የኢትዮጵያ ንግድ ባንክ
Commercial Bank of Ethiopia

Security Vulnerability Disclosure Standard Procedure

INFORMATION SYSTEMS DIVISION

February 2023

This page is left intentionally

Acronyms

Terms	Definition
CBE	Commercial Bank of Ethiopia
IS	Information Systems Security
ISS	Information Systems
INSA	Information Network Security Administration
API	Application Programming Interface
SSL	Secure Sockets Layer
SQL	Structured Query Language
DoS	Denial of Service
DDoS	Distributed Denial of Service
HTTP	Hypertext Transfer Protocol
UI/UX	User Interface and User eXperience
CSRF	Cross-Site Request Forgery
XSS	Cross-Site Scripting
HTML	HyperText Markup Language
CLI	Command Line Interface

1 INTRODUCTION

1.1 Preamble

Whereas, Cybercrime is increasing exponentially and becoming a global problem due to organizations' fast digital transformation and the growing sophistication of threats.

Whereas, the Commercial Bank of Ethiopia (CBE) is committed to maintaining the security of its banking systems and protecting sensitive information from unauthorized disclosure.

Whereas, CBE identifies and manages vulnerabilities that exist in its infrastructure. However, the security professional that can be hired is often minimal, ethical security researchers can help in identifying vulnerabilities that are left unidentified by the internal security team.

Whereas, safe and clear communication is needed so that goodwill security researchers ethically engage with CBE.

Now, therefore, this Standard Procedure is issued per international vulnerability disclosure policy templates and CBE's internal Information System Security Policy. It describes **what systems and types of research** are covered under this Procedure, **how to send** vulnerability reports, and **how long** CBE asks security researchers to wait to fix the security issue. If you are a security researcher and have discovered a security vulnerability in one of our services and infrastructure, CBE appreciates your help in disclosing it responsibly. The Bank will validate and fix vulnerabilities under this standard procedure and CBE's internal security policies. CBE reserves all its legal rights in the event of any non-compliance to the applicable laws and regulations.

1.2 Short Title

This document can be cited as "**CBE Vulnerability Disclosure Standard Procedure**".

1.3 Definition of Terms

a. **Availability:** Means the state of being accessible and usable upon demand by an authorized person or entity.

b. **Best Practice:** Means a standard, a set of guidelines, or a recommended checklist that is known to produce a good outcome in protecting an organization's information, resources, or business operations if followed.

c. **Confidentiality:** Means ensuring that information is made available or disclosed only to those individuals, entities, or processes authorized to have access.

d. **Command-line interface access:** Means gaining access to the infected CLI without connecting to the actual computer.

e. **Cross-site scripting:** Means a type of injection attack that injects malicious code into otherwise safe websites.

f. **DoS/DDoS:** Means an attack type in which an attacker makes the system or data unavailable to someone who needs it. In the case of distributed denial-of-service (DDoS), the attacks come from many distributed sources.

g. **Exfiltrate data:** Means an unauthorized transfer of data from a computer.

h. **Ethical hacker:** Means a person or company doing an authorized practice of detecting vulnerabilities in an application, system, or organization's infrastructure and identifying potential data breaches and threats in the organization's infrastructure and service.

i. **Integrity:** Means safeguarding the accuracy and completeness of assets/data.

j. **Security researcher:** Means skilled experts that use their technical knowledge to identify vulnerabilities.

k. **Phishing:** Refers to the type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware.

l. **Pivoting:** Means the act of an attacker moving from one compromised system to one or more other systems within the same or other organizations.

m. **Physical testing:** Means assessing all physical security controls, including locks, fences, security guards, cameras, and other security measures.

n. **Sensitive Data:** Means confidential information/data that must be kept safe and out of reach against unwarranted disclosure.

o. **Security Breach:** Means any incident that results in unauthorized access to computer data, applications, networks, or devices.

p. **Social Engineering:** Refers to a manipulation technique that exploits human error to gain private information, access, or valuables.

q. **The Bank** refers Commercial Bank of Ethiopia (CBE).

r. **Transport Layer Security (TLS):** Refers to a cryptographic protocol designed to protect data sent over the internet. It is used to prevent data from being eavesdropped on or tampered with. Currently at version 1.3 and the minimum version recommended to be used is TLS1.2.

s. **Vishing:** Refers to the type of phishing that uses the phone to steal personal confidential information from victims.

t. **Vulnerability:** Means the weakness of an asset or control that can be exploited by one or more threats.

u. **Vulnerability Disclosure:** Refers to the practice of reporting security flaws in computer software or hardware.

v. **Zero-day vulnerabilities:** Means a vulnerability in a system or device that has been disclosed but is not yet patched.

1.4 The objective of the Standard Procedure

The objective of this standard procedure is to set the rules of engagement for an ethical security researcher to identify and submit security vulnerabilities in a responsible and accountable manner. The document establishes an engagement and communication framework for researching and reporting discovered security weaknesses and vulnerabilities.

1.5 Governing Rules

This Standard Procedure shall be governed by:

- National Computer Crime Prevention Proclamation No.958/2016;
- National Information Security Policy 2011;
- National Bank of Ethiopia (NBE) policies and directives;
- CBE Compliance Policy;
- CBE's Information Systems Security Policy.

2 SCOPE

2.1 Scope of the standard procedure

This standard procedure applies to all ethical hackers and security researchers, internal or external to CBE. However, the below-listed in-scope and out-of-scope systems, services, and activities should be considered.

2.2 In Scope

All internet-accessible and public-facing systems and services of CBE are covered within the scope of this Standard Procedure, including:

- Internet-facing services:
  - *.cbe.com.et,
  - *.cbeib.com.et,
  - *.combanketh.et,
  - *.cbebirr.com.et,
- Mobile Applications provided by the bank, and
- Any Desktop (If any).

Any services not expressly listed above, such as any connected services, are excluded from the scope and are not authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of this standard procedure's scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren't sure whether a system is in scope or not, contact CBE at mailto:cybersecurity@cbe.com.et before starting your research.

2.3 Out of Scope

In addition to the above scoping, please consider the following out-of-scope activities, systems, and services:

a) Any services and systems hosted by 3rd party providers and integrators are excluded from the scope.
b) Not original, previously reported, and already discovered by internal procedures.
c) Volumetric vulnerabilities are not in scope - meaning that simply overwhelming a service with a high volume of requests is not in scope.
d) Reports of non-exploitable vulnerabilities, or reports indicating that our services do not fully align with "best practice", for example missing security headers, are not in scope.
e) TLS configuration weaknesses, for example, "weak" cipher suite support or the presence of TLS1.0 support, are not in scope.

In addition to this, please refer to ***Section 5*** for activities and testing rules that security researchers or ethical hackers are not permitted to perform.

3 AUTHORIZATION AND LEGAL EXPOSURE

Security researchers must comply with all applicable international, national, or CBEs internal laws, regulations, and policies in connection with security research activities. CBE does not authorize, permit, or otherwise allow (expressly or implied) any person, including any individual, group of individuals, consortium, partnership, or any other business or legal entity to engage in any security research or vulnerability or threat disclosure activity that is inconsistent with this standard procedure or the law.

Security researchers may be subject to fines, imprisonment, or other penalties if they engage in any activities in violation of this standard procedure or the law, including unauthorized attempts to access, obtain, upload, modify, change, and/or delete information on this system, which are strictly prohibited and are subject to criminal prosecution under:

- Ethiopian Computer Crime Proclamation 958/2016;
- CBE's policies including Information Systems Security Policy;
- Other national applicable laws and regulations.

If you make a good-faith effort to comply with this Standard Procedure during your security research, we will consider your research to be authorized. CBE will work with you to understand and resolve the issue quickly, and *CBE* will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted per this Standard Procedure, we will make this authorization known.

4 GUIDELINES

Under this Standard Procedure, "research" means activities in which you:

- ✓ Notify CBE as soon as possible after you discover a real or potential security issue.
- ✓ Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- ✓ Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command-line access, or use the exploit to pivot to other systems.
- ✓ Provide a reasonable amount of time, **at least 120 working days,** to resolve the issue before you disclose it publicly or request an explanation. CBE has a security patch management standard procedure and will follow it to address the reported issue.
- ✓ Do not submit a high volume of low-quality reports.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, proprietary information, or trade secrets of any party), **you must stop your test, notify CBE immediately, and not disclose this data to anyone else**.

5 TESTING RULES

Security researchers **must NOT**:

- Test any system or service other than those listed above,
- Perform Network Denial of Service (DoS or DDoS) tests or other tests that impair access to or damage/disable a system or data,
- Test Physical testing (e.g., office access, open doors, tailgating), social engineering (e.g., phishing, vishing), or any other non-technical vulnerability testing.
- Disclose vulnerability information except as outlined in the 'How to Report a 'Vulnerability' and 'Disclosure' sections below.
- Introduce malicious software to CBE infrastructure,
- Test third-party applications, websites, or services that integrate with or link to or from CBE systems or services.
- Do not use an exploit to exfiltrate data, establish command-line access, establish a persistent presence on CBE systems or services, or "pivot" to other CBE systems or services.
- Do not use social engineering to gain access to a system.

6 DISCLOSURE

Information submitted under this Standard Procedure will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely CBE, we may share your report with the Information Network Security Administration (INSA), other banks, and Cybersecurity Agencies, where it will be handled under their policies. We will not share your name or contact information without express permission.

What you expect from CBE

We accept vulnerability reports via cybersecurity@cbe.com.et. Reports may be submitted anonymously. However, when you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible:

- We will acknowledge receipt of your report within 5 business days.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.
- CBE does not provide any recognition or reward payment for submitting the vulnerabilities. However, in return, CBE will not recommend or pursue legal action related to your research if you report your research to CBE following this standard procedure.

7 HOW TO REPORT A VULNERABILITY

To help triage and prioritize submissions, CBE recommends that your reports shall:

- be in acceptable message formats are plain text, rich text, and HTML,
- provide a detailed technical description of the steps required to reproduce the vulnerability, including a description of any tools needed to identify or exploit the vulnerability,
- contain and attached Images, e.g., screen captures, and other documents. It is helpful to give attachments illustrative names,
- include proof-of-concept (PoC) code that demonstrates exploitation of the vulnerability. We request that any scripts be embedded into non-executable file types. We can process all common file types as well as file archives including .zip, .7zip, and .gzip,
- in English, if possible.

8 MISCELLANEOUS

8.1 Enforcement

a) All ethical hackers or security researchers, internal or external, have a responsibility to follow this standard procedure.

b) Violation of this requirement will result in Legal action since it is a violation of the Computer Crime Prevention Proclamation No.958/2016 and the CBE's internal regulations and Security Policy.

8.2 Revision

a) This standard procedure document shall be reviewed and updated every two years, or on-demand when new major security practices and standards are introduced globally or internally.

b) CBE may modify or terminate this standard procedure at any time in its sole and absolute discretion.

8.3 Effective Date

a) This standard procedure document shall become effective upon the date approved by the Bank.

8.4 Document Change History

Version	Date	Description
1.0	25/03/2023	First Issuance

9 Questions and Contacts

Use the following contacts for any inquiry or submit security findings: informationsecurity@cbe.com.et or cybersecurity@cbe.com.et. We also invite you to contact us with suggestions for improving this Standard Procedure.