Vulnerability Disclosure Policy

Capitec is committed to safeguarding and protecting our information and any other information entrusted to us.

We take cyber security very seriously and recognise the importance of privacy and cyber security. We are committed to addressing and reporting security issues through a coordinated and constructive process, designed to drive the greatest protection for technology users, and protection of Capitec information, along with information relating to our customers and employees.

When appropriately notified of legitimate issues, we will do our best to acknowledge your vulnerability report, assign resources to investigate the issue, and fix potential problems as quickly as possible.

Reporting security issues

If you believe you have discovered a vulnerability in a Capitec asset / system or have a security incident to report, please send an email to cyberdefence@capitecbank.co.za.

In all cases, you must:

- Respect our privacy, which includes the privacy of our employees, clients and 3rd parties. Contact us immediately if you access anyone else's data, personal, financial, or otherwise. This includes usernames, passwords and other credentials. You must not save, store, process or transmit this information.
- Act in good faith. You should report the vulnerability to us without any conditions attached.
- Work with us. Promptly report any findings to us, stopping after you find the first vulnerability and requesting permission to continue testing. Allow us a reasonable amount of time to resolve the vulnerability before publicly disclosing it.

And you must not:

- Exfiltrate data.
- Exploit a vulnerability or disable further security controls.
- Perform social engineering activities.
- Use automated scanners.

Next Steps

Upon receipt of vulnerability / security report, Capitec will undertake a series of steps to address the issue:

1. Capitec requests the reporter keep any communication regarding the vulnerability confidential.
2. Capitec investigates and verifies the vulnerability.
3. Capitec addresses the vulnerability and releases an update or patch to the software. If for some reason this cannot be done quickly, or at all, Capitec will provide information on recommended mitigations.
4. Capitec endeavours to keep the reporter apprised of every step in this process as it occurs.

We greatly appreciate the efforts of security researchers and discoverers who share information on security issues with us, giving us a chance to improve our products and services, and better protect our clients. Thank you for working with us through the above process.

T +27 21 809 5900 **E** enquiries@capitecbank.co.za
5 Neutron Road, Techno Park, Stellenbosch, 7600 PO Box 12451, Die Boord, Stellenbosch, 7613 capitecbank.co.za