are involved or possible, or where significant potential harm to the independence, integrity or effectiveness of the Bank" is indicated.

8.2.2 **Code Blue**: Involves the potential to inflict serious harm or where the potential for violence exists but has not yet occurred or where serious reputational harm to the Bank is possible.

8.2.3 **Code Yellow**: Involves the potential to inflict harm but does not have wide impact but could potentially escalate and have negative consequences.

8.3 The CM shall direct the actions to be taken commensurate with the classification allocated and indicate the triggers that will escalate the classification to higher or lower levels of severity, and the subsequent actions to be taken.

8.4 Business disruptions for which the Directive on Business Continuity applies shall not be classified under this Part.

I. DEACTIVATION

9.1 Upon successful resolution of the Crisis, the CM shall advise the President who shall declare the Crisis over and give instructions for the resumption of normal Bank activities.

9.2 The CC shall prepare a report on the handling of the Crisis indicating strong and weak points in the handling of the Crisis, and identify any lessons learned to be applied in future Crises.

9.3 On deactivation of the CMT, the CC shall provide all the records of the management of the Crisis to the officer responsible for management of Bank records.

*****

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 14: SECURITY COMPLIANCE

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules and processes for guiding the officer responsible for the management of security and safety for the monitoring and assessing of security compliance.

B. GENERAL PRINCIPLES

2.1 Security compliance is an individual responsibility required pursuant to the Code of Conduct for Bank Personnel and by the various Parts of the Directive on Security and Safety.

2.2 The monitoring and assessment of compliance with security rules by the officer responsible for the management of security and safety enhances the protection of individuals and groups as well as the Bank's assets and operations.

C. SECURITY COMPLIANCE FRAMEWORK

3.1 The scope of the security compliance framework shall include:

3.1.1 All Parts of the Directive on Security and Safety.

3.1.2 Security rules, instructions, advisories, or measures issued by the officer responsible for the management of security and safety from time-to-time under the authority of the President, the Vice President and Chief Administration Officer (VP & CAO) or the Director General of the Facilities and Administration Services Department (DG FAS).

3.1.3 Administrative Guidance on security topics issued under the authority of the VP & CAO.

3.2 Five elements shall be involved in security compliance as follows:

3.2.1 **Monitoring**. The officer responsible for the management of security and safety shall develop and implement processes to monitor compliance with security rules, including the effectiveness and efficiency of the relevant Directives, processes and general security and safety guidance, and to record the results of this monitoring.

3.2.2 **Assessment**. The officer responsible for the management of security and safety shall assess the results of monitoring to determine the impact on the security of individuals, Bank assets and Bank Premises so as to identify any vulnerabilities resulting from non-compliance.

3.2.3 **Reporting**. The officer responsible for the management of security and safety shall report non-compliance to security rules that is assessed as exposing the Bank to a High, Very High or Unacceptable level of Risk as defined in the Directive on Security and Safety (Part 10: Security Risk Management) to the DG FAS.

3.2.4 **Remedial Action**. The officer responsible for the management of security and safety shall analyse all instances of non-compliance with security rules for the purposes of identifying trends and lessons learned and shall take appropriate actions to prevent reoccurrence of the non-compliance.

3.2.5 **Learning**. The officer responsible for the management of security and safety shall use the lessons learned and best practice from the monitoring and assessment of compliance for continuous learning and improvement within the Security and Emergency Management Unit at FAS, and within the Bank as a whole.

D. ANNUAL ANALYSIS AND REPORTING OF NON-COMPLIANCE

4.1 The officer responsible for the management of security and safety shall compile an annual report, by the end of February of the following year, of observed trends and lessons learned of non-compliance to security rules, and the remedial action taken. Such report shall not name individuals involved or be of such specificity as to identify individuals. This report shall be presented to the President, advised by the Executive Committee, and published for informational purposes within the Bank at the discretion of the President. The report may also be used for training purposes. The purpose of this report will be to prevent recurrence and to assist in developing a spontaneous and sound security culture within the Bank.

*****

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 15: ARREST AND DETENTION

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules for handling of incidents where individuals covered by section 4.1 of the Directive on Security and Safety (Part 3: Applicability) are arrested or detained by a State or other jurisdiction.

B. GENERAL PRINCIPLES

2.1 The provisions of the Headquarters Agreement between the Government of the People's Republic of China and the Bank, in particular Article 14(3)(a), shall provide guidance for this Part as it relates to arrest and detention within the jurisdiction of the People's Republic of China.

2.2 Should individuals be arrested or detained with respect to acts performed by them in their official capacity in the jurisdiction of a member country of the Bank, the Articles of Agreement, in particular, Article 50(i) shall provide guidance for this Part.

2.3 The Bank shall always assist individuals who are arrested or detained in any jurisdiction as a result of their official duties and may offer limited assistance to those arrested or detained in their private capacity. Arrest and detention during Official Travel of individuals shall by default be considered as arrest within the scope of Official Duties, unless and until proven otherwise.

2.4 Handling of arrests and detentions is primarily a legal matter under the authority of the General Counsel, and may have human resources management implications, however, as security personnel are frequently the first to be called by the individual arrested or detained, this Part of the Directive on Security and Safety is required to guide the actions of such security personnel in the event of an arrest or detention with the aim of ensuring the safety and welfare of the individuals concerned.

C. DEFINITION

3.1 "Arrest" means the seizure or forcible restraint of an individual.

3.2 "Detention" means the act of holding a person in custody.

D. NOTIFICATION

4.1 Irrespective of the method by which the news of an incident involving arrest or detention reaches the Bank, any individual receiving news of an individual being detained or arrested shall notify the officer responsible for the management of security and safety as soon as practically possible.

4.2 The officer responsible for the management of security and safety shall notify the Director General of the Facilities and Administration Services Department (DG FAS) first promptly, who in turn shall notify the President, the Vice President and Chief Administration Officer and the General Counsel.

E. SECURITY RESPONSIBILITIES

5.1 The officer responsible for the management of security and safety shall be responsible for managing the security aspects related to arrest and detention. Security personnel shall make no determination or statements concerning the legal status of any person detained or arrested.

5.2 The primary security objective relating to arrest and detention shall be to ensure the safety and welfare of the individual arrested or detained.

5.3 General security responsibilities:

5.3.1 The officer responsible for the management of security and safety shall without delay notify the Human Resources Department (HRD) and the Communications Department (COM) once initial reporting in Section 4.2 has been done.

5.3.2 On advice of the General Counsel, the officer responsible for the management of security and safety shall make contact with local authorities to ascertain the whereabouts of the individual arrested or detained and make arrangements for visiting such individual.

5.3.3 When there are concerns that the safety or wellbeing of the individual arrested or detained is in jeopardy, the officer responsible for the management of security and safety shall arrange stand-by medical assistance and make arrangements for repatriation to the home country of the individual or to Beijing as determined by the Bank in consultation with the arrested or detained individual should such individual be released and is unable, for medical or psychological reasons, to travel on their own.

5.4 Outside of the People's Republic of China the officer responsible for the management of security and safety shall arrange security support, if required, with the respective Host Nation authority, under the guidance and support of the Corporate Secretariat, or with any security service provider contracted by the Bank within that jurisdiction, or arrange support from any other available source.

F. NON-SECURITY RESPONSIBILITIES

6.1 The Director General HRD shall provide all human resources management support necessary, which shall include, but not be limited to, contact with relatives of the individual arrested or detained, arrangements for repatriation of personal effects if required and, medical or psychological follow-up for the individual who was arrested or detained.

6.2 Other Business Units (as such term is defined in the Directive on Business Continuity) including the Business Unit for which the individual arrested or detained works, shall provide

any additional support required relevant to that Business Unit, including but not limited to, administrative, logistic and legal support to successfully resolve the incident.

G. INFORMATION TO BE CAPTURED

7.1 The officer responsible for the management of security and safety shall coordinate the collection and collation of the basic information required to address incidents of arrest and detention and make such information available to other Business Units involved.

7.2 The following information shall be collected for all cases of arrest or detention arising from the official duties of the individual arrested or detained:

7.2.1 The name and nationality of the individual arrested or detained, their employment status with, and official functions for, the Bank. For family members the family relationship must be given. In the case of children, the age(s) should be given;

7.2.2 The time, place and other circumstances of the arrest or detention;

7.2.3 The expression or term used by the entity that arrested or detained the Bank individual to describe the reason for arrest or detention;

7.2.4 The name of the governmental agency, such as a court or an administrative authority, under whose authority the measure was taken;

7.2.5 Whether a representative of the Bank has been, or will be, given access to the individual arrested or detained. In the affirmative, any request or other reaction from the individual concerned also shall be conveyed;

7.2.6 Whether consular protection and/or legal counsel is, or is planned, to be availed to the individual arrested or detained. In the affirmative, the nature of these services shall be conveyed; and

7.2.7 An assessment of the welfare or safety of the arrested or detained individual, including any reports of mistreatment and whether medical assistance is planned, or has been provided.

7.3 Information listed in section 7.2 shall be made available according to section 7.4 without delay. If information on some of the items is not immediately available, the missing information shall be forwarded, when it is available, without delay in a supplementary report or reports.

7.4 All information relating to incidents of arrest and detention shall be handled in accordance with the rules for handling information at the highest level of classification for sensitive information in use in the Bank.

H. ARREST OR DETENTION RESULTING FROM PRIVATE ACTIVITIES

8.1 In the event of an individual being arrested or detained in their private capacity not connected to their official duties, the Bank may or may not assist at the discretion of the President. In order for the President to take such a decision, all the information contained in

Section G shall still be collected by the officer responsible for the management of security and safety and provided for review.

I. DETENTION BY NON-STATE ACTORS

9.1 The present procedures shall also be applied, as appropriate, with respect to detention carried out by persons or entities other than authorities of the jurisdiction in which the incident occurred. These could include non-state actors where the authority of the state does not extend to the location where the arrest or detention took place.

*****

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 16: SECURITY OF BANK ACTIVITIES

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules and processes for ensuring the security of Bank Activities conducted in Bank Premises as defined in the Directive on Security and Safety (Part 5: Security of Bank Premises) and at other locations.

B. GENERAL PRINCIPLE

2.1 The Bank recognizes the importance of ensuring that activities of the Bank are conducted in a secure and safe manner.

C. DEFINITIONS

3.1 "Bank Activity" means any Bank-related group activity, conference or meeting arranged, sponsored or organized by the Bank other than a regular, routine activity or a Special Event as defined in the Directive on Security and Safety (Part 6: Security of Special Events).

3.2 "Organizer" for the purposes of this Part means the Bank Personnel, as such term is defined in the Code of Conduct for Bank Personnel, or Business Unit, as such term is defined in the Directive on Business Continuity, responsible for organizing the Bank Activity.

D. PLANNING FOR BANK ACTIVITIES

4.1 The Organizer shall consider security as an integral component of the planning of any Bank Activity.

4.2 The Organizer shall notify the officer responsible for the management of security and safety at the Facilities and Administration Services Department (FAS) of the intention to arrange a Bank Activity in advance of the activity within a reasonable time frame to allow for security assessments and planning.

4.3 The officer responsible for the management of security and safety shall provide any security advice and support, as may be required by the Organizer.

4.4 The Organizer shall be responsible for all costs associated with security not covered under regular budget provision for the day-to-day functioning of the Bank.

E. RISK ASSESSMENT

5.1 The officer responsible for the management of security and safety shall conduct a Security Risk Assessment as defined in the Directive on Security and Safety (Part 10: Security Risk Management) to determine any potential security risks associated with the Bank Activity

and specify any prevention or mitigation measures required. The measures determined may involve the acquisition or provision of security services external to the Bank.

5.2 The proposed Bank Activity shall not take place until all measures prescribed by the officer responsible for the management of security and safety are implemented.

F. STANDING SECURITY MEASURES FOR BANK ACTIVITIES

6.1 The Organizer shall take the following standing security measures into consideration when planning Bank Activities.

6.2 **Venue:**

6.2.1 The venue shall be protected against intrusion from persons uninvited to the activity. To this end the provisions of the Directive on Security and Safety (Part 5: Security of Bank Premises) shall apply for Bank Activities held at the Bank's Premises.

6.2.2 For events held outside the Bank's Premises, the officer responsible for the management of security and safety shall determine if special security arrangements are required.

6.3 **Transport:**

6.3.1 Bank Personnel and other categories of persons listed in the Directive on Security and Safety (Part 3: Applicability), attending Bank Activities, shall only be transported in vehicles or watercraft licenced for carrying passengers and provided either by the Bank itself, by licensed transportation vendors of public ferries, taxis and limousine companies, or by private vehicles belonging to attendees.

6.3.2 Where aircraft are involved, the special provisions for air travel stipulated in the Directive on Security and Safety (Part 7: Travel Security) shall apply.

6.3.3 The rules applicable to the number of senior staff who may travel in the same conveyance as stipulated in the Directive on Security and Safety (Part 7: Travel Security), shall apply.

6.4 **Security Awareness**. The Organizer of, and Bank Personnel attending, Bank Activities shall apply reasonable judgement with respect to security in line with guidance in the Directive on Security and Safety (Part 8: Security Awareness).

*****

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 17: HOST NATION RELATIONS

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules for security and safety personnel of the Bank as described in Section 5.6. of the Directive on Security and Safety (Part 2: Accountability) when dealing with the Host Nation authorities of jurisdictions where activities of the Bank are conducted.

1.2 This Part of the Directive on Security and Safety is aimed at establishing the parameters for the engagement of security and safety personnel with Host Nation authorities only in the direct execution of their official security responsibilities.

B. GENERAL PRINCIPLES

2.1 The primary entity for the establishment of relations with Host Nations in any jurisdiction where the Bank may conduct activities is the Corporate Secretary. Contact by security and safety personnel, as described in Section 5.6. of the Directive on Security and Safety (Part 2: Accountability), with Host Nation authorities is based on the relationship established by the Corporate Secretary. Security and safety personnel shall not establish official relationships with Host Nation authorities on their own authority.

2.2 Within the parameters set by the Corporate Secretary, the officer responsible for the management of security and safety shall make every effort to establish relationships beneficial to the Bank with Host Nation authorities so as to enhance security collaboration.

C. DEFINITION

3.1 “Host Nation” means a jurisdiction where activities of the Bank are conducted.

D. SCOPE OF ENGAGEMENT

4.1 Engagement with Host Nations shall be for the following purposes:

4.1.1 To notify Host Nation authorities of an actual or planned AIIB presence within the jurisdiction.

4.1.2 To notify Host Nation authorities of a planned Bank Activity as defined in the Directive on Security and Safety (Part 16: Security of Bank Activities) within the jurisdiction.

4.1.3 To request or arrange security support from Host Nation authorities or to notify Host Nation authorities of security services that will be provided by third parties.

4.1.4 To request information on Threats and Hazards, and the associated Risks as defined in the Directive on Security and Safety (Part 1: Introduction) to the Bank, or to provide such information to Host Nation authorities.

4.1.5 To collaborate with Host Nation authorities on the development of security Threat and Risk Assessments as defined in the Directive on Security and Safety (Part 10: Security Risk Management).

4.1.6 To collaborate on security crisis management where the Bank is involved or threatened.

4.1.7 To coordinate security measures where the Bank and the Host Nation authorities are collaborating on security for any reason.

4.1.8 To collaborate on a hostage situation as defined in the Directive on Security and Safety (Part 12: Hostage Incident Management).

4.1.9 To enquire after the safety and wellbeing of an individual who has been arrested or detained as described in the Directive on Security and Safety (Part 15: Arrest and Detention), and to act as liaison between the Host Nation authorities, the individual affected, and the Bank.

4.1.10 To report a missing person, criminal incident, accident involving a third party or any other relevant security or safety issue.

4.1.11 To liaise with Host Nation authorities on the importation and exportation of security equipment.

4.1.12 In the pursuance of any matter governed by the Directive on Security and Safety not listed above.

E. *DE FACTO* AUTHORITIES IN THE ABSENCE OF LEGITIMATE AUTHORITIES

5.1 This Part of the Directive on Security and Safety does not cover collaboration with *de facto* authorities and “non-state actors” that may be in control of areas where no Host Nation authority is in place or functioning. If it is in the best interests of the Bank, as determined by the President, advised by the Executive Committee, the principles outlined in this Part shall be applied to instances where non-state actors or *de facto* authorities control areas within a given nation.

*****

DIRECTIVE ON SECURITY AND SAFETY
April 28, 2020

PART 18: ARMED PROTECTION

A. OBJECTIVE OF THIS PART

1.1 This Part establishes rules for the use of Armed Protection to protect: Bank Personnel as defined in the Code of Conduct for Bank Personnel; Bank Premises as defined in the Directive on Security and Safety (Part 5: Security of Bank Premises); and, Assets as defined in the Directive on Asset Management.

B. APPLICABILITY

2.1 This Part applies to Armed Protection provided by any person or entity other than Bank Personnel.

2.2 This Part applies to Bank operations and business in any location globally.

C. GENERAL PRINCIPLES

3.1 Bank Personnel shall not be armed as defined under the term Armed Protection while on Bank Premises or at any time during the implementation of any Bank operation or business.

3.2 The use of Armed Protection is a significant, and visible, increase in the security profile of the Bank and shall be utilized only when unarmed protection has been assessed as insufficient to provide the required level of security.

3.3 Primary accountability for the use of a Weapon, and the consequences of such use, remains with the operator of the Weapon involved. Secondary accountability lies with the person or organization who gave instructions for its use.

D. DEFINITIONS

4.1 “Armed Protection” means the provision of security services where the persons providing the services are armed with a Weapon(s) irrespective of whether the Weapon(s) is visible or concealed, and whether performing protection tasks in the static guarding or mobile role.

4.2 “Weapon” means a device designed or used for inflicting bodily harm or physical damage. This definition includes, but is not limited to, firearms of any caliber or type; explosives; batons or clubs; pepper or chemical sprays; tasers; and, edged Weapons such as knives, daggers, axes or machetes.

4.3 “Deadly Force” means any force that creates a substantial risk of causing death or serious bodily injury.

E. UTILIZATION OF ARMED PROTECTION

5.1 Armed Protection arranged by the Bank may be utilized for the protection of Bank Personnel, Bank Premises, and Assets, but only when unarmed protection has been assessed as insufficient to provide the required level of security.

5.2 Armed Protection shall only be utilized after the officer responsible for the management of security and safety as defined in the Directive on Security and Safety (Part 2: Accountability) has determined that this level of security is required after assessing the risk according to the Directive on Security and Safety (Part 10: Security Risk Management).

5.3 The officer responsible for the management of security and safety shall authorize the use of Armed Protection in the Bank. For Armed Protection during missions, the authorization process shall take place at the point of applying for Travel Security Clearance as defined in the Directive on Security and Safety (Part 7: Travel Security).

5.4 Armed Protection may be provided in the form of direct close personal protection; as escorts accompanying Bank Personnel in separate vehicles; or, in the role of static guarding.

5.5 **Limitations on the use of Armed Protection**. Armed Protection is aimed, *inter alia*, at protecting Bank Personnel, however any Weapon is also capable of inflicting harm on Bank Personnel and as such the following limitations on the use of Armed Protection apply:

5.5.1 Armed Protection shall not to be utilized if such use, or presence, of Weapons is assessed by the officer responsible for the management of security and safety as potentially harmful to Bank Personnel.

5.5.2 Armed Protection shall not to be utilized if local laws in the jurisdiction where the Bank operation or business is to be conducted do not permit such use.

5.5.3 Conversely, Armed Protection shall only be utilized after all local laws in the jurisdiction where the Bank operation or business is to be conducted have been considered and all required permits or licenses obtained by the provider of Armed Protection services.

5.5.4 Where Armed Protection is provided by the security agencies of Host Nations in accordance with the Directive on Security and Safety (Part 17: Host Nation Relations) in the jurisdictions where the Bank operation or business is being performed, no limitations are placed by the Bank on the arming of such personnel by Host Nations with the exception of access to Bank Premises where armed (or unarmed) security personnel of any government shall only be permitted to enter Bank Premises in accordance with Article 6(2) of the Headquarters Agreement. The provisions of the Directive on Security and Safety (Part 5: Security of Bank Premises) shall apply.

5.5.5 Armed (or unarmed) personnel of private security service providers shall not be permitted to enter Bank Premises unless the service provider is providing the service pursuant to a contract it has with the Bank, and the use of Weapons is stipulated in such contract.

5.6 Bank Personnel shall not interfere with, or handle, any Weapons carried by persons involved with Armed Protection for the Bank.

5.7 No member of Bank Personnel shall unilaterally or privately arrange or contract Armed Protection for use during the performance of Bank operations or business. In exceptional circumstances where the officer responsible for the management of security and safety has assessed that Armed Protection is required in accordance with Sections 5.2 and 5.3 of this Part, but is unable to personally arrange such protection, authority may be given to Bank Personnel on mission to make such arrangements, but the authority shall be in writing and include clear instructions on how this shall be done.

F. USE OF FORCE

6.1 Any force used during the protection of Bank Personnel, Bank Premises or Assets has the potential to cause serious reputational harm to the Bank and as such shall comply with the following principles:

6.1.1 Weapons shall be primarily used to deter physical assault against Bank Personnel, Bank Premises and Assets. Such deterrence value is diminished if the Weapons are concealed.

6.1.2 Where deterrence has failed, physical application of a Weapon to counter a threat using Deadly Force shall only occur when the imminent threat of death or serious bodily injury to Bank Personnel is present. The principle shall be to use the Weapon to save lives and not as retaliation when the threat has passed.

6.1.3 Deadly Force shall not be used to protect Bank Premises or Assets unless the lives and safety of Bank Personnel are directly threatened.

6.1.4 Weapons shall only be used to apply force according to the laws of the jurisdiction where the force is to be applied, and in accordance with international law.

6.2 **Criteria for the use of Deadly Force**. When the use of Deadly Force is unavoidable, restraint shall be exercised, respecting and preserving human life and causing the minimum harm to people and property. Deadly Force shall only be used when all three of the following criteria apply:

6.2.1 The force is necessary, under all the circumstances known at the time, to negate the threat; and,

6.2.2 the force is reasonable, proportional to the threat presented and the minimum required to negate the threat; and,

6.2.3 there is no other reasonable alternative available.

G. CONTRACTUAL STIPULATIONS FOR PRIVATE SECURITY SERVICE PROVIDERS

7.1 Private security service providers shall only be considered for the provision of Armed Protection services when the Host Nation authorities in the jurisdiction where the service is required are unable, or unwilling, to provide such service.

7.2 Contracting for the provision of Armed Protection services shall follow the rules stipulated in the Bank's Internal Legal Framework including, but not limited to: the Policy on Corporate Procurement; the Directive on Corporate Procurement and its related Administrative Guidance; the Policy on Prohibited Practices; and, any Directives regulating the domain of anti-money laundering and terrorist financing. Contractual stipulations in this Section are in addition to the rules contained in these documents.

7.3 Where the contracting of Armed Protection services is being considered, the officer responsible for the management of security and safety shall endeavor to only contract private security service providers who are signatories to the International Code of Conduct for Private Security Service Providers (http://www.icoc-psp.org). In addition, the officer responsible for the management of security and safety shall seek to contract service providers who have already been vetted by other multi-lateral development banks and the United Nations Security Management System, and for the purposes of rapid contracting when required, to maintain a list of service providers who conform to the conditions of this Part. Where no such service provider is available, the officer responsible for the management of security and safety shall apply reasonable and sound professional judgement in appointing the service provider.

7.4 Any security service provider contracted for the provision of Armed Protection services must provide a current license for the provision of such services in the jurisdiction where the contract is to be performed if the laws of such jurisdiction require such services to be licensed.

7.5 The officer responsible for the management of security and safety shall ensure that all contracts which include provision for Armed Protection contain clauses reflecting the following:

7.5.1 Express statement that personnel of the service provider may be armed based on the risk assessment performed by the officer responsible for the management of security and safety. The officer responsible for the management of security and safety shall use their discretion based on their reasonable and sound professional judgement to determine if the service provider must declare the nature of Weapons to be used in the contract, or conversely, if the Bank shall specify the nature of Weapons to be used. Weapons for the purposes of this Part shall exclude large caliber, crew-served Weapons, normally associated with offensive and defensive operations conducted by military or para-military forces, and shall exclude chemical weapons listed under the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction of April 29, 1997, as amended.

7.5.2 Certification that personnel of the service provider who are to be armed in accordance with the contract, are adequately trained in the legal application of force and in the practical use all Weapons that will be used in the performance of the contract.

7.5.3 Description of the use of force policy of the service provider which must be consistent with, and no less stringent than, the principles and criteria set out in Section F (Use of Force) of this Part.

7.5.4 Express stipulation that when security and safety personnel of the Bank as defined in the Directive on Security and Safety (Part 2: Accountability) are present at the time when the use of force is being considered, such security and safety personnel shall determine the nature and extent of the force to be used. In the absence of security and safety personnel of the Bank, the decision will be taken by the private security

service provider according to their own rules of engagement or standard operating procedures, and their use of force policy.

7.5.5 The requirement for a written report within 72 hours to the officer responsible for the management of security and safety of any incident when a Weapon was used, or threatened to be used, in the performance of the contract with the Bank, irrespective of whether Deadly Force was employed or not.

7.5.6 Contracts with service providers shall contain language indicating that failure to comply with these contractual stipulations shall be considered a material breach of the contract that may result in termination of the contract.

7.6 The contracts with private security service providers contracted solely for unarmed services shall expressly state that Weapons are not to be used in the performance of the contact.

7.7 This Section does not apply to Armed Protection provided by Host Nations. In cases where security services, whether armed or unarmed, are provided by Host Nations, and when deemed necessary by the officer responsible for the management of security and safety, a private security service provider shall be contracted to provide a liaison officer to accompany the Bank Personnel to facilitate liaison between the Bank Travelers and the security forces of the Host Nation assigned to the task of protecting the Bank Personnel.

H. REPORTING AND COMPLIANCE CHECKING

8.1 Any Bank Personnel witnessing the use, or threat of use, of Weapons in the process of protecting them, Bank Premises or Assets, shall report such use to the officer responsible for the management of security and safety at the earliest opportunity. There is no specified format for reporting. A report shall be made irrespective of whether the protection was provided by Host Nation security authorities or a private security service provider.

8.2 The officer responsible for the management of security and safety shall report any use of force during the protection of Bank Personnel, Bank Premises and Assets to the Director General of the Facilities and Administration Services Department (DG FAS) as soon as reasonably possible with an update once the facts of the incident have been confirmed, and maintain records of such incidents.

8.3 The officer responsible for the management of security and safety shall randomly debrief Bank Personnel who were protected by **unarmed** security service providers while on mission to ascertain if any Weapons were used in the performance of the contracts for unarmed protection, and follow-up with the service provider and the Corporate Procurement Unit where non-adherence to contract requirements is found.

8.4 Similarly, the officer responsible for the management of security and safety shall randomly debrief Bank Personnel who were protected by **armed** security service providers while on mission to ascertain if compliance with the letter and spirit of this Part in the performance of the contract was observed, and report any concerns they may have regarding the carrying or use of Weapons. The officer responsible for the management of security and safety shall follow-up with the service provider and the Corporate Procurement Unit where non-adherence to contract stipulations is found, including any matters of concern not specifically covered under such contract stipulations.

8.5 At the discretion of DG FAS, further reports shall be made to senior management of the Bank.

I. EXCEPTIONS TO THE RULES FOR THE USE OF ARMED PROTECTION

9.1 In situations where Bank Personnel on a field mission fall under the protection of implementing partners or entities involved with a project, and such partners or entities have Armed Protection which was not known during the Travel Security Clearance Process, and where this protection is extended to Bank Personnel, advance authorization on the use of Armed Protection may not be possible. In such cases, the Bank Personnel involved shall accept the protection, but inform the officer responsible for the management of security and safety at the earliest opportunity and seek guidance on how to manage the situation.

9.2 In situations where advance assessments for the need for Armed Protection during the Travel Security Clearance process indicate that such protection is not required, but where the security situation deteriorates once the Bank Personnel involved arrive in the mission area to the extent that they become aware of a potential escalating threat, they shall inform the officer responsible for the management of security and safety, who shall make the required assessment and if deemed necessary, make arrangements for Armed Protection. This officer may also remotely initiate such assessments and arrangements.

9.3 Conversely, in situations where assessments during the Travel Security Clearance process indicated the requirement for Armed Protection but where this need is no longer required due to an improved security situation, the officer responsible for the management of security and safety shall reassess the requirement, and, if necessary, cancel or modify the arrangements for Armed Protection. This action may be initiated directly by the officer responsible for the management of security and safety, or prompted by the Bank Personnel involved who shall report such change in the situation to the officer responsible for the management of security and safety at the earliest opportunity.

9.4 In exceptional unforeseen situations where prior provision for Armed Protection was not made, but based on the reasonable and sound professional judgement of the officer responsible for the management of security and safety, the risk of death or injury to Bank Personnel is possible, the Contractual Stipulations in Section G may be set aside for the purposes of urgent provision of Armed Protection. Such cases shall be reported without delay to DG FAS who shall provide guidance whether to rectify the contractual arrangements *ex post facto*, or limit the involvement with the service provider to only the immediate and urgent requirement.

*****