Galaxy Backbone Limited

Third Party Information Security Policy

Version 1.0

DOCUMENT REFERENCE NUMBER:
GBB/ISMS/TPISP

Document Information

Document ID:	GBB/ISMS/TPISP
Document Version:	Version 1.0
Date of Version:	23/09/2019
Document Classification	Public
Document Status	Active

Change history

Version	Date	Created by	Description of change
Version 1.0	23/09/2019	Fatai Akinsola	Initial Draft

Distribution List

Name	Version	Date
Third Party Suppliers, Contractors, Customers and Users	Version 1.0	23/09/2019

Change Control

The contents of this document are subject to change control

Table of contents

1. Introduction

Galaxy Backbone Limited (GBB) relies on the confidentiality, integrity and availability of information, in all its ramification, to deliver services as per its mandate. It is essential that the security of information are ensured. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for GBB to recover. In the like manner, any third party who manages, accesses or processes GBB information must adhere to these principles to allow GBB maintains the trust of all stakeholders and interested parties to achieve compliance with relevant contractual, statutory, legal, regulatory and service requirements.

2. Purpose

The purpose of this policy is to set out compliance requirements expected of third parties who have access to GBB information and information processing facilities critical to the operation of GBB's business. The policy seeks to ensure that Third Parties understand their own responsibilities for protecting the confidentiality, integrity and availability of the GBB information they handle.

3. Reference Documents

This policy forms part of a suite of policy documents and Standards that guide information security management in Third Party relationships. These include but not limited to:

i. GBB Third Party Network Access Agreement
ii. GBB Data Protection Policy
iii. Nigeria Data Protection Regulation (NDPR)
iv. ISO/IEC 20000-1:2018
v. ISO 22301: 2012
vi. ISO/IEC 27001:2013
vii. PCI DSS Version 3.2.1

4. Scope

The scope of this policy includes any third party who manages, processes or accesses GBB information. This includes, but is not limited to stakeholders, service providers, contractors, suppliers, customers, users, and any other interested parties. The requirements also cover staff (permanent or temporary) employed directly and indirectly by the Third Party organization including subcontractors.

The scope of GBB's information assets include but not limited to GBB data, all physical locations holding GBB information assets, all information systems that access, process, or have custody of GBB information and or data.

5. Exception

The Third Party Information security policy is in place to assist GBB stakeholders, suppliers, service providers, customers and users to comply with information security best practices, applicable contractual, legal/regulatory and service requirements as well as to continually improve information security management. Where it is not currently feasible for the Third Party to comply with any of the specified requirements, Third Parties are advised to take steps to implement recommended controls in order to achieve conformity and improve security architecture of their organizations. GBB as a service provider will be willing to support such initiatives directed to continual improvement of the information security management system.

6. Information Security Policy

a. Third Party senior management shall ensure that information security policy and information security objectives are established and maintained.

b. Third Party shall at all times maintain duly approved Information Security policy, or set of Information Security policies, defining responsibilities and setting out the Third Party's approach to information security.

c. Third Party shall ensure that its Information Security Policies are available as documented information and are communicated to all staff responsible for GBB informtion.

7. Third Party Organisation

a. Third Party shall define and allocate information security roles and responsibilities to named individuals. Nominated individuals will have responsibility and accountability for information security policy, implementation and processes.

b. Third Party shall ensure the integration of the information security management system requirements into the organisation's processes and support assessment, monitoring and control of information security risk as well as ensure that information security issues related to GBB information and information processing facilities raised are properly addressed.

c. Third Party shall not process or otherwise make use of GBB information, for any purpose other than that which is directly related to the fulfilment of the agreed contract or Services.

d. Third Party shall maintain a register of the information security risks associated with GBB information and communications technology assets.

8. Human Resource Security

a. Third Party shall enusre their employees understand their responsibilities and are suitable for GBB's information processing or access roles for which they are considered.

b. Third Party shall ensure that information security policy and procedures clearly define information security responsibilities for all personnel

c. Third Party shall have a formal disciplinary process in place to take action against employees who have committed and information security breach.

d. Third Party shall ensure that all personnel working in the provision of the Services or accessing GBB information and information processing facilities sign an appropriate employee non-disclosure agreement relating to GBB information in the possession of the Third Party before they are given access to such GBB Information.

e. Third Party shall ensure that all employees of the organisation shall receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function. Such security awareness shall be sufficient to include information protection and security, the password and user account policy, issues of confidentiality and company security standards.

9. Asset Management

a. Third Party shall identify and maintain an inventory of the assets associated with GBB information and information processing facilities. All information assets used to process or access GBB Information must be owned by a designated individual of the Third Party organisation.

b. Third Party shall ensure that GBB Information is classified in terms of its legal requirements, service requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

c. Third Party shall ensure that any media used to record, store or process GBB Information as part of the Services, including (but not limited to) hard copy output, laptops, USB sticks, pen drives, CDs, or other magnetic media are securely handled, transported and disposed. The use of such removable media shall also be authorized

d. Policies and procedures for the acceptable use of GBB information and assets associated with GBB information and information processing facilities shall be established and implemented.

10. Access Control

a. Third Party shall establish, document and review access control policy that prevent unauthorized access to GBB information, systems and services.

b. Third Party access control policy shall include procedure for the provision and limitation of access to the Third Party Systems, any GBB Systems, and GBB Information so that access is limited to those personnel that need access to such information or systems to perform their duties.

c. Third Party shall have a system-enforced password and user account policy that meets or exceeds GBB password policy, i.e. minimum password length, strength; minimum and maximum age and password reuse prevention.

d. Third Party shall ensure that restrictions on connection times shall be used to provide further security for high risk applications processing sensitive GBB Information.

e. Third Party sahll ensure access rights of all employees and external party users to GBB information and information processing facilities are removed upon termination of their employment, contract or agreement or adjusted upon change

f. Third Party shall ensure that all systems and application user account creation are authorized, unique and regularly reviewed.

g. Third Parties shall ensure the access rights of Third Party employees and that of subcontractors users to GBB information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change of role.

11.Physical and Environmental Security

a. Third Party shall implent a policy to prevent unauthorized physical access, damage and interference to GBB's information or inforfmation processing facilities.

b. Third Party shall ensure that secure areas are protected by appropriate entry controls to ensure that only authorized personnel of the Third Party (or its Subcontractor) are allowed access to GBB's information or information processing facilities.

c. Third Party shall design and implement controls that ensures physical security for offices, rooms and facilities where services are provided or access granted to GBB's information or information processing facilities

d. Third Party shall design and apply physical protection against natural disasters, malicious attack or other external and environmental threats

e. The Third Party shall have in place a video surveillance system with sufficient coverage to monitor reception areas, exit/entry points, and vulnerable or secured working areas where GBB information and information processing assets are hosted.

f. The Third Party shall ensure that power and telecommunications cabling carrying GBB data or supporting information services are protected from interception, interference or damage.

g. The Third Party shall (and shall ensure that its Subcontractors shall) ensure that all power supplies and fire safety mechanisms in facilities from which Services are provided undergo regular maintenance checks and that facilities comply with Health and Safety regulations.
`

h. Third party shall create and enforce a clear desk policy for papers and removable storage media and a clear screen policy for information processing assets or facilities

12.Operations Security

a. Third Party shall put in place operating procedures to ensure corect and secure operations of GBB information processing facilities or accessing GBB's information

b. Third Party shall control changes to business processes, information processing facilities and systems that affect GBB information or information processing facilities.

c. Third Party shall ensure that development, testing, production and operational environments are separated to reduce the risks of unauthorised access or changes to the operational environment.

d. Third Party shall implement controls against malware for detection, prevention and recovery.

e. The Third Party shall promptly notify GBB in writing as soon as it becomes aware of any viruses in any Third Party Systems or GBB Systems, directly (or indirectly) affecting GBB Information, which have not been auto-corrected or detected and quarantined, and shall provide a written report to the GBB describing the incident, the measures that were taken to resolve the incident and what measures were taken to prevent any reoccurrence.

f. Third Party shall ensure requlars and consistent patching of all softwares being used to managed GBB informtion for the detection, prevention and recovery of relevant information.

g. Third Party shall ensure that backup copies of systems hosting GBB information, software and system images are taken and tested regularly.

h. Third Party shall develop and implement an appropriate internet, email and acceptable use policy and ensure that appropriate controls are in place and documented to prevent unauthorised download of software or web content.

i. Third Party shall develop and implement solutions that record event logs of user activities, exceptions, faults and information security events related to the processing of GBB information.

The log log files must be kept in a secured location protected against unathorized alteration or deletion.

j. Third Party shall ensure the clocks of all relevant information processing systems related to the process of GBB information be synchtronized to a single reference time source.

k. Third Party shall implement procedures to control the installation of software on systems related to the processing of GBB information.

l. Third Party shall put in place mechanisms for managing technical vulnerabilities. Technical vulnerabilities communicated to Third Parties in respect of Third Party's hosted systems or services shall be remediated in a timely manner.

13.Communication Security

a) Third Party shall maintain the confidentiality, integrity, and availability of GBB Information by implementing network controls to protect information in networks, applications and its supporting information processing assets.

b) Third Party shall ensure that networks carrying GBB Information are designed, built, monitored, and managed according to industry standards and best practice.

c) Third Party shall ensure secure transfer of GBB business information between the Third Party and external parties.

14. Information Security Incident Management

a. Third Party shall ensure procedures are in place to ensure consistent and effective approach to the management of information security incidents, events or weaknesses.

b. The Third Party shall at all times maintain a security incident response procedure. Where required by GBB, the Third Party will provide such information regarding information security incidents to the GBB.

c. The Third Party shall require all Third Party personnel to report any observed or suspected security weaknesses in Systems or Services to the Third Party. The Third Party shall inform GBB immediately about any such weaknesses that relates to GBB information or information processing facilities for wich it becomes aware.

d. In the provision of Services to GBB or accessing information or services provided by GBB, if the Third Party becomes or is made aware of any contravention of the information security

requirements under the Contract, or of unauthorised access to GBB information or information processing facilities including GBB network, Third Party shall immediately report the incident to GBB.

15.Business Continuity Management

a. Third Party shall ensure information security continuity is embedded in the Third Party's business continuity management systems.

b. Third Party shall comply with GBB Business Continuity policies notified to the Third Party from time to time.

c. Third Party shall ensure that a Business Continuity Plan is in place in relation to the provision of Services to GBB or access to GBB information or information processing facilities.

16. Compliance

a. Third Party shall at all times ensure that it maintains and abides by an appropriate Data Protection Policy to safeguard GBB Information in accordance with the terms of the Contract and the Nigeria Data Protection Regulation 2019

b. Where any GBB Information is intended to be transferred, stored or processed outside of Nigeria, Third Party shall provide, for GBB written approval, full details of the locations, security arrangements and what information is to be transferred, stored or processed outside of Nigeria.

c. Third party shall manage and process all personal information which they acquire from GBB in accordance with applicable Data Protection regulation.

d. The Third Party shall ensure that appropriate retention and secure deletion/destruction policies and procedures are in place for all GBB Information held.

e. Third Party shall ensure that the storage and subsequent destruction of GBB Information is secure and in compliance with GBB's instructions. All items of equipment used in the provision of the services containing storage media shall be checked by the Third Party to ensure that any GBB Information and licensed software has been removed or securely overwritten prior to secure deletion.

f. If GBB Information is to be shared with a Sub-contractor, the Third Party shall notify GBB in advance and provide GBB with a copy of the legal agreement in place.

g. Legal, regulatory, contractual and service requirements must be complied with and taken into account in the processing of GBB Information. In particular this includes, but is not limited to

compliance with the CyberCrime Act, Data Protection Regulation, Freedom of Information and privacy requirements.

h. Third Party shall grant to the GBB such access to the Sites used as is necessary to allow the GBB to perform its responsibilities or exercise its rights under the Contract and shall participate in information security reviews as and when reasonably requested by the GBB.

17.Information Security Baseline Recommendation

Third Party shall at minimum ensure the following information security baseline:

i. Establish and maintain information security policies and procedures for protecting GBB information
ii. Make personnel be aware of and follow security policies and procedures
iii. Ensure there is an established process for engaging third parties or subcontractors that affect GBB information
iv. Establish and maintain information assets inventory
v. Install anti-malware software with automatic updating
vi. Recognize the importance of passwords
vii. Eliminate vulnerabilities with good system administration
viii. Keep up-to-date backups to allow easy recovery from user mistakes and hardware failure
ix. Minimizing services offered by systems and eliminate unnecessary services
x. Establish and implement incident management process.

18. Declaration

Galaxy Backbone (GBB) Limited is a Governance, Risk and Compliance (GRC) focused organization. GBB has attained external accreditations to diverse industry standards and frameworks. These include but not limited to ISO/IEC 20000-1:2018, ISO/IEC 27001:2013, Payment Card Industry Data Security Standards (PCI DSS) Nigeria Data Protection Regulation (NDPR), among others. GBB shall provide evidence of relevant certification upon request or as the need arises.

19.Contact Us

For more information on Third Party Information Security policy, visit **galaxybackbone.com.ng/Third Party Information Security policy**.

For any questions, comments or clarifications about this policy, kindly contact us:

By Email: information.security@@galaxybackbone.com.ng