2021

Privacy Policy

sewa assets

SEWA ASSETS MANAGEMENT LIMITED PRIVACY POLICY

1. **Introduction**

   This Privacy Policy gives you a clear view of how we use personal information that you provide, our dedication to protecting it and your rights and the options you have to control your personal information and protect your privacy. It also outlines what personal information we collect about you when you visit our website, speak to our support staff, or investment experts and how we use your personal information. It also sets out how to contact us if you have any questions about this privacy policy or want to make a complaint to us about how we handle your personal information.

2. **What information do we collect about you?**

   The personal data that we collect, and process may include:

   2.1 basic information such as name, date of birth, employer, title, age, relationship affiliations with a person or organization.
   2.2 contact information such as physical address, email address, fax and telephone.
   2.3 technical information (including your IP address): Information obtained from a visit to our website.
   2.4 payment details.
   2.5 confidential information generated by us in the course of providing our services.
   2.6 details relating to your visits to our offices; and/or
   2.7 any other information relating to you which you may provide to us.

   Sewa Assets Management Limited (SEWA) will only collect information that is necessary for the provision of the product or service that you have subscribed to. The type of information collected will depend on the nature of the product or service demanded.

3. **How we protect your personal Information**

   We are committed to protecting your personal information and implementing appropriate technical and organizational security measures to protect it against any unauthorized or unlawful processing and against any accidental loss, destruction or damage.

   Our security policies are attached as Schedule 1 to this Privacy Policy in our **Information Security Policy**

4. **How we use your Personal information**

   We will only use your personal information if and to the extent that applicable law allows.

4.1 Processing your transaction: we use relevant personal information described above to process and deliver your transaction and to notify you of the status of your transaction.

4.2 Ability to proceed with an offer on our products or services: We will process your personal information for the purposes of our legitimate interests in determining your ability to proceed with a transaction or agreement so that we have an informed choice should there be an offer. This also has the potential to speed up any subsequent transaction.

4.3 To engage with you in relation to our products and services: we will use your personal information to provide you with the products and services you have requested from us, to conduct market research surveys, for statistical analysis to determine application usage and for direct marketing purposes relating to our business. We will process your personal information in this way if it is necessary for the performance of the contract with us.

4.4 To do all things necessary to comply with our customers' instructions and our legal obligations to our customers and in compliance with privacy legislations such as GDPR and NDPR.

We will therefore only process your personal information if:

i. you have given your consent (where necessary) to such use or the organization you work for has obtained your consent (where necessary) to share your information with us; or

ii. if we have a legitimate interest which is not overridden by your interests or your rights and freedoms.

If you have given us your express consent, we may process your personal data for additional purposes. **Please note that you may withdraw your consent at any time you may so wish.**

5. If you fail to provide personal data?

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with our products or services). In this case, we may have to cancel a product or service you have with us, but we will notify you if this is the case at the time.

6. How is your personal data collected?

We use different methods to collect data from and about you including through:

6.1 **Direct interactions.** You may give us your identity, contact and financial data by filling in forms or by corresponding with our support staff by post, phone, email or otherwise. This includes personal data you provide when you:

6.1.1 apply for our products or services.
6.1.2 create an account on our website.
6.1.3 subscribe to our service or publications.
6.1.4 request marketing to be sent to you.
6.1.5 enter a competition, promotion or survey or
6.1.6 give us feedback or contact us.

7. **Sharing your personal data**

Irrespective of how we obtain your personal data, it may be shared among all our offices as may be found on our website. All our offices will always ensure at least a standard level of data protection is always in place. Where we share your personal data with third parties, we will do this in accordance with applicable data protection laws and will take appropriate safeguards to ensure its protection. Your personal information may also be transferred to countries or jurisdictions which may not provide the same level of data protection as us. If we do make such a transfer, we will, if appropriate, put a contract in place that imposes obligations on our counterparties to protect your information.

8. **Marketing**

We would like to send you information about our products and services and special offers which may be of interest to you. Where we have your consent or it is in our legitimate interests to do so, we may do this by post, email, telephone, text message (SMS) or automated call. We will only ask whether you would like us to send you marketing messages when you tick the relevant boxes. If you have previously agreed to being contacted in this way, you can unsubscribe at any time by contacting us at Sewa Assets Management Limited, 6th Floor, Right Wing Ibukun House, 14, Adetokunbo Ademola Street, Victoria Island, Lagos or by using the 'unsubscribe' link in emails or 'STOP' number in texts.

9. **Retaining your personal data**

We will only retain your personal information for as long as is necessary for the purpose for which it was collected, including for the purposes of complying with any legal, regulatory, accounting or reporting requirements. We will delete your personal data when it is no longer reasonably required for the authorized uses or you withdraw your consent (whichever is applicable), provided that we are not legally required or otherwise authorized to continue to hold such data.

10. **Your rights**

In addition to your rights under applicable data protection legislation and where we are authorized or required by applicable law and by our professional obligations, we will provide you, upon request, with a copy of your personal data and we will correct any errors identified by you. Except as provided above, we will not use your data for any automated decision making or any profiling. You also have the right to withdraw your consent for a specific processing at any time. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

11. **Opting out**

You can ask us to stop sending you marketing messages at any time [by logging into the website and checking or unchecking relevant boxes to adjust your marketing preferences **OR** by following the opt-out links on any marketing message sent to you **OR** by contacting us at any time].

Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of [a product/service purchase, warranty registration, product/service experience or other transactions].

You are entitled to remedies for breach of your rights and the NDPR as stated in Schedule 2 to this Privacy Policy titled **PERSONAL DATA BREACH & INCIDENT HANDLING PROCEDURE**

12. **Other websites**

Our website may contain links to other websites. This Privacy Policy only applies to this website so when you link to other websites you should read their own privacy policies.

13. **Changes to our Privacy Policy**

We keep our Privacy Policy under regular review and we will place any updates on this web page. This Privacy Policy was last updated in July 2021.

If you would like to exercise any of these rights, please contact us by emailing m.nwogu@sewaassetsmanagement.com and info@sewaassetsmanagement.com

SCHEDULE 1
SEWA ASSETS MANAGEMENT LIMITED INFORMATION SECURITY POLICY

PURPOSE
The purpose of Information Security for Sewa Assets Management Limited ("SEWA or the Company") is to protect the Company's information assets, regardless of whether these are held in manual or electronic form. This will help to safeguard the reputation of the Company, to optimize the management of risk and to minimize the impact of Information Security incidents. Implementation of this Policy will provide assurance to stakeholders, partners and data subjects, that their information is held securely and used appropriately by the Company, whilst complying with the General Data Protection Regulation (GDPR) and Nigerian Data Protection Regulation (NDPR) and satisfying auditors. Further, it is a key enabler for information sharing through enhanced controls e.g., supporting access channel strategy, business continuity planning, citizen focused services, first contact deployment and flexible working.

POLICY DEFINITION
According to the NDPR, anyone involved in data processing or the control of data shall develop security measures to protect data these measures will include ensuring that information is only available to those that are authorized to gain access, safeguarding the accuracy and completeness of information and processing methods, and assurance that authorized users have access to information and associated assets when this is required.

Information takes many forms. It may be processed and stored on computers or in other electronic form, printed or written on paper, shared through voice or video communications, transmitted through post or electronic means such as e-mail or fax, made available on corporate videos or web sites. Whatever form the information may take, or means by which it is shared, stored or processed, it should always be appropriately classified and protected according to that classification.

Information systems and the information they process and store are a vital asset to the Company. Any loss of computer systems or the information they contain could have serious repercussions for the Company and/or its clients. A breach of security during processing, storage or transfer of data could result in financial loss, personal injury to a member of staff, or client, serious inconvenience, embarrassment, or even legal proceedings against the Company, and possibly the individuals involved. In order to ensure the confidentiality, integrity and availability of these systems an appropriate level of security must be achieved and maintained. The level of security implemented on each of the various systems will be consistent with the designated security classification of the information and the environment in which it operates.

Information on computer systems will be protected with anti-virus software, which will be updated regularly. Scans will be carried out regularly on all servers, workstations and laptops, and virus definitions will be updated each weekday. Updates and scans will be automatic for every machine and must not be turned off or bypassed.

The Company will take appropriate steps to prevent, detect, and recover from any loss or incident, whether accidental or malicious, including error, fraud, misuse, damage and disruption to, or loss of computing or communications facilities.

A security risk assessment will be carried out on each information asset to identify the level of protection required. The security and control procedures required will take into account the sensitivity and value of the information.

DIRECTION

Information Security promotes trust both internally and externally in shared data and infrastructure. The Company's strategic direction for Information Security is to provide a strong forward-looking information management system that is clearly aligned to the Company's corporate vision and strategic priorities. This vision for Information Security reflects its growing role in maintaining trust and confidence both within the company and outside.

SCOPE AND RESPONSIBILITIES

The Company's Information Security Policy is applicable to:

1. All Company information, information owned by its clients and partners, and information about its clients.
2. All Company members, permanent, contract and temporary personnel, and all third parties, who have access to the Company's premises, systems or information (Users).
3. All Company systems, software, and information created, held, processed or used on those systems or related media, electronic, magnetic, or written/ printed output from the Company's systems.
4. All means of communicating information, both within the Company and externally. For example, data and voice transmissions or recordings, post, e-mail, SMS/text, cameras, whiteboards, memory sticks, disks, fax, telex, image/sound processing, videoconferencing, photocopying, flip charts, general conversation etc.

The IT Manager and DPO are responsible for defining Information Security policy and standards. Department heads and service providers are responsible for implementing policies and standards in their area of jurisdiction. Furthermore, these policies and standards must be included in service level agreements and contracts with IT service providers.

Non -compliance with this policy will be dealt with under the relevant Company procedures and may result in disciplinary action, termination of contract, or criminal prosecution in the most serious of cases.
This policy is a living document and thus frequently updated to reflect technological, legal and organizational changes. It should therefore be revisited on a regular basis by all staff.

SPECIFIC RESPONSIBILITIES

1. **Employees**
   a. Will be alert and report any suspected security incident.
   b. Will be receptive to external parties reporting possible misuse of information but will refrain from accepting any fault or responsibility until the report has been investigated and the possible misuse confirmed.

2. **Board**
   The Board shall:
   a. Set the tone at the top on data protection.
   b. Ultimately responsible for ensuring that the Organization meets the obligations of the Regulation.

3. **Executive Management Committee**
   The Management shall:
   a. Ensure data protection objectives are established and are aligned with the strategic direction of the Company.
   b. Ensure that the resources needed for the protection of data are available.
   c. Communicate the importance of effective data protection in the Company and of conforming to its requirements.
   d. Support other relevant Management roles to demonstrate their leadership as it applies to their areas of responsibility.

4. **Heads of SBUs and Shared Services**
   a. Will take over external contacts in case of an alleged misuse or theft of information; obtain the necessary details and pass on the information to the IT.
   b. Escalate security incidents according to local procedures/governing body.
   c. Inform the management.

5. **All Users**
   Users of systems and information must:
   a. Access only systems and information, including reports and paper documents, to which they are authorized.
   b. Use systems and information only for the purposes for which they have been authorized, and only from the Company's ICT controlled or authorized secure equipment and approved software.

c. Comply with all appropriate legislation, and with the controls defined by the Information Owner, and all Company Policies, Standards, Procedures and Guideline.
d. Not disclose confidential information to anyone without the permission of the Information Owner.
e. Keep their passwords and other access credentials secret, and not allow anyone else to use their account, or equipment or media in their care, to gain access to any system or information.
f. Notify their immediate superior, or the DPO of any actual or suspected breach of Information Security, or of any perceived weakness in the Company Security Policies, Procedures and Practices, Process or infrastructure.
g. Establish the identity and authority of anyone requesting information access or information system access e.g. for servicing or repairs.
h. Familiarize themselves with this Policy, and all applicable supporting Policies, Procedures, Standards and Guidelines. Compliance with this Policy is mandatory, and any employee failing to comply will be subject to disciplinary procedures, revoking of access &/or prosecution in serious cases.
i. If responsible for management of third parties you must ensure that those third parties are contractually obliged to comply with this Policy and are aware that their failure to comply may lead to contract termination &/or prosecution in serious cases.
j. Be aware that the Company monitors the content and usage of its systems and communications to check for Policy compliance.
k. Never leave computers logged into the network unattended unless password protected screen locking is available and has been engaged.
l. Keep your desk clear of all confidential paper files and documents when you are not working on them. Maintain a clear desk policy when leaving your desk unattended for any period of time and out of office hours. Keep all confidential paper files and documents in secure, lockable cabinets.
m. Not take confidential documents or materials home, however, if this is unavoidable, do consider the use of lockable bags or cases when it is necessary to carry paper files or documents in person.
n. Stand at public printers or have documents containing confidential information retrieved immediately so that unauthorized individuals have no opportunity to see the information.
o. Not store confidential electronic files and documents on your computer's local drive or mail to a personal email address in order to work on them at home.
p. Not use standard USB data sticks or digital drives as portable temporary storage for electronic files and documents. Standard **encrypted** USB data sticks may be used only

after the IT Manager for Information Management has approved a valid business case. If permission is granted, these USB data sticks may only be purchased from Procurement.

q. Purchase all new laptops, mobile phones, and any other hand-held devices capable of storing data, through the IT Manager to allow encryption software to be installed prior to being released to you. This ensures that the device is protected should it be lost or stolen. Any existing Company owned laptops or portable devices should be returned to the IT Manager who will make appropriate arrangements to have the encryption software installed at a predetermined rate.
r. Lock all laptops away in a secure cabinet when not in use in the office or in the home and never leave on the back seat of a car.
s. Ensure that in complying with this policy, users comply strictly with the Company's Acceptable Use Policy which monitors the use of company-supplied technologies.
t. Ensure compliance with the company's Access Control Policy ensuring authorized access to information systems.
u. Ensure compliance with the Company's Communications & Operations Management Policy a well as the Company's Physical and IT Environment Security Policy.
v. Ensure compliance with all other IT Policies developed by the Company including but not limited to the Company's Human Resources Security Policy, Data Classification Policy, Global Information Security Policy, Information Security Incident Policy and the Licensing and Duplication Restriction Policy

6. **Onsite IT Function**

In case of systems compromise the IT will:

a. isolate the compromised system (damage control/containment of the incident).
b. Follow defined remediation procedures.
c. Escalate security incidents according to defined procedures.
d. Inform management.
e. Ensure all systems, services and equipment used for storing data meet acceptable security standards.
f. Evaluate any third-party services VG Pensions is considering using to store or process data such as private cloud computing services.

The IT Manager will act as the focus for all Information security issues, suggesting policies to mitigate risk, and assisting with their interpretation into team procedures and standards, whilst implementing those aspects affecting the operational security of the Company's Information and IT infrastructure.

7. **Data Protection Officer**

The duties of the DPO shall include:

a. Specifying minimum training requirements and arranging its availability.
b. Monitoring pre-employment reference checking and advising management to ensure compliance with requirements of the role.
c. Ensuring that system administrators receive prompt notification of employee role changes and departures.
d. Ensure that procedures are in place reflecting the controls and access levels.
e. Periodically review access to ensure that procedures are followed, especially in the event of process changes that affect the asset.
f. Specifying the retention period for each asset, and the manner in which it should be deleted or destroyed at the end of that period.

8. **Human Resources and Development**
   The Human Resources Department shall:
   a. Promote awareness of training, including induction training and for ensuring inclusion of relevant security awareness therein & in employee documentation.
   b. Support the DPO and management to define disciplinary action in the event of misconduct, and non-compliance with Security Policies and assisting management with disciplinary procedures.

9. **Enterprise Risk Management**
   They are to provide reasonable assurance regarding the achievement of the operational objectives, such as the effectiveness and efficiency of the security controls.

10. **Internal Audit/Control**
    a. Carry out internal audit and report findings to Executive Management Committee
    b. Recommend preventive and corrective action.

Review of Information Security Policy

The Company's Management will review this policy on a yearly basis, and the results of the review will be detailed on the minutes of this meeting. Any resulting changes will be notified to all relevant stakeholders.
In the event of major network configuration changes, change of policy, security incidents or a lack of security identified in the yearly penetration test performed on the Company's network, the policy will be reviewed for effectiveness, and modified if appropriate,

Information Security Policy – Exceptions

It is not intended that any exceptions will be permitted even on a temporary basis but rather the Policy should be reviewed at the next opportunity. Any changes must be approved by the relevant Board Committee.

SCHEDULE 2
PERSONAL DATA BREACH & INCIDENT HANDLING PROCEDURE

1. POLICY STATEMENT

Sewa Assets Management Limited (hereinafter referred to as "SEWA" or "the Company") is committed to its obligations under the regulatory system, the General Data Protection Regulation (GDPR) and the Nigerian Data Protection Regulation (NDPR) and maintains a robust and structured program for compliance adherence and monitoring.

We carry out frequent risk assessments and gap analysis reports to ensure that our compliance processes, functions and procedures are fit for purpose and that mitigating actions are in place where necessary. However, we recognize that breaches can occur, so this policy states our intent and objectives for dealing with such incidents. Although we understand that not all risks can be mitigated, we operate a robust and structured system of controls, measures and processes to help protect data subjects and their personal information from any risks associated with processing data.

The protection and security of the personal data that we process is of paramount importance to us and we have developed data specific controls and protocols for any breaches relating to the NDPR and data protection laws.

2. PURPOSE

The purpose of this policy is to provide the Company's intent, objectives and procedures regarding data breaches involving personal information. As we have obligations under the NDPR, we also have a requirement to ensure that the correct procedures, controls and measures are in place and disseminated to all employees, ensuring that they are aware of what the protocols and reporting lines are for personal information breaches. This policy details our processes for reporting, communicating and investigating incidents.

3. SCOPE

This policy applies to all persons within the Company (permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Company). Adherence to this policy is mandatory and noncompliance could lead to disciplinary action.

4. INFORMATION SECURITY INCIDENT:

Information security incident is defined as the suspicion or evidence of one or more of the following events:

Fire, flooding and other environmental interruptions

a. Fraud.

b. Information leakage/theft of data.
c. Malware infections.
d. Physical forced access to secured areas.
e. Sabotage
f. Theft of information assets.
g. Unauthorized access of information systems.
h. Utility supply interruptions (power, cooling, communication links)

5. Data Security & Breach Requirements

The Company's definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. Alongside our 'Privacy Policy' approach to protecting data, we also have a legal, regulatory and business obligation to ensure that personal information is protected whilst being processed by the Company. Our technical and organizational measures are detailed in our **Data Protection Policy & Procedures and Information Security Policies**.

We carry out information audits to ensure that all personal data processed by us is accounted for and recorded, alongside risk assessments that assess the scope and impact of any potential data breach; both on the processing and on a data subject. We have implemented adequate, effective Personal Data Breach & Incident Handling Procedure and appropriate technical and organizational measures to ensure a level of security appropriate to the risks, including (but not limited to):

a. encryption of personal data
b. Restricted access
c. Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
d. Audit procedures and stress testing on a regularly basis to test, assess, review and evaluating the effectiveness of all measures and compliance with the data protection regulations and codes of conduct.
e. Frequent and rolling training programs for all staff on the NDPR, its principles and applying those regulations to each role, duty and the company as a whole.
f. Staff assessments and testing to ensure a high level of competency, knowledge and understanding of the data protection regulations and the measures we have in place to protect personal information.
g. Recheck processes to ensure that where personal information is transferred, disclosed, shared or is due for disposal, it is rechecked and authorized by the Data Protection Officer

6. OBJECTIVES

6.1 To adhere to the GDPR,NDPR and Nigerian Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches.

6.2 To develop and implement adequate, effective and appropriate technical and organizational measures to ensure a high level of security with regards to personal information

6.3 To utilize information audits and risk assessments for mapping data and reducing the risk of breaches

6.4 To have adequate and effective risk management procedures for assessing any risks presented by processing personal information.

6.5 To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes.

6.6 To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring.

6.7 To use the Data Breach Incident Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected.

6.8 To protect clients and staff – including their data, information and identity

6.9 To ensure that where applicable, the Data Protection Officer is involved in and notified about all data breaches and risk issues.

6.10 To ensure that the Supervisory Authority is notified of the data breach (where applicable) with immediate effect and at the latest, within 72 hours after having become aware of the breach.

7. DATA BREACH PROCEDURES & GUIDELINES

The Company has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below. Our documented breach incident program aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

7.1 Breach Monitoring & Reporting

The Company has appointed a Data Protection Officer/Compliance Officer who is responsible for the review and investigation of any data breach involving personal information, regardless of the severity, impact or containment. All data breaches are reported to this person with immediate effect, whereby the procedures detailed in this policy are followed. All data breaches will be investigated, even in

instances where notifications and reporting are not required, and we retain a full record of all data breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to a data breach, revision to any such process is recorded.

7.2 Breach Incident Procedures

i. Identification of an Incident - As soon as a data breach has been identified, it is reported to the direct line manager and the Data Protection Officer immediately so that breach procedures can be initiated and followed without delay. Reporting incidents in full and with immediate effect is essential to the compliant functioning of the Company. These procedures are for the protection of the Company, its staff, customers, clients and third parties and are of the utmost importance for legal regulatory compliance. As soon as an incident has been reported, measures must be taken to contain the breach. Such measures are not in the scope of this document due to the vast nature of breaches and the variety of measures to be taken; however, the aim of any such measures should be to stop any further risk/breach to the organisation, customer, client, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident record in all cases.

ii. Breach Recording - The Company utilizes a Breach Incident Form for all incidents, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident Folder and reviewed against existing records to ascertain patterns or reoccurrences. In cases of data breaches, the Data Protection Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the breach, recording the incident on the breach form and making any relevant and legal notifications. The completing of the Breach Incident Form is only to be actioned after containment has been achieved.
A full investigation is conducted and recorded on the incident form, with the outcome being communicated to all staff involved in the breach, in addition to senior management. A copy of the completed incident form is filed for audit and record purposes.

7.3 Breach Risk Assessment

i. Human Error - Where the data breach is the result of human error, an investigation into the root cause is to be conducted and a formal interview with the employee held. A review of the procedure(s) associated with the breach is conducted and a full

risk assessment completed. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause. Resultant employee outcomes of such an investigation can include, but are not limited to: -

a. Re-training in specific/all compliance areas
b. Re-assessment of compliance knowledge and understanding.
c. Suspension from compliance related tasks
d. Formal warning (in-line with the Company's disciplinary procedures)

ii. System Error - Where the data breach is the result of a system error/failure, the IT team are to work in conjunction with the DPO to assess the risk and investigate the root cause of the breach. A gap analysis is to be completed on the system(s) involved and a full review and report to be added to the Breach Incident Form. Any identified gaps that are found to have caused/contributed to the breach are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident:

a. Attempting to recover any lost equipment or personal information.
b. Shutting down an IT system
c. Removing an employee from their tasks
d. The use of back-ups to restore lost, damaged or stolen information.
e. Making the building secure
f. If the incident involves any entry codes or passwords, then these codes must be changed immediately, and members of staff informed.

iii. Assessment of Risk and Investigation - The DPO should ascertain what information was involved in the data breach and what subsequent steps are required to remedy the situation and mitigate any further breaches. The lead investigator should look at:

a. The type of information involved.
b. It's sensitivity or personal content.
c. What protections are in place (e.g. encryption)?
d. What happened to the information/Where is it now?
e. Whether there are any wider consequences/implications to the incident.

The appointed lead should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or

statements, the assessment of risk/investigation and any recommendations for future work/actions.

8. Record Keeping

All records and notes taking during the identification, assessment and investigation of the data breach are recorded and authorized by the Data Protection Officer and are retained for a period of 6 years from the date of the incident. Incident forms are to be reviewed monthly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

9. Responsibilities

The Company will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the breach incident reporting lines. The Data Protection Officer is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.

DATA BREACH INCIDENT FORM

DPO/COMPLIANCE OFFICER/INVESTIGATOR DETAILS:			
NAME:		**POSITION:**	
DATE:		**TIME:**	
		EMAIL:	
INCIDENT INFORMATION:			
DATE/TIME OR PERIOD OF BREACH:			
DESCRIPTION & NATURE OF BREACH:			
TYPE OF BREACH:			
CATEGORIES OF DATA SUBJECTS AFFECTED:			
CATEGORIES OF PERSONAL DATA RECORDS CONCERNED:			
NO. OF DATA SUBJECTS AFFECTED:		**NO. OF RECORDS INVOLVED:**	
IMMEDIATE ACTION TAKEN TO CONTAIN/MITIGATE BREACH:			
STAFF INVOLVED IN BREACH:			
PROCEDURES INVOLVED IN BREACH:			
THIRD PARTIES INVOLVED IN BREACH:			
OUTCOME OF INVESTIGATION			
ACTION TAKEN:			

Document Control Sheet

DOCUMENT CONTROL SHEET

Version and Update History:

Version	Date	Author	Change from Previous Version
1.0	JULY 2021	ERM and IT Units	

Approval List:

Name	Position	Signature	Date
	IT Unit		
	Legal & Compliance Unit		
	Enterprise Risk Management Unit		
	Managing Director		
	Chairman - Board Risk, Audit & Compliance Committee		

Distribution List:

Name	Version	Date
All Staff	1.0	JULY 2021
Partners, Clients, Vendors	1.0	JULY 2021

Policy Review

This policy is subject to continuous changes. In case there are no changes, then an annual review shall be performed.