Supplier Security Policy

Version 2.0

May, 2020

Revision History

Version	Date	Author	Title	Change Summary
1.0	10-03-2018	Denis Mwaniki	Head of Information Security	Document creation
1.1	31-07-2019	Brenda Wambua	Information Security GRC Officer	Annual review
1.2	07-02-2020	Brenda Wambua	Information Security GRC Officer	Addition of PCI DSS requirements
2.0	22-05-2020	Brenda Wambua Sentinel Africa	Information Security GRC Officer Risk consultants	Annual review Addition of ISO 27701 requirements

Approval

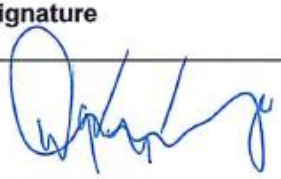
Role	Name	Signature
Head, Technology Operations	George Murage	

Table of Contents

1. Purpose

This policy sets out Cellulant's expectations with respect to protection of its assets accessible to third parties. This Supplier Security Policy demonstrates Cellulant's commitment to safeguarding the confidentiality, integrity and availability of all its physical and operational Information assets that are critical to the provision of its services in accordance with Operational, Contractual and Regulatory requirements.

2. Scope

This policy governs all information that is created, transmitted, processed, stored or disposed during Cellulant business, information assets and the systems used to create and maintain that information.

The scope of this policy applies to procurement and partnership agreements that involve IT solutions or provision of services which require access to/or the processing of confidential data for the delivery and/or support of Cellulant's services and business functions.

3. Policy

Cellulant is committed in accordance with our purpose and values to:

- maintaining and improving information security
- minimizing exposure to risk within the company
- provide and support our services for our customers
- ensure secure and resilient Services
- offer timely and reliable Customer Support services thus enriching the customer experience.

It is Cellulant's policy therefore to ensure that;

a. Information security and privacy risks will be identified and maintained at an acceptable level to ensure procurement of solutions that are able to provide the level and quality of Information Security required

b. Risks resulting from organisational, physical, environmental and emerging technological changes and the use of third parties will be assessed and appropriately managed.

c. Contracts with third parties shall define their information security responsibilities for example in an NDA

d. During the duration of contracts with third parties, Cellulant will manage the relationship to ensure information security is maintained.

e. Cellulant, as appropriate, will allow third parties access to its information/ information systems where a formal contract stating information security responsibilities exist

f. Information security awareness will be made available to all third parties as appropriate

g. Cellulant will specify in its agreements with it partners, suppliers and applicable third parties whether PII is processed and the minimum technical organisation measures that need to be maintained in order to meet its information security and privacy protection obligations

h. All breaches of information security will be reported to and investigated by following the existing Incident Management Procedure

i. Third party access to Cellulant's information/information systems for support and/or maintenance will be monitored and subject to periodic checks

j. Maintenance of a written agreement that includes an acknowledgement that the service providers will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer's cardholder data or sensitive authentication data, or manages the customer's cardholder data environment on behalf of a customer.

k. Maintenance of information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

l. Maintenance of a program to monitor its service providers' PCI DSS compliance status at least annually.

m. Maintenance of a program to monitor third party compliance with relevant and applicable information security and privacy standards at least annually.

4. Responsibilities

4.1. The Chief Technology Officer is the owner of this document and will ensure its revision.