COMMERCIAL INTERNATIONAL BANK KENYA
CCTV NOTICE

1. WHAT'S THE SCOPE OF THIS DOCUMENT?

Commercial International Bank Kenya (CIB Ke) is committed to the safety of its' staff, visitors and premises. We therefore use a closed-circuit television system ("CCTV") at our sites to achieve this purpose. The objective of this document is to set out how the CCTV system will be managed and used by the Bank and to inform individuals whose personal data may be captured on the CCTV system, about how and why that personal data may be processed by the Bank.

2. WHO COLLECTS THE INFORMATION?

CIB is the data controller of personal information collected about you. This means that we are responsible for deciding how we hold and use personal information about you and that we are required to notify you of the information contained in this Notice. It is important that you read this Notice so that you are aware of how and why we are using your personal information and how we will treat it.

3. COMPLIANCE

The Bank is aware that images of recognizable individuals, such as staff and site visitors, captured by the CCTV system constitute 'personal data', use of which is governed by data protection law.

CIB will ensure that its use of the CCTV system and the personal data that it captures complies with the law. This document has been drafted in accordance with the Data Protection laws and regulations of Kenya, industry best practices and global privacy standards such as the GDPR.

4. PURPOSE OF THE CCTV SYSTEM

The purpose of the CCTV system is:

a. To increase the personal safety of our staff and visitors to our sites.
b. To support our health and safety measures.
c. To assist in identifying, apprehending and prosecuting any offenders within the Bank's site.
d. To protect CIB buildings and assets and those of its staff from intrusion, theft, vandalism, damage or disruption.

The legal basis for the Bank's use of any personal data which is captured by the CCTV system is that the processing is necessary for the legitimate interests set out in this paragraph (provided that those interests are not overridden by individuals' rights and interests). The Bank may also need to use this personal data to establish, exercise or defend against legal claims.

5. YOUR RIGHTS

You have the right to exercise certain rights regarding the personal data collected through CCTV surveillance, including the right to access, rectify, erase, restrict processing, and object to processing.

Please note that the rights stated above are not absolute. While we strive to comply with all applicable data protection laws, there may be certain limitations or exceptions to the exercise of these rights. For example, we may be required to retain certain personal data to defend a legal action, comply with legal or regulatory requirements and hence the right to deletion may be declined.

To fulfill your request, we may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is a security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

For information on your specific rights and how to exercise them, please contact the Bank's Data Protection Officer via: dataprotection@cibke.com

6. OPERATION

CCTV cameras are located at strategic points on our sites, primarily access points, such as the gates to the sites, in office areas and in certain production areas. Signs are displayed prominently around the sites to inform staff and visitors that CCTV cameras are in operation and who to contact for further information. The cameras are in operation 24 hours a day, 7 days a week and they will be monitored from the Security Control Room. The security department manages all the footage from the CCTV cameras.

In addition, the bank has deployed cameras in all its Branches. These are monitored by the Operation Managers on site. The CCTV system is regularly maintained in accordance with the manufacturer's instructions. We also use a third-party service provider who regularly perform maintenance checks and confirm the efficiency of the system, including that the equipment is properly recording, that the cameras are functional, that the time and date are correct, and that the footage is being deleted or retained in accordance with this document.

7. SECURITY MEASURES

Physical protective measures: The Security Control Room can only be accessed with the correct access control privilege, which is primarily limited to security staff. A record is kept of all those who are given access to the Control Room.

Technical protective measures: We have put in place appropriate security measures to prevent personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. This includes ensuring CCTV hard drives are in a secured server room and access to this room is only via a formal approval process. Password protection, technical access control and the use of encryption are also technical protection measures that we use. We have put in place procedures to deal with any suspected personal data breach and will notify any affected individuals and/or the ODPC where appropriate.

8. ACCESS AND DISCLOSURE

Access to recorded CCTV footage is restricted to a limited number of security staff as authorised by the Security Operations Manager from time to time ("Authorised Persons") and all requests for disclosure of CCTV footage must be submitted to one of these Authorised Persons.
CCTV footage may only be accessed or disclosed to the extent necessary in order to deal with an incident which falls within the purpose identified above or in order to respond to a request made by an individual under the law. CCTV footage will not be accessed or used for any other purpose.
CCTV footage will be viewed in a secure office and any access to and any disclosures of recorded footage will be recorded in the CCTV log. This process is overseen by the Security Operations Manager and as appropriate, with reference to the relevant member of our Data Protection Committee. External disclosure of CCTV footage will usually not be permitted other than to law enforcement agencies or to regulators, or in order to comply with a court order. CCTV footage shall not be uploaded to the internet.

9. TRAINING

All staff who may be involved in the management or operation of the CCTV system will be trained on how to comply with this document and to ensure that the system is used in accordance with the law.

10. COVERT RECORDING

Covert recording will only be carried out in very limited circumstances and with the authorisation of our Head of Security and/or Data Protection Officer. Covert surveillance will only be carried out where specific criminal activity is suspected and where informing the relevant individuals would be likely to prejudice the prevention of crime and/or apprehension/prosecution of the offender.

Any authorisation to use covert recording will be documented in writing and include confirmation that it is required to obtain evidence of suspected criminal activity in a specific case, an assessment of the

alternative methods of obtaining the evidence and the permitted duration of the covert recording. The authorisation will be regularly reviewed, for example, every 28 days, to assess whether it is continued to be required or should cease.

11. CHANGE OF PURPOSE

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will usually notify you and we will explain the legal basis which allows us to do so.

12. DISCLOSURE OF YOUR INFORMATION

We may share your personal information with the third parties set out below for the purposes described above:

a. service providers (generally based in Kenya) such as those who provide IT and system administration services
b. if we are under a duty to disclose or share your personal information in order to comply with any legal obligation), or in order to enforce or apply our contract with you
c. in the event that we sell or buy any business or assets, in which case we may (where relevant) disclose your personal information to the prospective seller or buyer
d. if we, or substantially all of our assets, are acquired by a third party, in which case personal information held by us will be one of the transferred assets
e. to protect the rights, property or safety of us, our customers and others. This includes exchanging information with other organisations such as fraud and theft prevention agencies for the purposes of reducing credit risk, fraud and theft.

Third Parties: We require all service providers that we share your personal information with to respect the privacy and security of your personal information and to treat it in accordance with the law. We do not allow our third-party service providers to use your personal information for their own purposes and only permit them to process your personal information for specified purposes and in accordance with our instructions.
As part of our Third-Party Privacy Onboarding policy, we carry out due diligence on our third-party providers and assess whether your personal information will be transferred to them or accessed by them from outside Kenya. If that is the case, we ensure a similar degree of protection is afforded to it.

Location of your data: All the personal information we collect about you is based in Kenya.

13. INFORMATION RETENTION

The images captured by the CCTV System will not be stored for any longer than is required to achieve the purposes identified above. CCTV footage will automatically be deleted on a 30-day rolling basis, unless specific images are required in order to deal with an incident or in order to respond to a request by an individual made under the law (see further below).

14. CHANGES TO THIS PRIVACY NOTICE

We reserve the right to update this Notice at any time, and we will provide you with a new Notice when we make any material change.

15. CONTACTING US

If you wish to make an individual rights request, or you are a law enforcement or government organisation wishing to make an enquiry, please visit our secure website.

Any queries or complaints about the CCTV system should be addressed to the Security Operations Manager via email to dataprotection@cibke.com