1. INTRODUCTION

1.1. In recent years, information has increasingly become a critical resource that has to be managed carefully. Generally, much of today's information consists of personal data relating to individuals. Kenya like other countries has been experiencing technological growth that has impacted the way personal data is generated, processed, stored and distributed. Kenya acknowledges the importance of accessing information and safeguarding it as articulated in the Constitution of Kenya 2010. As a result, the transformative developments in computing are presenting major concerns for privacy in the way information is processed.

1.2. As a modern, forward-looking business, Orbit Capital Limited (hereinafter "the Company") recognizes at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customer, shareholders and other stakeholders.

2. POLICY STATEMENT

2.1. This Policy is intended to provide minimum standards with respect to the protection of personal data that is collected, received, processed and stored on Company owned physical and electronic databases. and will cover the use of personal data about all individuals, including employees, customers and other third parties, that deal with Company. It shall apply to all users of the Company's applications, software, databases, websites, social media platforms and all other suchlike resources.

2.2. This Data Protection Policy is available in both paper and electronic form and will be communicated within the organization and to all relevant stakeholders and interested third parties.

3. GOVERNANCE AND AUDIT

3.1. The Constitution of Kenya 2010 and the Data Protection Act, 2019 are the most significant pieces of legislation affecting the Company. Significant fines are applicable if a breach is deemed to have occurred under the legislation designed to protect the privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold, use or disclose personal information and for related matters. It is the Company's policy to ensure compliance with the Data Protection Act and other relevant legislation is clear and demonstrable at all times.

3.2. In collecting and using this data, the Company is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

4. APPLICABLE REGULATIONS

4.1. The Data Protection Act No. 24 of 2019 (the "DPA").

4.2. The Kenya Information and Communications Act, 1998.

4.3. The Data Protection (General) Regulations, 2021.

4.4. The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021;

4.5. The Data Protection (Compliance and Enforcement) Regulations, 2021; and

4.6. Any other relevant Kenyan data protection laws.

5. DEFINITIONS

The main terms used in this Policy are defined in Appendix A of this Policy.

6. POLICY GUIDELINES

6.1. The Company shall in dealing with personal information and data ensure that the information/ data is processed:

a) without infringing the privacy rights of the data subject;

b) in a lawful manner; and

c) in a reasonable manner.

6.2. Collection, use, storage and transfer of personal data will only be done in a manner guided by the fundamental principles of the Company.

6.3. The data shall be collected for purposes of decision making and provide an idea of the financial integrity and credit worthiness of the client(s).

7. ACCURACY

7.1. The Company shall store personal data/information as accurately as possible and update and systematically review it to ensure it fulfills the purpose(s) for which it is processed.

7.2. The data subject may request the correction of personal data that is inaccurate, incomplete, unnecessary, or excessive.

7.3. When personal data is corrected, the Company will notify, as soon as is reasonably practicable to the data subject.

8. DATA COLLECTION

8.1. When collecting personal data from the user, the Company shall inform the user of the following in writing/orally and in a manner and language that is understandable to the user:

a) The specific purpose(s) for which the personal data or categories of personal data will be processed.

b) Whether such data will be transferred to third parties and the specific third parties.

c) The data subject's right to request access to their personal data, or correction or deletion of it.

d) How to lodge a complaint with the data controller.

e) The mandate and contact details of the data controller.

8.2. Where data is not collected directly from the data subject either electronically, orally or in writing, other means will be considered as far as is practicable such as online postings and any other appropriate method of transmission.

8.3. At the request of the data subject the data controller may restrict the processing of personal data where:

a) The accuracy of the data is contested by the data subject.

b) The data subject has objected to the processing.

9. TYPE OF INFORMATION COLLECTED

9.1. The Company will collect and hold personal client information either electronically or written in a language they can understand for its operational purposes. This may include:

a) Contact details such as name address, email address and phone numbers.

b) Nationality

c) National ID and Passport information

d) Date of birth

e) Gender

f) Information about race and ethnicity

g) Bank account details and all financial records

h) Pay slip details

i) Employment details

j) Tax and residency status for statutory requirements

k) References from employers

l) Contact details for family members and next of kin

m) Details of criminal convictions (where necessary)

9.2. The Company will ensure that the customer is notified of collection of personal data before being prompted to provide the said data.

10. REASONS FOR DATA COLLECTION

Personal data can be processed only for the purpose that was defined before the data was collected. Subsequent changes to the purpose are only possible to a limited extent and require substantiation. The Company shall in the collection of personal data only collect such customer information as is reasonably required for a customer's credit appraisal, approval, disbursement and collection. The Company shall also ensure that the data collected is not intrusive or collected for other reasons apart from the specific appraisal exercise. The Company shall give due regard when processing sensitive

personal data relating to deposits, subscriptions, billing statements, withdrawals and mobile money transactions.

11. PROCESSING OF PERSONAL DATA RELATING TO A CHILD

11.1. The Company shall not process personal data relating to a child unless—

(a) consent is given by the child's parent or guardian; and

b) the processing is in such a manner that protects and advances the rights and best interests of the child.

11.2. The Company shall incorporate appropriate mechanisms for age verification and consent in order to process personal data of a child. The mechanisms shall be determined on the basis of available technology, volume of personal data processed, proportion of such personal data likely to be that of a child and the possibility of harm to a child arising out of processing of personal data.

12. TRANSPARENCY

The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be aware of, or informed of:

a) The identity of the Data Controller.

b) The purpose of data processing.

c) Third parties or categories of third parties to whom the data might be transmitted, if any.

13. RETENTION PERIOD OF INFORMATION

13.1. The Company will only retain the Customers personal data for as long as reasonably necessary to fulfil the purposes the Company collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements.

13.2. The Company may retain the Customer's personal data for a longer period in the event of a complaint or if the Company reasonably believes there is a prospect of litigation in respect to our relationship with the Customer.

13.3. To determine the appropriate retention period for personal data, the Company considers the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of the Customer's personal data, the purposes for which the Company processes the Customer's personal data and whether the Company can achieve those purposes through other means, the need to comply with the Company's internal policy and the applicable legal, regulatory, tax, accounting or other requirements.

13.4. The Company shall delete, erase, anonymise or pseudonymise personal data not necessary to be retained under clause 13.1 in a manner as may be specified at the expiry of the retention period. Anonymized information that can no longer be associated with the Customer may be held indefinitely.

13.5. The Company shall keep a data inventory for purposes of data retention. The duration of retention of personal data shall be determined by:

i. Requirements of national and county legislation.

ii. The lawful purpose for retaining the data.

iii. Authorisation or consent by a customer.

14. SAMPLE DATA RETENTION TABLE TO BE USED BY THE COMPANY SHALL INCLUDE:

Record Type	Retention Period	Disposition
Byline lists	Permanently	Archive
Camera footage	Permanently	Archive
Customers personal data	Permanently	Archive
Clip libraries	Permanently	Archive
Website Articles	Permanently	Archive
ePaper Materials	Permanently	Archive
Press releases	Permanently	Archive
Social media posts	Permanently	Archive
Website analytics	Permanently	Archive
Active user login details	Permanently	Shred/encrypt user data after 7 years of inactivity

15. LAWFUL AND FAIR PROCESSING

15.1. Data processing shall be carried out in a lawful and fair manner for specified and legitimate purposes without prejudicing the fundamental rights and freedoms of data subjects. The processing relates to personal data that has been made public by the data subject.

15.2. Processing is necessary for the lawful purposes:

a) data subject giving his or her consent.

b) the processing is necessary for the performance of a contract with the data subject.

c) to meet legal compliance obligations.

d) to protect the data subject's vital interests or any other person who may be indirectly affected.

e) public interest.

f) to pursue the Company's legitimate interests which are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects.

16. FACTAUAL ACCURACY; UP-TO-DATE DATA

Personal data on file must be correct, complete, and – if necessary – kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented, or updated within 7 days.

17. FURTHER PROCESSING

17.1 Further processing for research purposes shall be compliant with the conditions outlined to be compatible with the purposes for which the data is obtained.

17.2 Personal data which is processed for research purposes may be exempt from provisions of this policy if the results of the research and statistical data is not made available in a form which identifies the data subject.

17.3. Further processing of data shall comply with the data protection principles set out in this policy, in particular in ensuring the security and confidentiality of sensitive personal data.

18. CONFIDENTIALITY

18.1. The confidentiality of personal data must be always respected by the Company when processing data with access to the same limited on a need-to-know basis.

18.2. The Company shall maintain the confidentiality of the personal data throughout and even after the user is no longer of concern to the Company.

18.3. The data controller may specify other categories of personal data that will require additional safeguards and restrictions and may be classified as sensitive personal data.

18.4. In the processing of sensitive personal data, the data controller will specify further grounds on which these categories will be processed with consideration of:

a) the increased risk of significant harm that may be caused to the data subject by processing this category of personal data

b) the degree of confidentiality attached to the category of personal data.

c) the level of protection afforded by provisions applicable to personal data.

19. ACCESS TO PERSONAL DATA

19.1. The following rights shall be exercisable by a customer in relation to their personal data held by the Company:

i. Right to be informed of the use to which personal data is to be put.

ii. Right to access personal data in the custody of the Company.

iii. Right to data portability a customer shall have the right to receive their personal data in a structured and machine-readable format. The Company shall provide the data in printed format or in PDF format.

iv. Right to object to the processing of all or part of personal data.

v. Right to restriction of processing of personal data where the Company may at the request of a customer restrict the processing of personal data where:

a) accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the data;

b) personal data is no longer required for the purpose of the processing, unless the data controller or data processor requires the personal data for the establishment, exercise, or defence of a legal claim;

c) processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; or

d) data subject has objected to the processing, pending verification as to whether the legitimate interests of the data controller or data processor overrides those of the data subject.

vi. Right to correction of false or misleading data.

vii. Right to deletion of false or misleading data.

viii. Right to file a complaint to the Data Commissioner where a customer is aggrieved by a decision by Company relating to their personal data.

ix. Right to representation shall be exercised when such a right conferred to a data subject in the case of a minor, may be exercised by a person with parental authority or by a guardian.

x. Where a customer has a mental or other disability, another person may be authorized to act as their guardian or administrator.

xi. A customer may also authorize any personal to act on their behalf.

20. DATA SUJECT ACCESS REQUESTS

20.1. Anybody who makes a request to see any personal data held about them by the Company will be making a Data Subject Access Request. All data relating to the individual, including that held in electronic or manual files should be considered for disclosure.

20.2. The Data Subject Access Request will be to enable a data subject to establish:

i. whether personal data about him or her is being processed;

ii. the purposes of the processing;

iii. the categories of personal data concerned;

iv. the recipients or categories of recipients to whom their personal data have been or will be disclosed;

v. the envisaged period for which the data will be stored or where that is not possible, the criteria used to determine how long the data are stored;

vi. the existence of a right to request rectification or erasure of personal data or restriction of processing or to object to the processing;

vii. where the personal data are not collected from the individual, any available data as to their source; and

viii. details of the safeguards in place for any transfers of their data to locations outside Kenya.

20.3 All Data Subject Access Requests shall be sent to the Data Protection Officer who shall be appointed within 90 days from the date of the issuance of the DCP License and must be dealt with in full without delay and at the latest within one (1) month of receipt. The Company may extend the time to respond by a further one (1) month if the request is:

20.3.1. complex; or

20.3.2. The Company has received a number of requests from the individual.

20.4 Where a child does not have sufficient understanding to make his or her own request (usually those under the age of eighteen (18) a person with parental responsibility can make a request on their behalf. The Data Protection Officer must, however, be satisfied that:

20.4.1 the child lacks sufficient understanding; and

20.4.2 the request made on behalf of the child is in their best interest.

20.5 Any individual, including a child with full understanding of their rights, may appoint another person to request access to their records. In such circumstances the Company must have written evidence that the individual has authorized the person to make the application on their behalf and the Data Protection Officer must be satisfied by the identity of the individual making the request and of the authorization of the individual to whom the request relates.

20.6 Access to records will be denied in exceptional circumstances, for example, data sharing may place the individual at risk of significant harm or jeopardize police investigations into any alleged offence(s). In such circumstances, the Data Protection Officer shall inform the data subject of the reasons for the denial of a request within reasonable timelines and shall not unreasonably deny an access request without justifiable reasons.

20.7 A Data Subject Access Request must be made in writing. The Company may ask for any further data reasonably required to effectively respond to a Data Subject Access Request.

20.8 An individual only has the automatic right to access data about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the data.

Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

20.9 All files must be reviewed by the Data Protection Officer or in the lack thereof, by a person(s) duly authorized to access and review personal data before any disclosure takes place. Access will not be granted before this review has taken place. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured, redacted or extracted. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

20.10 A data subject shall have the right to receive their personal data concerning them in a structured, commonly used and machine-readable format.

21. DATA SECURITY

21.1 The Company will ensure and implement a high level of data security that is appropriate to the risks presented by the nature and processing of personal data taking into account the level of technology available and existing security conditions as well as the costs of implementing additional security measures.

21.2. In order to ensure and respect confidentiality, personal data will be filed and stored in a way that is accessible only to authorized staff and transferred only through the use of protected means of communication.

21.3. In order to ensure the confidentiality of the personal data, the Company shall take appropriate technical and organizational data security measures.

21.4. The nature of risks will include but not be limited to risk of accidental or unlawful/illegitimate destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

21.5. Access to personal data/content/knowledge shall be restricted to authorized personnel using it in the performance of their duties and as determined by appropriate authorization of both the employees, supervisor and data subjects.

21.6. Personal data/content/knowledge may not be used by any employee for purposes other than the business of the Company.

21.7. Staff and volunteers allowed access of personal data/content/knowledge of the Company shall sign a non-disclosure agreement banning them from using the content for business other than the Company's core mandate.

21.8. Private email accounts shall not be used to transfer Personal Data.

21.9. Information technology will be used to process, communicate and store Company data and information which will be classified as Confidential Information (CI).

21.10. Data security measures will be routinely reviewed and upgraded as deemed appropriate to ensure the level of protection is commensurate to the degree of sensitivity applied to personal data and considering the possible development of new technology in enhancing data security.

22. DISCLOSURE OF INFORMATION

22.1. Any disclosure of the Customer's information shall be in accordance with applicable law and regulations. The Company shall assess and review each application for information and may decline to grant such information to the requesting party.

22.2. The Company may disclose your information to:

22.2.1. Law-enforcement agencies, regulatory authorities, courts or other statutory authorities in response to a demand issued with the appropriate lawful mandate and where the form and scope of the demand is compliant with the law;

22.2.2. Its subsidiaries, associates, partners, software developers or agents who are involved in delivering the Company's products and services the Customer orders or uses;

22.2.3. Fraud prevention and Anti money laundering agencies, credit- reference agencies;

22.2.4. Publicly available and/or restricted government databases to verify the Customer's identity information in order to comply with regulatory requirements;

22.2.5. Debt-collection agencies or other debt-recovery organizations;

22.2.6. Survey agencies that conduct surveys on behalf of the Company; and

22.2.7. Any other person that the Company deem legitimately necessary to share the data with.

22.3. Some of the Customer's information may be passed on to any person whom you receive mobile money from or send or intend to send mobile money to. The Customer's information may be available to any third party involved in the operation of the mobile money service including Telecommunication Providers, mobile money interoperability partners and ATM Switch providers.

22.4. The Company shall not release any information to any individual or entity that is acting beyond its legal mandate.

22.5. The Company will get the Customer's express consent before the Company shares the Customer's personal data with any third party for direct marketing purposes.

23. BREACH NOTIFICATION

23.1. In the event of breach of Customer's data, the Company shall contact the Customer's resource person in the next 48hrs. This will be managed in accordance with our Incident Response Mechanism which sets out the overall process of handling information security incidents.

23.2. The Company may however delay or restrict communication referred to under subsection (1)(b) as necessary and proportionate for purposes of prevention, detection or investigation of an offence by the concerned relevant body.

23.3. The Company will maintain a register of all data breaches and the records shall include: the facts relating to the breach; its effects; and the remedial action taken.

23.4. The Company employees will notify their supervisors as soon as possible upon becoming aware of a personal data breach.

23.5. If a personal data breach is likely to result in personal injury or harm to a data subject, the data controller will communicate the personal data breach to the data subject and take mitigating measures as appropriate without undue delay. In such cases, the data controller shall also notify the Secretary General of the personal data breach.

23.6. The notification will describe:

a) description of the measures that the Company or intends to take or has taken to address the data breach;

b) recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise;

c) where applicable, the identity of the unauthorized person who may have accessed or acquired the personal data; and

d) the name and contact details of the data protection officer where applicable or other contact point from whom more information could be obtained.

24. COMPLAINT HANDLING MECHANISM

24.1. Any person/s may lodge a complaint in their own name or on behalf of another person against the Company or staff in respect of a service rendered by the Company or staff of the Company.

24.2. The complaint may be lodge by an individual complainant or a group or institution acting on behalf of a complaint; or anonymously.

24.3. All complaint shall be received and processed free of charge by the Company.

24.4. A data subject or any person aggrieved on any matter may lodge a complaint with the Data Protection Officer.

24.5. A complaint may be lodged in writing through electronic means, including email, web posting, complaint management information system; or by any other appropriate means.

24.6. The Data Protection Officer shall acknowledge receipt of the complaint within seven (7) days of receipt of the complaint.

24.7. The Data Protection Officer shall keep and maintain an up to date Register of Complaints. An entry into the register of complaints shall state the particulars of the complainant and the complaint filed with the Data Protection Officer.

24.8. The Data Protection Officer shall protect the identity of the complainant where the request to protect the identity is sought by the complainant.

24.9. The Data Protection Commissioner shall review, carry out an investigation where necessary and advice the complainant in writing accordingly within seven (7) days and shall provide the complainant with sufficient reasons and guidance on any steps taken or to be taken to address or resolve the complaint together with reasonable timelines.

24.10. Where a complainant is dissatisfied with the advice, response and measures to be taken by the Data Protection Officer and the Company, the Complainant may proceed to lodge a formal complaint with the Office of the Data Protection Commissioner in accordance with the procedures laid down under the Data Protection Act, 2019 and the relevant regulations thereto.

25. DISCIPLINARY ACTIONS

Employees of the Company are mandated to conform to this policy. Failure to comply shall result in disciplinary actions as stated in the Company's HR processes.

26. DISASTER RECOVERY PLAN

26.1. The Disaster Recovery Plan is maintained by the Company's Security Officer and Privacy Officer.

26.2. The objectives of the plan are to maximize the effectiveness of contingency operations through an established plan that consists of the following phases:

26.2.1. **Notification/Activation phase** to detect and assess damage and to activate the plan.

26.2.2. **Recovery phase** to restore temporary operations and recover damage done to the original Database.

26.2.3. **Reconstitution phase** to restore Database processing capabilities to normal operations.

26.3. Identify the activities, resources, and procedures needed to carry out processing requirements during prolonged interruptions to normal operations.

26.4. Identify and define the impact of interruptions to the Company's Databases.

26.5. Assign responsibilities to designated personnel and provide guidance for recovering the Company's Databases during prolonged periods of interruption to normal operations.

26.6. Ensure coordination with other staff who will participate in the Disaster Recovery Planning strategies.

26.7. Ensure coordination with external points of contact and vendors who will participate in the Disaster Recovery Planning strategies.

27. TRANSFERRING PERSONAL DATA TO THIRD PARTIES

27.1. In order to mitigate risks associated with transfer of data to third parties, the Company will only transfer data to a third party if:

a) The data is stripped off personal and identifiable information;

b) The transfer is based on one or more legitimate basis including:

i. explicit consent by the data subject;

ii. compliance with national or international law; or

iii. in exercise, establishment and defense of any contractual or legal obligations.

c) The personal data to be transferred is adequate, relevant, necessary and not excessive in relation to the purpose(s) for which it is being transferred; The data subject has been informed either at the time of the collection or subsequently, about the potential transfer of his/her personal data.

d) The third party maintains a high level of data security that protect personal data against the risk of accidental or unlawful/illegitimate destruction, loss, alteration unauthorized disclosure of, or access to it.

27.2. The Company will also ensure that transferring personal data does not negatively impact:

a) The safety and security of Company employees and beneficiaries.

b) The effective functioning of an operation or compromise in the Company's mission, vision or fundamental principles, for example due to the loss of trust and confidence between the Company and persons of concern.

27.3. The processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards.

28. DATA TRANSFER RECORDS

28.1. The Company shall keep and maintain full and accurate records reflecting all phases of data management cycle, including records of data subjects' consents and procedures for obtaining consent, where consent is the legal basis of processing.

28.2. The data transfer records shall include, at a minimum:

a) the name and contact details of the individual entity authorizing the transfer;
b) clear descriptions of the personal data types;

c) data subject types;

d) processing activities;

e) processing purposes;

f) third-party recipients of the personal data;

g) personal data storage locations;

h) personal data transfers;

i) the personal data's retention period; and

j) a description of the security measures in place.

29. DATA TRANSFER AGREEMENTS

29.1. the Company will require all third parties to comply with this Policy through an agreement or an MOU as part of the signing of partnership agreements. Such agreements will specify the specific purpose(s) and legitimate basis for the processing or transfer of personal data.

29.2. Data transfer agreements shall;

a) address the purpose(s) for data transfer, specific data elements to be transferred as well as data protection and data security measures to be put in place;

b) require the third party to undertake that its data protection and data security measures are in compliance with this Policy; and

c) stimulate consultation, supervision, accountability and review mechanisms for the oversight of the transfer for the life of the agreement.

29.3. Company Legal Representatives shall review and approve all data transfer agreements and maintain copies of final agreements.

30. TRAINING AND AWARENESS

The Company will train staff on the contents and implementation of this policy. Staff who join the Company will be required to go through an induction process that entails familiarization with this policy. The Company will ensure that the requirements of this policy form part of its agreement with its grantees, contractors and third parties who process the Company's data.

31. DISASTER RECOVERY PROCEDURES

In accordance with the Company's information and security incident response procedure:

a. Notification and Activation Phase

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption. Based on the assessment of the Event, sometimes according to the Incident Response Policy, the Disaster Recovery Plan may be activated by the Security Officer and/or Chief Technology Officer (CTO) (The CTO shall be appointed within 90 days following the issuance of the DCP License).

b. The notification sequence is listed below

i. The first responder is to notify the CTO. All known information must be relayed to the CTO.

ii. The CTO is to contact the rest of the team and inform them of the event. The CTO is to begin assessment procedures.

iii. The CTO is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed locally because of unsafe conditions, the CTO is to follow the steps below.

c. Damage Assessment Procedures

The CTO is to logically assess damage, gain insight into whether the infrastructure is salvageable, and begin to formulate a plan for recovery.

d. Alternate Assessment Procedures

i. Upon notification, the CTO is to follow the procedures for damage assessment with combined DevOps and Web Services Teams.

ii. The Disaster Recovery Plan is to be activated if one or more of the following criteria are met:

a) Databases will be unavailable for more than 48 hours.

b) Hosting facility is damaged and will be unavailable for more than 24 hours.

c) Other criteria, as appropriate and as defined by the Company.

e. If the plan is to be activated, the CTO is to notify and inform team members of the details of the event and if relocation is required.

f. Upon notification from the CTO, group leaders and managers are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.

g. The CTO is to notify the hosting facility partners that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.

h. The CTO is to notify remaining personnel and executive leadership on the general status of the incident.

i. Notification can be delivered via message, email, or phone.

32. EFFECTIVE DATE

The policy shall come into effect on 1st October 2024. It will remain in force until an updated version of the policy is approved and effected.

APPENDIX A: Definitions of key terms

Anonymization: Irreversible removal of personal identifiers from information so that the data subject is no longer identifiable.

Collection: The act of gathering, acquiring, or obtaining Personal Data from any source, including third parties and whether directly or indirectly by any means.

Consent: Any freely given specific and informed indication of the wishes of the data subject by which they signify their agreement to personal data relating to them being processed.

Control: An agency, natural or legal person, public authority, organization or any other body which alone or jointly with others has the power to determine the purposes and means of the processing of data, and the manner in which the data is processed.

Critical system: Any system whose 'failure' could threaten human life, the system's environment or the existence of the organization which operates the system. Such systems include but not limited to electric grid, manufacturing system, transportation system, financial institutions, water treatment facilities and water supply systems.

Data: All data including personal data in electronic or manual form.

Data controller: A person who either alone or jointly with other persons or in common with other persons or as a legal duty determines the purpose for and the manner in which data is processed or is to be processed.

Data Processor: In relation to personal data, any person (other than an employee of the data controller) who processes the data on behalf of the data controller

Data Subject: A Natural person whose personal data is held by the data controller.

Disclosure: Making data available to others outside the Agencies

Encryption: The process of converting information or data into code, to prevent unauthorized access

Investigation — means an investigation relating to:

a) A breach of this policy;

b) A contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

c) A circumstance or conduct that may result in a remedy or relief being available under any law.

National Interest — includes national security, defense, public security, the conduct of international affairs and the financial and economic interest of Kenya;

Notification: Notifying the Data Protection Regulator/Data Subject about the data breach.

Office of the Data Protection Commissioner: An independent public authority established by state to regulate compliance with data protection law by Data Controllers and Processors and take enforcement action in the case of non-compliance.

Personal data: Any information relating to an identified or identifiable natural person (Data Subject) an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, passport number, birth certificate or to one or more specific factors like physical or physiological.

Processing: Any operation performed on personal data, such as collecting, creating, recording, structuring, organizing, storing, retrieving, accessing, using, seeing, sharing, communicating, disclosing, altering, adapting, updating, combining, erasing, destroying or deleting personal data, or restricting access or changes to personal data or preventing destruction of the data.

Restriction of processing: The marking of stored personal data with the aim of limiting their processing in the future.

Pseudonymization: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable person. Pseudonymized data is therefore re-identifiable and falls within the definition of personal data

Sensitive personal data means personal data as to:

a) The racial, ethnic or social origin,
b) The political opinions or the religious or conscience belief, culture dress language or birth) of the data subject.
c) Gender
d) Whether the data subject is a member of a trade-union.
e) disability
f) Sexual life or orientation
g) Pregnancy
h) Colour
i) Age
j) Marital status
k) Health Status
l) the commission or alleged commission of any offence by the data subject, or
m) Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.
n) Biometrics (where needed for identification).

Third Party-Third party, in relation to personal data, means any person/entity other than the data subject, the data controller, or data processor or other person authorized to process data for the data controller or processor.