

# **TERRA SWITCHING & PROCESSING COMPANY**

## **CONFIDENTIALITY POLICY**

**March 2023**

## OVERVIEW

Terra Switching & Processing Company confidentiality policy explains how the company expects its employees to treat the information they receive about clients, partners and the company and make sure it remains well-protected.




## DOCUMENT INFORMATION

### Document Owner

This document is owned by the Chief Information Security Officer (CISO). He is responsible for ensuring that the Policy is reviewed in line with the requirements of the organization.

Policy Owner	Role	Date	Version
CISO	Chief Information Security Officer (CISO)	March 1, 2023	1.0

### Document Review & Approval

	Name	designation	Signature
Prepared by	Ajayi Oluwafemi A	Chief Compliance Officer (CCO)	
Concurrence	Mgbeahuru Uche	Head, HR	
Approved	Adeniji Kayode	Ag. MD/CEO	

## Table of Content

1.	Aim and Objective	4
2.	Purpose	4
3.	Scope	4
4.	Governance	4
5.	Management	4
6.	Staff & Contractor	5
7.	Acknowledgement of Confidentiality	5
8.	Failure to comply	5
9.	Collection of credentials information	5
10.	Accuracy of Confidential Information	5
11.	Principle	5
12.	Release of information	6
13.	Accessing or Sharing Confidential Information with Third Parties	6
14.	Security of information	6
15.	Retention and Detection of confidential information	7
16.	Personal Identification Information (Pii) Risk Assessment	7
17.	Compliance Monitoring	7
18.	Breach of Policy	7
19.	Maintenance of Confidentiality & Non-disclosure	7
20.	Other Circumstances in which information can be disclosed	8
21.	Storage of Data	9
22.	The Media	9
23.	Disposal of Information	9

## **1. AIMS & OBJECTIVES**

Employees and personnel of Terra Switching & Processing Company (Terra) have a duty of maintaining the confidentiality of information received by them in the course of their employment or engagement. This Confidentiality Policy documents the confidentiality and non-disclosure duties and obligations of Terra's employees

The employees and personnel of Terra will, in the course of their employment and engagement, become aware of and possess information of Terra or of third parties disclosed to Terra that is not generally known. This may include information which if disclosed could jeopardize the interests of the Company. It may also include commercial trade secrets disclosure of which could harm the interests of the Company.

All employees and personnel of the Company have a duty to keep such information strictly confidential and to use it only for the proper purposes in accordance with the law.

## **2. PURPOSE**

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work with Terra Switching & Processing Company (Terra) and have access to its confidential information.

This policy, where relevant, should be read in conjunction with the appointment letter and/or employment contract applicable to Terra Switching & Processing Company employees and personnel, and other work rules, policies and procedures applicable to Company employees and personnel.

## **3. SCOPE**

This policy applies to all Company associates, contractors and other persons working with confidential information that is within the possession, custody or control of Company. For purposes of this Policy, "confidential information" means all customer data, Company data and application and systems software that is created, stored, accessed and distributed, regardless of whether such information is in physical or electronic form.

## **4. GOVERNANCE**

Overall responsibility for ensuring compliance with this Policy rests with the Human Resource Manager and Chief Information Security Officer (CISO). All employees must comply with this Policy in connection with day-to-day use, collection and processing of confidential information in the ordinary course of Company's business.

## **5. MANAGEMENT**

Each company manager is responsible for ensuring that Company employees within such Company manager's area(s) of responsibility are complying with this Policy. Company management is also responsible for making all external parties aware of any changes to our confidentiality policy.

## **6. STAFF AND CONTRACTORS**

All Employees of Terra are responsible for ensuring that appropriate steps are taken to protect Client confidential Information at all times. Employees are encouraged to regularly review and consult this Policy to ensure their own practices are in accordance with this Policy as it concerns the collection, access, use or disclosure of confidential information. Employees are expected to report any issues, problems, questions and concerns about this Policy to the CISO. Employees are encouraged to make suggestions to the CISO to help improve privacy and security procedures. In the event of any incident involving confidential information or privacy and data security, employees are expected to fully cooperate with such investigations.

## **7. ACKNOWLEDGEMENT OF CONFIDENTIALITY**

In order to promote compliance with this Policy, Company requires that all Employees be provided with a copy of this Policy. Company management must also regularly refresh and remind employees of this Policy and the importance of maintaining the confidentiality of confidential information. As a condition of employment or affiliation with Company, all new employees and contractors are required to read and sign a Confidentiality Acknowledgment or non-disclosure agreement, which specifies that such employee or contractor understands the importance of maintaining the confidentiality of confidential information and will fully comply with this Policy. Company employees are also required to maintain confidence over confidential information after their affiliation with company comes to an end.

## **8. FAILURE TO COMPLY**

Any failure by a Company employee or to comply with this Policy may result in disciplinary action including, but not limited to, the termination of employment or affiliation with Company.

## **9. COLLECTION OF CONFIDENTIAL INFORMATION**

The collection of confidential information by Company is governed by applicable international, federal and state law. As a practical matter, the collection of confidential information should be limited to what is needed to fulfill a specific purpose identified to the client or other person from whom it is collected.

## **10. ACCURACY OF CONFIDENTIAL INFORMATION**

All employees must take all reasonable steps to ensure the accuracy and completeness of any confidential information that such employees collect or record. Employees must be diligent to protect against making any errors due to carelessness or other oversights.

## **11. PRINCIPLES**

The Company expects all of its employees and Board of Directors to handle all confidential information in a sensitive and professional manner. All employees are under an obligation not to gain access or attempt to gain access to information which they are not authorized to have. The Company, however, recognizes the importance of an open culture with clear communication and accountability. It therefore wishes to maintain personal and

organizational safety and expects all employees to handle confidential information in a way which protects organizational security.

The purpose of confidentiality is essentially two-fold. Firstly, it protects sensitive or confidential information of the Company, its clients and customers. Secondly, it builds trust among employees such that they can effectively share information and knowledge together without fear.

The best protection against breaches in confidentiality is to keep the number of employees and personnel who have access to sensitive information to a necessary minimum. Intentional, repeated, accidental, or unauthorized disclosure of any confidential information by any member of staff will be subject to disciplinary action. Any such disciplinary action will take account of the confidential and possible sensitive nature of the information and will make sure that in dealing with it, no further breaches of confidentiality take place.

## **12. RELEASE OF INFORMATION**

Employees are expected to comply with all Company policies, procedures and guidelines for the release of confidential information. Employees must also ensure that any release of confidential information, including personally identifiable information is done in accordance with applicable law.

## **13. ACCESSING OR SHARING CONFIDENTIAL INFORMATION WITH THIRD PARTIES**

Before confidential information that is within the possession, custody or control of Company is accessed by or shared with a contractor or other third-party organization, the third party must execute a Non-Disclosure Agreement (NDA) or information sharing agreement with Company. Senior Company management must approve the form of all such agreements.

All Employees are required to take all reasonable steps to ensure no unauthorized personnel or third parties are provided with access to records containing confidential information. In the event a third-party requests access to confidential information, all of the following steps must be taken prior to granting access:

- (1) the third party must produce identification verifying their identity,
- (2) a Company manager must confirm that the third party has signed a non-disclosure or information sharing agreement with Company,
- (3) a Company Manager must confirm that the applicable Company management has approved the third party for access to confidential information, and
- (4) the third party's access to such confidential information is limited only to the information absolutely necessary for such third party to perform their job task or function.

The CISO must be consulted before any program is implemented in which confidential information will be transmitted outside the boundaries of the Company's system.

#### **14. SECURITY OF INFORMATION**

Company is committed to maintaining the security of confidential information and other sensitive information and has implemented technical and organization security mechanisms to help ensure the security and availability of physical and digital records, computer and network systems. All Employees are expected to comply with Company's security requirements and policies for use of such systems, including without limitation, Company's Acceptable Use Policy.

#### **15. RETENTION AND DESTRUCTION OF CONFIDENTIAL INFORMATION**

Company Records will be retained in accordance with Company's Record Retention Policy and all legal, regulatory and accreditation requirements. It is the responsibility of each employee in possession of a Company record to identify the applicable retention period for the particular record and to follow Company guidelines and procedures for the secure destruction of those records when the applicable retention period has expired and the information is no longer necessary to retain.

#### **16. PERSONAL IDENTIFICATION INFORMATION (PII) RISK ASSESSMENT**

On at least an annual basis, a PII Risk Assessment must be completed by Company and before implementing or significantly changing any program or system that requires the collection, use, disclosure or sharing of confidential information.

#### **17. COMPLIANCE MONITORING, AUDITING & CONSEQUENCES**

Access, use and disclosure of confidential information will be monitored. All suspected breaches of this Policy will be investigated by Company management. Any actions taken as a result of such a breach will be determined by Company management in consultation with representatives from Human Resources, Legal Services and/or other Company stakeholders, depending upon the nature of the breach, circumstances and parties involved. Each Company department and program must conduct appropriate reviews and audits of their systems and processes to ensure compliance with internal policies and standards of Company.

#### **18. BREACH OF POLICY**

All Employees are expected to report any real or suspected breaches of this Policy to the CISO, including any actual or suspected data breach involving personal or confidential information belonging to or within the possession, custody or control of Company.

All incidents involving theft or loss of confidential information will be promptly addressed for containment, investigation, reporting and remedial actions.

#### **19. MAINTENANCE OF CONFIDENTIALITY & NON-DISCLOSURE**

Terra Switching & Processing Company employees:

- must keep confidential all confidential information;
- may use confidential information solely for the purposes of performing their duties as an employee of the Company and

- may only disclose confidential information to persons who are aware that the confidential information must be kept confidential and who have a need to know (but only to the extent that each person has a need to know).

The employee's obligation of maintaining confidentiality and non-disclosure does not extend to confidential information that is required to be disclosed by the employee pursuant to an order of a Court or any statutory authority. The employee or person will promptly notify the Company of any such requirement to enable the Company to take necessary action as deemed fit by the Company in the circumstances.

At the end of the period of employment, each Terra's employees must return back to the Company:

- all confidential information in material form;
- those parts of all notes and other records in whatsoever form, based on or incorporating confidential information;
- all copies of confidential information and notes and other records based on or incorporating confidential information; and
- all of Company's property and assets, in the possession or control of the Company employee.

The obligation of maintaining confidentiality and non-disclosure will continue even after the end of the period of employment or engagement in respect of all confidential information.

Any Terra employee found to be in breach of this confidentiality and non-disclosure obligation, whilst employed by the Company will be disciplined, and in serious instances, dismissed.

Any ex-employee found to be in breach of this confidentiality obligation may be subject to legal action being taken against them, dependent upon the circumstances of the breach, including cancellation/ withdrawal of any or all benefits, if extended to the ex-employee by the Company.

This policy will operate in conjunction with the contract of employment or letter of appointment for Company employees and personnel.

## **20. OTHER CIRCUMSTANCES IN WHICH INFORMATION CAN BE DISCLOSED**

An employee can disclose confidential information with the written consent of his/her reporting Line manager, who is a member of the Company's management team:

- If the information is required by or under a Court order or of a statutory authority, the employee or person will promptly notify the Company of any such requirement to enable the Company to take necessary action
- If it is deemed fit by the Company in the circumstances where disclosure can be justified for any other purpose. This is usually for the protection of the public and is



likely to be in relation to the prevention and detection of serious crime. A request for information by Law enforcement Agencies must be carefully considered.

All Terra employees must be able to justify any decision when information has been disclosed.

## **21. STORAGE OF DATA**

No written document containing confidential information must be left visible where it can be read by anyone. This includes telephone messages, computer prints, letters and other documents. All hardware containing confidential information must be housed in a secure environment. Security precautions must be taken in accordance with the Company's Policy and Procedures.

## **22. THE MEDIA**

Confidential information must not be passed by any employee on to members of the press, or other media communications without the written consent of his reporting Line manager, who is a member of the Company's management team.

## **22. DISPOSAL OF INFORMATION**

All media containing confidential information must be disposed off in a manner that ensures that information is not disclosed to an unauthorized person.