## Request for penetration testing of FINCA Bank Georgia’s IT systems

JSC FINCA Bank Georgia is a part of FMH (FINCA Microfinance Holding). Its Partners are IFC, World Bank Group, KFW, Bankengruppe, FMO, Development Bank of Germany, Development Bank of Netherlands, responsAbility GLobal Microfinance Fund, Triple Jump and other international financial organizations. FINCA Bank Georgia serves more than 80000 clients through 39 service centers in almost all regions of Georgia.

FINCA Bank Georgia Branch of FINCA International Inc. – a fund in Partnership with the international community was established in Georgia in May 1998 by support of the US Agency for International Development and US Department of Agriculture. For more information visit: [www.FINCA.org](http://www.FINCA.org), [www.FINCA.ge](http://www.FINCA.ge)

FINCA Bank Georgia conducts its activities according to the highest ethical and professional standards and as per Bank’s internal regulation, customer employees and/or their related persons shall not have direct or indirect financial interests with the Vendors or other Service Providers of the Customer (Conflict of Interest). Therefore, there should be no kind of Conflict of Interest with the Supplier and Customer employees and/or related person.

## Purpose:

* #1: Detection of information security vulnerabilities in FINCA Bank’s IT systems;
* #2: Fulfillment of the request of National Bank of Georgia

## Project Scope

Defined IT systems will be scanned and tested for known vulnerabilities. Detected risks will be analyzed and sorted according to impact and risk level. System architecture and design will be studied to identify and suggest security best practices. Finally, detailed actions will be suggested to mitigate identified risks.

* Testing will be done on IT systems which are reachable from Internet (External Penetration Test);
* Known vulnerabilities will be identified and analyzed for possible manipulations;
* Possible exploitation of vulnerability will be appropriately proven;
* Risk assessment of tested applications/services will be conducted;
* Recommendations on mitigation will be provided for identified risks;
* Expert evaluation and consulting on IT infrastructure design and security of its components will be provided.

Components to be evaluated:

* Internet Bank
* Mobile bank
* Microsoft Exchange - OWA
* Corporate website
* Network devices:
	+ Remote VPN
	+ Internet Router
	+ Internet Firewall

Following optional items should be provided separately

* Social Engineering (Mail Phishing);
* Evaluation and vulnerability testing of office WIFI network.

Note:

* Internet and mobile bank systems will also be tested from customer portal;
* Black / Gray box type testing will be used.

## Testing Scenarios

 Penetration test should include (but not be limited to) following steps:

1. Research and description;
2. Evaluation of network components and identification of services;
3. Network penetration test;
4. Password hijacking;
5. Manual testing / OWASP methodology
	1. Access Control
	2. Authentication
	3. Session Control
	4. Configurations / revision of web application architecture
	5. Error processing
	6. Data Protection

Note: FINCA Bank should be notified in advance before

## Candidate evaluation criteria

Candidate should provide documentation at FINCA Bank’s head office in sealed envelopes, on the following address: Vazha- Pshavela Av. 71, Block 1, Floor3, Office 12, Tbilisi, Georgia; **Deadline Is April 19th, 2017 18:00**;

For additional information contact us on the following e-mail: procurement@finca.ge

 Only short-listed candidates will be contacted and invited for an interview. All short-listed candidates will be notified (via e-mail) about the outcome. **Following documentation is required:**

* Description of the methodology used;
* Experience in relevant field:
	+ Evaluator should have at least 5 years of experience in relevant field and should provide short description, scale and number of implemented projects.
	+ Minimum 1 recommendation letter about successful implementation of similar projects (would be a plus).
* Project timeline and completion time;
* Total price of the project (Social Engineering and WIFI test prices should be provided separately);
* Evaluator should have permanent staff of experts with relevant certification (OSCP, CCIE/CCNP Security, CPTE, etc.) Candidate should provide list of certificates and number of certified staff.

## Final Report

The full report should be presented in English language (additional short report in Georgian is also required) and should contain at least the following:

* Executive summary;
* Risk analysis;
* Recommendations;
* Detailed description of carried out actions and findings;

Evaluator should make a power-point presentation about detected vulnerabilities, risks and possible solutions and present it to FINCA Bank’s responsible personnel. Evaluator is required to immediately inform the Bank once critical vulnerability is detected.