



Security Classification: Document Reference: /ISRACC/2021/PRGM/001
Version 1
Document Owner: ISRACC

Version and Update History

Date	Document Version	Document Revision History/ Group	Document Author/Reviewer
26-07-2021	1.0	ISRACC	ISRACC






Review Cycle

Change Clause/Frequency
This document is subject to modification on a twelve-month review cycle (regular) or at the instance of a policy review, business rules modification or regulatory requirement.

Distribution List

Name	Title
Musiliu Adeosun	Chief Information Security Officer
Ebenezer Ahisu	Chief Information Officer
Pelumi Alli	Head, Digital and Operational Risk
Edward Onwubuya	Head, Intelligence and Investigation
Temitayo Adegoke	Chief Legal Officer
Ibidapo Martins	Chief Marketing Officer

Approval

<p>Raheem Owodeyi (ED, Operations/COO)</p>	 <p>13/9/2021</p>
<p>Tunde Adeola (ED, Commercial Banking)</p>	
<p>Emmanuel Emefienim (ED, Institutional Banking)</p>	
<p>Yemi Odubiyi (ED, Corporate & Investment Banking)</p>	
<p>Abubakar Suleiman (MD/CEO)</p>	

Sterling Bank Responsible Disclosure Program

Sterling Bank is committed to maintaining the security of our systems and our customers' information. We appreciate and encourage security researchers to contact us to report potential vulnerabilities identified in any product, system, or asset belonging to Sterling Bank.

The trust we have earned from our customers is the most important asset we have, and we will never take it for granted. To maintain trust, we significantly invest in the people, processes and technology needed to keep our customers and their information safe. We also recognize the important role the security research community plays in helping protect the bank from cyber threats. The Sterling Bank Responsible Disclosure Program provides the security research community a channel to communicate directly with Sterling to identify rare but possible vulnerabilities as we all work to maintain the security of the Sterling network (systems and data).

Reporting a Vulnerability

Please report all perceived vulnerabilities by email to sterlingrsdp@sterling.ng. To aid our review, please include as much detail as possible in your report including, but not limited to:

- The full URL.
- Steps taken and any tools used.
- Objects possibly involved (e.g., filters or entry fields).
- Evidence (screen captures).
- Your assessment of perceived risk.
- Any proposed solution.

Sterling Bank will acknowledge your email with an automatic reply. We will contact you as required once we review your findings. We appreciate all reports but may not be able to share specific investigative steps or resolution(s) with you.

Guidelines for Reporting

To ensure a collaborative approach, please respect the guidelines set out below.

- You are contacting us in your personal capacity and are at least 18 years of age or have your parent or guardian's permission to contact us if less than 18 years. If you are making such report on behalf of an organization, you will report the vulnerability by including the name of the organization in your submission.
- You will not engage in any activity that could harm Sterling Bank, our customers, employees, services and/or assets.
- You agree not to destroy, modify data, or attempt to interrupt or degrade our services in anyway.
- You will not share, compromise, or disclose any personally identifiable information (PII). Examples of PII include all information that personally identifies a person, including first names and/or surnames, date and place of birth, Bank Verification Number (BVN), etc.
- You will only conduct security and vulnerability research with accounts you own or with the express consent of the account holder. You will not use social engineering or brute force methods to attempt to obtain confidential credentials.
- You agree to comply with all applicable laws and regulations in connection with your security research activities and your participation in Sterling Bank Responsible Disclosure Program.
- You will allow us a reasonable opportunity to investigate and respond prior to contacting anyone else about the identified issue.

By responsibly submitting your findings to Sterling Bank following these guidelines, Sterling Bank agrees not to pursue legal action against you. Sterling Bank reserves all legal rights in the event of non-compliance with these guidelines.

Sterling Bank Responsible Disclosure Program

Services in Scope

Any Sterling Bank owned website, web-service or mobile application that handles reasonably sensitive user data is intended to be in scope. Examples include virtually all contents in the following domains:

- sterling.ng
- saf.ng
- Sterling mobile applications for Android, IOS
- Product websites and applications (e.g., Double, Specta, i-invest, etc.).