Information Security and Privacy Policy

Version 3.0

April, 2020

Information Security and Privacy Policy Statement

1. The leadership team of Cellulant Corporation Limited located at 2nd and 4th Floor, West Wing, Vienna Court, State House Crescent, Nairobi, Kenya, is committed to preserving the confidentiality, privacy, integrity and availability of all the physical and electronic information assets throughout the organization in order to ensure the achievement of Cellulant business, information security and privacy objectives and compliance with legal, regulatory and contractual requirements. Cellulant leadership team is committed to ensuring the continual improvement of the Information Security and Privacy Information Management Systems.

2. The goal of this policy is the protection of information and information assets related to the delivery of Cellulant services, against internal, external, deliberate or accidental threats. Cellulant is committed to aligning its processes, operations, products and services to ISO 27001:2013, ISO 27701:2019 and PCI DSS requirements.

3. Information is a valuable asset for Cellulant and it exists in many forms; printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. It is the responsibility of ALL staff members to adhere to the requirements laid out in this policy, more specifically;

   a. **It is the responsibility of ALL staff members to:**
      i. Ensure that Information confidentiality will be kept and protected against any unauthorized access
      ii. Ensure Integrity of Cellulant information through protection from unauthorized modification.
      iii. Availability of Cellulant information to authorized users when needed.
      iv. Ensure privacy of Personally Identifiable Information of Cellulant interested parties
      v. Report any security incident or breach to the appropriate staff member according to the Incident Management Policy.
      vi. Undergo appropriate annual security awareness training in support of the goals of this policy.

   b. **It is the responsibility of ALL managers to:**
      i. Implement this policy within their business areas, and make sure it is adhered to by their team members.
      ii. Make sure that all staff within their business area undergoes appropriate annual security awareness training in support of the goals of this policy.

4. Within Cellulant, an Information Security and Privacy Management System (ISMS and PIMS) has been put in place, which includes a risk management framework for the identification, assessment, evaluation and control of all information security and privacy risks. The ISMS and PIMS are subject to continuous and systematic review with improvements, where necessary.

5. Information security and privacy requirements will continue to be aligned with organizational goals and objectives, and are intended to be enabling mechanisms for information sharing, processing, transmitting, storage, electronic operations, e-commerce and reducing information-related risks to acceptable levels.

6. A current version of this document is available to all members of staff. It does not contain confidential information and can be released to relevant external parties. This information security and privacy policy was agreed and approved by the Executive Management and is issued on a version controlled basis under the signature of the Chief Executive Officer (CEO).

7. All employees of Cellulant and related external parties identified are expected to comply with this policy without exception. Any person found to breach this policy or any of the supporting policies, may be subject to the HR disciplinary process, up to and including termination of employment. External parties may be subject to termination of service contract or project assignment. Violation which constitutes unlawful behavior can or will be subject to civil and/or criminal liability.

Approval

Role	Name	Signature
Chief Executive Officer (CEO)	Ken Njoroge	

Revision History

Version	Date	Author	Title	Change Summary
1.0	16-03-2016	William Kiama	Information Sec. Analyst	Initial draft
2.0	12-03-2018	Denis Mwaniki	Head, InfoSec & Risk	Final ISO27001 compliant Policy
2.1	12-06-2019	Brenda Wambua	GRC Officer	Include audit recommendations
3.0	28-04-2020	Brenda Wambua and Sentinel Africa	GRC Officer and Risk Consultant	Annual review Inclusion of ISO 27701 requirements