**Audit Questionnaire Document**

**SECTION: ACCOUNTABILITY AND GOVERNANCE**

1. **Did you process the personal data of:**
   * a) More than 1,000 Data Subjects in the last 6 months
   * b) More than 2,000 Data Subjects in the last 12 months  
     Options: [Yes / No]
2. **Is your top-management aware of the Nigeria Data Protection Act (NDPA) and the potential implication on your organisation?**  
   Options: [Yes / No]
3. **Have you implemented any information security standard in your organisation before?**  
   Options: [Yes / No]
   * *If Yes, specify standard*
   * **Client to upload document**
4. **Do you have a documented data breach incident management procedure?**  
   Options: [Yes / No]
   * **Client to upload document**
5. **Do you collect and process personal information through digital mediums?**  
   Options: [Yes / No]
6. **Have you organised any NDPA awareness seminar for staff or suppliers?**  
   Options: [Yes / No]
   * **Client to upload training evidence**
7. **Have you conducted a detailed audit of your privacy and data protection practices?**  
   Options: [Yes / No]
   * **Client to upload audit report**
8. **Have you defined management support for data protection compliance through policy frameworks?**  
   Options: [Yes / No]
   * **Client to upload policy document**
9. **Do you have a data protection compliance and review mechanism?**  
   Options: [Yes / No]
10. **Have you developed a capacity building plan for staff on data protection compliance?**  
    Options: [Yes / No]
    * **Client to upload plan**
11. **Do you know the types of personal data you hold?**  
    Options: [Yes / No]
12. **Do you know the sources of the personal data you hold?**  
    Options: [Yes / No]
13. **Who do you share personal data with?**
    * *Open text*
14. **Have you reviewed your HR policy to ensure employee data is NDPA compliant?**  
    Options: [Yes / No]
    * **Client to upload HR policy**
15. **Have you assessed whether you are a Data Controller or Processor?**  
    Options: [Controller / Processor / Both / Not Sure]
16. **Have appropriate technical and organisational measures been implemented for data protection?**  
    Options: [Yes / No]
    * **Client to upload supporting documents**
17. **Do you have a DPIA policy for assessing privacy impact in new/existing projects?**  
    Options: [Yes / No]
    * **Client to upload DPIA policy**
18. **Does your DPIA policy address the following?**

* a) Description of processing operations
* b) Purpose of processing
* c) Legitimate interest pursued
* d) Assessment of necessity and proportionality
* e) Risk to rights and freedoms
* f) Mitigation measures  
  Options: [Yes / No for each]

1. **Who is responsible for data protection compliance in your organisation?**
   * *Open text*
2. **Are your service providers/merchants compliant with the NDPR?**  
   Options: [Yes / No / Some]
   * If yes: **Client to upload Audit trust**
   * If no: Have you mandated them to be compliant? [Yes / No]
3. **What training programs are in place for employee data privacy and security awareness?**
   * *Open text*
   * **Client to upload training materials or summary**
4. **How often are employees updated on changes in privacy regulations?**  
   Options: [Quarterly / Bi-annually / Annually / Not at all]
5. **What accountability measures exist for processing activities?**
   * *Open text*
6. **What strategies support embedding privacy culture in the organisation?**
   * *Open text*
7. **Have workshops been conducted to educate stakeholders about privacy obligations?**  
   Options: [Yes / No]
   * **Client to upload workshop evidence**
8. **How do you ensure all individuals understand their data protection responsibilities?**
   * *Open text*
9. **Is privacy awareness promoted at all levels of the organisation?**  
   Options: [Yes / No]
10. **Are there training programs/resources on privacy best practices?**  
    Options: [Yes / No]
11. **How are staff held accountable for privacy policy adherence?**
    * *Open text*

**SECTION: DATA PROTECTION OFFICER / COMPLIANCE ORGANISATION**

1. **Does your DPCO also perform the role of your DPO?**  
   Options: [Yes / No]
2. **Has a DPO been appointed for NDPA compliance oversight?**  
   Options: [Yes / No]
   * **Client to upload appointment letter**
3. **Do you use the same DPCO for compliance implementation and audit?**  
   Options: [Yes / No]
4. **Has your DPO been trained in the last year?**  
   Options: [Yes / No]
   * **Client to upload training certificate**
5. **Does your DPO hold a valid data privacy certification?**  
   Options: [Yes / No]
   * **Client to upload certification proof**
6. **Does the DPO have sufficient access, support, and budget?**  
   Options: [Yes / No]
7. **Has conflict of interest been evaluated if the DPO holds multiple roles?**  
   Options: [Yes / No]
8. **Does the DPO have expertise to:**

* a) Advise business and third parties [Yes / No]
* b) Monitor NDPA compliance [Yes / No]
* c) Raise awareness and assign responsibilities [Yes / No]
* d) Provide DPIA-related advice [Yes / No]

1. **Is there a channel (e.g. webpage) for data subjects to reach your organisation?**  
   Options: [Yes / No]
   * **Client to provide webpage link**
2. **Are there checks to ensure individual rights are preserved under NDPA?**  
   Options: [Yes / No]
3. **Is there a public-facing mechanism for Data Subject inquiries (e.g., webpage)?**  
   Options: [Yes / No]

* **Client to upload webpage link or screenshot**

1. **Are all staff trained to recognise Subject Access Requests (SARs)?**  
   Options: [Yes / No]
2. **Do you have procedures for handling SARs from third parties?**  
   Options: [Yes / No]
3. **Have you implemented breach detection, reporting and investigation protocols?**  
   Options: [Yes / No]
4. **Do you notify affected individuals of breaches that pose high risk to their rights?**  
   Options: [Yes / No]
5. **Have all staff handling personal data been trained on their responsibilities?**  
   Options: [Yes / No]
6. **Are these responsibilities documented in job descriptions?**  
   Options: [Yes / No]
7. **Do you use third-party data processors?**  
   Options: [Yes / No]

* If Yes: Are contracts NDPA-compliant? [Yes / No]
* **Client to upload contract sample**

1. **Do you review contracts regularly for NDPA compliance?**  
   Options: [Yes / No]
2. **Do you transfer personal data outside Nigeria?**  
   Options: [Yes / No]

* If Yes: Are contracts and safeguards in place? [Yes / No]
* Are destination countries on the NDPA White List? [Yes / No]
* If No: Have you recorded legal transfer basis? [Yes / No]
* Which countries do you transfer data to? [Open text]
* What types of data are transferred? [Open text]
* Purpose of transfer? [Open text]
* Legal basis? [Open text]
* **Client to upload data transfer policy**

1. **How do you assess adequacy of protection in recipient countries?**

* Open text

1. **What technical and organisational measures are in place (e.g., encryption, access control)?**

* Open text

1. **Do you inform Data Subjects about international transfers and rights?**  
   Options: [Yes / No]
2. **How do you respond to SARs for internationally transferred data?**

* Open text

1. **Do you meet ISO/IEC 27001 standards or similar for securing personal data?**  
   Options: [Yes / No]

* **Client to upload certification or summary of controls**

1. **Are staff aware that unauthorised access to personal data is prohibited?**  
   Options: [Yes / No]
2. **Are staff informed that data confidentiality continues after employment ends?**  
   Options: [Yes / No]

### SECTION: DATA INVENTORY AND MAPPING

1. **Have you developed a data inventory/map identifying data usage and location?**  
   Options: [Yes / No]

* **Client to upload sample**

1. **How frequently is the data inventory updated?**  
   Options: [Quarterly / Annually / As needed / Not updated]
2. **Are specific individuals/teams responsible for data inventory accuracy?**  
   Options: [Yes / No]
3. **Who maintains the data inventory, and how is cross-departmental input managed?**

* Open text

1. **What tools/technologies support your data inventory process?**

* Open text

1. **Do you use third-party tools/services for inventory automation or accuracy?**  
   Options: [Yes / No]

### SECTION: DATA CLASSIFICATION ASSESSMENT

1. **Do you have a data classification policy for risk-based categorisation?**  
   Options: [Yes / No]

* **Client to upload policy**

1. **How are classification categories defined?**

* Open text

1. **Do you have procedures to identify/classify personal data in your systems?**  
   Options: [Yes / No]
2. **What classification levels are used (e.g., Public, Confidential, Restricted)?**

* Open text

1. **Provide examples of data**

**SECTION 1: ADMINISTRATION**

1. Do you use technology/an automated process to handle data?
   1. Options: Yes / No
2. Is there a documented data governance policy in place? Does it align with the way you process data on the system?
   1. Options: Yes / No / Partially
3. Are there procedures for data access control and user permissions?
   1. Options: Yes / No / Partially
4. Do you use technology or automated processes to manage the collection, storage, use, and processing of data?
   1. Options: Yes / No
5. Does the technology/automated process in place comply with industry and regulatory standards?
   1. Options: Yes / No / Not Sure
6. Are security awareness training sessions conducted to educate employees about physical and environmental security measures?
   1. Options: Yes / No / Sometimes

**SECTION 2: CAPTURING**

1. Do you use technology or automated processes for data collection?
   1. Options: Yes / No
2. What methods or tools are used for data collection within the organization?
   1. **Client to provide document**
3. Are data collection processes standardized and documented?
   1. Options: Yes / No
4. Are there mechanisms to verify the accuracy and completeness of collected data?

* Options: Yes / No

1. Are there any tech or automated processes used in collecting and processing data?

* Options: Yes / No

101.What are the primary sources of data for the organization?

* **Client to provide document**

1. How is data from different sources processed and used?

* **Client to provide document**

1. Are there procedures for validating and cleansing incoming data?

* Options: Yes / No

1. Are there procedures for obtaining consent and permissions for data collection and processing, especially sensitive data?

* Options: Yes / No

1. What methods are used for processing and analysing data within the organization?

* **Client to provide document**

1. Are there controls in place to prevent unauthorized access or modification of data during processing?

* Options: Yes / No

1. How do you store/backup data?

* Options: On Premises / Cloud / Both

1. How frequently is data backed up, and what methods are employed for backups?

* **Client to provide document**

1. Do you have a disaster recovery plan? If yes:

* Is there a procedure for activating and carrying out the plan in the event of a calamity?
  + Options: Yes / No
* Do Employees receive training on the disaster recovery plan?
  + Options: Yes / No

1. Is your on-premises/cloud storage accessible to anyone?

* Options: Yes / No

1. Do you have measures in place to ensure the security of your premises/cloud infrastructure?

* Options: Yes / No

1. Do you have measures to authenticate and authorize access to your premises/cloud services?

* Options: Yes / No

1. Does the technology record and manage access to data?

* Options: Yes / No

1. Do you train employees on cloud security best practices? (Only for those who require access)

* Options: Yes / No

1. How is data quality monitored and maintained throughout its lifecycle?

* **Client to provide document**

1. Does a backup policy exist, and is it routinely tested?
2. Options: Yes / No
3. Are backups kept in a safe, off-site place?

* Options: Yes / No

1. Does the disaster recovery plan undergo routine testing?

* Options: Yes / No

**SECTION 3: ACTIONS & SECURITY**

1. Do you apply technology or automated processes to protect data?

* Options: Yes / No

1. Does the process protect data while in transit and at rest?

* Options: Yes / No

1. Do you use any encryption method?

* Options: Yes / No

1. Does the organization have an information security policy, and is it communicated to all employees?

* Options: Yes / No

1. Are access controls and authentication mechanisms in place?

* Options: Yes / No

1. How are security incidents and breaches detected, reported, and mitigated?

* **Client to provide document**

1. Do you authorize and verify user identities for your applications?

* Options: Yes / No

1. Do you have safeguards against unwanted access to your applications?

* Options: Yes / No

1. Do you update software regularly?

* Options: Yes / No

1. Do you ensure the security of third-party components in your applications?

* Options: Yes / No

1. Is the security of mobile applications ensured?

* Options: Yes / No

1. Are best practices for application security taught to employees?

* Options: Yes / No

1. Do you implement cybersecurity practices to secure the network?

* Options: Yes / No

1. Are firewalls and IDS/IPS in place?

* Options: Yes / No

1. Are network devices configured securely?

* Options: Yes / No

1. Are unnecessary network ports/protocols blocked?

* Options: Yes / No

1. Is there a process for monitoring network traffic?

* Options: Yes / No

1. Do you have staff that work from home?

* Options: Yes / No

1. Do they connect to the organisation network for tasks?

* Options: Yes / No

1. Do you provide secure connection technologies (e.g., VPN, tunneling)?

* Options: Yes / No

1. Are mechanisms provided to secure data during communication with clients?

* Options: Yes / No

1. Are physical controls (locks, alarms, CCTV) used?

* Options: Yes / No

1. What measures protect against physical threats?

* **Client to provide document**

1. Are systems and software updated frequently?

* Options: Yes / No

1. Is there a procedure to track system activities and detect irregularities?

* Options: Yes / No

1. Is there a documented data disposal plan for paper and electronic waste?

* Options: Yes / No

1. How is personal data destroyed before disposal? Is it NIST-compliant?

* **Client to provide document**