1. Introduction

The purpose of this document is to layout the procedures and establish the rules for collaboration with security researchers when security tests are performed against TBI Bank Group environment. This program is following Information Security Best practices. Such procedure is used in many Financial institution in Europe. The goals of this policy are:

- to determine whether and how a malicious user can gain unauthorized access to assets that affect the fundamental security of the system, files, logs and/or sensitive data
- to confirm that the applicable controls, such as scope, vulnerability management, methodology, and segmentation are in place.

2. Scope

Scope of this policy covers all the assets of: TBI Bank EAD, TBI Bank EAD Sofia – Branch Bucharest, TBI Credit IFN S.A. (Romania), TBI Leasing IFN S.A. (Romania). This Program covers mixed environment including all systems, applications, webservices, APIs, mobile and all targets part of the infrastructure of the bank.
Issues reported are only valid if they relate to code that is used in production environment.

3. Rules of Engagement

By submitting reports or otherwise participating in this program, you agree that you have read and will follow the Program Rules and Legal Terms sections of this program Policy.

3.1. Program Rules

Violation of any of these rules can result in ineligibility for a bounty and/or removal from the program.

- Never use a finding to compromise/exfiltrate data or pivot to other systems. Use a proof of concept only to demonstrate an issue.
- If sensitive information--such as personal information, credentials, etc.--is accessed as part of a vulnerability, it must not be saved, stored, transferred, accessed, or otherwise processed after initial discovery. All copies of sensitive information must be returned to TBI Bank and may not be retained.
- Researchers may not, and are not authorized to, engage in any activity that would be disruptive, damaging or harmful to TBI Bank, its brands or its users. This includes: social engineering, phishing, physical security and denial of service attacks against users, employees, or TBI as a whole.
- Researchers may not publicly disclose vulnerabilities (sharing any details whatsoever with anyone other than authorized TBI employees), or otherwise share vulnerabilities with a third party, without TBI express written permission.

3.2. Legal Terms

In connection with your participation in this program you agree to comply with TBI's General Terms and Conditions, TBI's Privacy Policy, and all applicable laws and regulations, including any laws or regulations governing privacy or the lawful processing of data.

TBI reserves the right to change or modify the terms of this program at any time.

TBI does not give permission/authorization (either implied or explicit) to an individual or group of individuals to extract personal information or content of TBI users or publicize this information on the open, public-facing internet without user consent or modify or corrupt programs or data belonging to TBI in order to extract and publicly disclose data belonging to TBI.

TBI employees (including former employees that separated from TBI within the prior 12 months), contingent workers, contractors and their personnel, and consultants, as well as their immediate family members and persons living in the same household, are not eligible to receive bounties or rewards of any kind under any TBI programs, whether hosted by TBI or any third party.

4. Safe Harbor

TBI will not initiate a lawsuit or law enforcement investigation against a researcher in response to reporting a vulnerability if the researcher fully complies with this Policy.

Please understand that if your security research involves the networks, systems, information, applications, products, or services of another party (which is not us), that third party may determine whether to pursue legal action. We cannot and do not authorize security research in the name of other entities. If legal action is initiated by a third party against you and you have complied with this Policy, we will take reasonable steps to make it known that your actions were conducted in compliance with this Policy.

You are expected, as always, to comply with all applicable laws and regulations.

Please submit a report to us before engaging in conduct that may be inconsistent with or unaddressed by this Policy.

Please note: going public with your finding before we have fixed it will exclude you from the “reward”. Instead, please talk to our experts and give them time to assess and solve the problem.

5. Responsible Disclosure of Vulnerabilities

We are continuously working to evolve our bug bounty program. We aim to respond to incoming submissions as quickly as possible and make every effort to have bugs fixed within **120 days** of being triaged.

The Penetration Tester shall remove all data related to the IT Security Penetration test for each site from the Pen Tester's computer(s) by a method approved by the TBI.

All documents, data logs/files, test results, and working papers generated by the Pen Tester for the IT Security Penetration test at each site shall not be retained by the Pen Tester and shall be provided to TBI. All data become property of TBI and be retained by Information security department.

Report should be created in two versions - Executive summary and detailed report. All files containing sensitive data should be transferred over encrypted channel.

Separate report has to be presented for Card Operation (PCI DSS scope) and for SWIFT environment.

6. Testing

Please do the following when participating in bug bounty program:

- Provide your IP address in the bug report. We will keep this data private and only use it to review logs related to your testing activity.
- Include a custom HTTP header in all your traffic. Burp and other proxies allow the easy automatic addition of headers to all outbound requests. Report to us what header you set so we can identify it easily. For example:
    - A header that includes your username: *X-Bug-Bounty:HackerOne-<username>*
    - A header that includes a unique or identifiable flag *X-Bug-Bounty:ID-<sha256-flag>*

When testing for a bug, please also keep in mind:

- Only use authorized accounts so as not to inadvertently compromise the privacy of our users
- When attempting to demonstrate root permissions with the following primitives in a vulnerable process please use the following commands:
    - Read: *cat /proc/1/maps*
    - Write: *touch /root/<your H1 username>*
    - Execute: id, hostname, pwd (though, technically cat and touch also prove execution)
- Minimize the mayhem. Adhere to program rules at all times. Do not use automated scanners/tools - these tools include payloads that could trigger state changes or damage production systems and/or data.
- Before causing damage or potential damage: Stop, report what you've found and request additional testing permission.

7. Crafting a Report

If our security team cannot reproduce and verify an issue, a bounty cannot be awarded. To help streamline our intake process, we ask that submissions include:

- Description of the bug
- Description of the attack scenario
- The impact of this scenario
- Steps to reproduce the reported vulnerability
- Proof of exploitability (e.g. screenshot, video)
- Perceived impact to another user or the organization
- List of URLs and affected parameters
- Other vulnerable URLs, additional payloads, Proof-of-Concept code
- Browser, OS and/or app version used during testing
- Bug resolution and fix.

Note: Failure to adhere to these minimum requirements may result in the loss of a reward.

All supporting evidence and other attachments must be stored only within the report you submit. Do not host any files on external services.

7.1. Same Bug, Different Host

For each report, please allow TBI sufficient time to patch other host instances. If you find the same bug on a different (unique) host, prior to the report reaching a triaged state, file it within the existing report to receive an additional 10% bonus (per host, not domain). Any reports filed separately while we are actively working to resolve the issue will be treated as a duplicate.

7.2. Same Payload, Different Parameter

In some cases, rewards may be consolidated into a single payout. For example, multiple reports of the same vulnerability across different parameters of a resource, or demonstrations of multiple attack vectors against a fundamental framework issue. We kindly ask you to consolidate reports rather than separate them.

8. Rewards

To encourage reporting vulnerabilities to TBI, we would urge you to send any vulnerabilities you detect to us. As mentioned, you may receive a reward. The amount of the reward depends on the severity of the vulnerability reported, the type of website (static information sites versus online banking sites) concerned and the quality of the report we receive. If the report is of great value for the continuity and reliability of the bank, the reward will be considerably higher.

You will be eligible for a bounty only if you are the first person to disclose an unknown issue. Qualifying bugs will be rewarded based on severity, to be determined by TBI in its sole discretion. Awards are granted entirely at the discretion of TBI.

At TBI discretion, providing more complete research, proof-of-concept code and detailed write-ups may increase the bounty awarded. Conversely, TBI may pay less for vulnerabilities that require complex or over-complicated interactions or for which the impact or security risk is negligible. Rewards may be denied if there is evidence of program policy violations.

Rewards will be declined if we find evidence of abuse.

8.1. Valued Vulnerabilities

This table is a general guide for how we may classify vulnerabilities, ranked by severity from highest to lowest (within their severity class). This table serves only as a guide and the severity classification of a particular vulnerability will be determined by TBI in its sole discretion.

Note: Non-listed vulnerabilities may also be eligible. Some vulnerability types may fall under a variety of severity ratings determined by scope/scale of exploitation and impact.

Severity	Short Name	Full Name
Critical	RCE	Remote Code Execution
Critical	SQLi	SQL Injection
Critical	---	Privilege Escalation to System Account
Critical	XXE	XML External Entity
Critical	XMLi	XML Injection
High	VPE	Vertical Privilege Escalation
High	IDOR	Insecure Direct Object Reference
High	SSRF	Server-Side Request Forgery

High	---	Authentication or Authorization Bypass
High	LFI	Local File Inclusion
High	ATO	Account Takeover
High	SSI	Server-Side Inclusions Injection
High	---	S3 Bucket Upload
High	---	Mass PII Extraction
Medium	SSRF	Blind & HTTP Response Status Based SSRF
Medium	XSS	Stored Cross-Site Scripting
Medium	UE	PII User Enumeration
Medium	CSRF	State Changing Cross-Site Request Forgery
Medium	---	Privileged Account Credentials Identified
Medium	HPE	Horizontal Privilege Escalation
Medium	CRLFi	CRLF Injection
Medium	SDTO	Subdomain Takeover
Medium	---	Sensitive Data Exposure
Low	gXSS	GET-based Reflected Cross-Site Scripting
Low	pXSS	POST-based Reflected Cross-Site scripting
Low	dXSS	DOM-based Cross-Site Scripting
Low	nCSRF	Non-State Changing Cross-Site Request Forgery
Low	---	Dangling DNS Record
Low	---	Cleartext Submission of Passwords
Low	fXSS	Flash-based Cross-Site Scripting
Low	---	MySQL Information page with credentials
Low	---	Open Redirect
Low	---	Server Information Page (with credentials)
Low	---	Server Information Page (without credentials)
Low	---	Confidential Data Disclosure
None	---	Non-Sensitive Data Disclosure

8.2. Borderline Out-of-Scope, No Bounty

These issues are eligible for submission, but not eligible for bounty or any award. Once triaged, they will be closed as Informative only if found to be valid or Spam if found to be not valid. When reporting vulnerabilities, please consider attack scenario / exploitability, and security impact of the bug.

Any non-TBI Media Applications	"Self" XSS
Missing Security Best Practices	HTTP Host Header XSS
Confidential Information Leakage	Clickjacking/UI Redressing
Use of known-vulnerable library (without proof of exploitability)	Intentional Open Redirects
Missing cookie flags	Reflected file download
SSL/TLS Best Practices	Incomplete/Missing SPF/DKIM
Physical attacks	Social Engineering attacks
Results of automated scanners	Login/Logout/Unauthenticated CSRF
Autocomplete attribute on web forms	Using unreported vulnerabilities
"Self" exploitation	Issues related to networking protocols
XSS in flash files not developed by TBI	Software Version Disclosure

Verbose error pages (without proof of exploitability)	Denial of Service attacks
TBI software that is End of Life or no longer supported	Account/email Enumeration
Missing Security HTTP Headers (without proof of exploitability)	Internal pivoting, scanning, exploiting, or exfiltrating data

Note: 0-day vulnerabilities may be reported 60 days after initial publication. We have a team dedicated to tracking these issues; hosts identified by this team and internally ticketed will not be eligible for bounty.

9. Out of Scope

The following issues are considered out of scope:

- Those that resolve to third-party services
- Issues that do not affect the latest version of modern browsers
- Issues that we are already aware of or have been previously reported
- Issues that require unlikely user interaction
- Disclosure of information that does not present a significant risk
- Cross-site Request Forgery with minimal security impact
- CSV injection
- Incomplete or missing SPF/DKIM
- General best practice concerns