



VULNERABILITY DISCLOSURE POLICY

Table of Contents

1. OVERVIEW	2
2. PURPOSE AND BENEFITS	2
3. SCOPE	2
4. REPORTING VULNERABILITY	3
5. SUBMISSION	3
6. HANDLING OF REPORTED VULNERABILITIES	4
7. ACKNOWLEDGEMENT OF REPORTED VULNERABILITIES	5
8. TERMS AND CONDITIONS OF VULNERABILITY DISCLOSURE	5
9. REPRESENTATION OF WARRANTIES	6
10. LEGAL CONSIDERATIONS	7
11. CONFIDENTIALITY	8

1. OVERVIEW

This policy harnesses the power of crowdsourcing by creating a channel for ethical hackers, security researchers and the public to report security vulnerabilities to Mauritius Telecom Group (MTG), ensuring that the vulnerabilities are addressed before they can be exploited by malicious actors.

2. PURPOSE AND BENEFITS

The purpose of this policy is to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey MTG preferences in how to submit discovered vulnerabilities to us.

3. SCOPE

This policy applies to everyone except for the MTG's partners and employees.

At this time, the scope of this policy is limited to security vulnerabilities found within MTG public-facing online environment. This includes, but is not limited to, MTG's websites, exposed APIs and mobile applications. The vulnerabilities shall be original, previously unreported, and not already discovered by internal procedures.

The Policy **does not apply** to following vulnerabilities:

- Network level Denial of Service attacks.
- Application Denial of Service by locking user accounts.
- Descriptive error messages or headers (e.g. Stack Traces, banner grabbing).
- Disclosure of known public files or directories, (e.g. robots.txt).
- Outdated software / library versions.
- OPTIONS / TRACE HTTP method enabled.
- CSRF on logout.
- CSRF on forms that are available to anonymous users.
- Cookies that lack HTTP Only or Secure settings for non-sensitive data.
- Self-XSS and issues exploitable only through Self-XSS.
- Reports resulting from automated scanning utilities without additional details or a POC demonstrating a specific exploit.
- Attacks requiring physical access to a user's device.
- Attacks dependent upon social engineering of MT employees or vendors.
- Username enumeration based on login or forgot password pages.
- Enforcement policies for brute force, rate limiting, or account lockout.

- SSL/TLS best practices.
- SSL attacks such as BEAST, BREACH, Renegotiation attack.
- Clickjacking, without additional details demonstrating a specific exploit.
- Mail configuration issues including SPF, DKIM, DMARC settings.
- Use of a known-vulnerable library without a description of an exploit specific to our implementation.
- Password and account recovery policies.
- Presence of autocomplete functionality in form fields.
- Publicly accessible login panels.
- Lack of email address verification during account registration or account invitation.
- Lack of email address verification password restore.
- Tab napping
- Session control during email/password changes.
- This Policy applies to

4. REPORTING VULNERABILITY

Vulnerability information is extremely sensitive. You are required to report the potential security issue to MT Security Department, at securityreporting@telecom.mu and include the following information in the report:

- Organisation and contact name.
- Your Reference / Advisory Number
- Products or solutions and versions affected.
- Description of the location and potential impact of the vulnerability
- Supporting technical details (such as system configuration, traces, description of exploit/attack code, sample packet capture, proof of concept, steps to reproduce the issue)
- Information about known exploits.
- Disclosure plans if any
- Signature of our secrecy agreement

5. SUBMISSION

Your submitted report shall provide:

- Details of the vulnerability, including information needed to reproduce and validate the vulnerability and a Proof of Concept (POC).
- A clear description of the issue, including the impact you believe it has to the user, MT or others.
- Specific reproduction steps including the environment used for testing (browsers, devices, tools, configuration) and any accounts used during testing.
- Your recommendations for remediating the vulnerability.

Requests for exceptions to this policy shall be approved by the respective Chief/Head. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein.

6. HANDLING OF REPORTED VULNERABILITIES

The Company is committed to resolving the reported issue as soon as feasible. We shall refrain from sharing your report with others while we resolve the matter.

Within 24 hours of submitting your vulnerability report, you will receive an acknowledgment from our security team. They will provide you with a unique reference number to be used in all further communication and correspondence regarding the reported vulnerability. At this stage, we may also request any additional supporting documentation, such as a 'proof of concept', to help us better understand and validate the issue.

If your reported vulnerability is in line with this Policy, we will collaborate with you in understanding, confirming, and addressing the vulnerability in a manner commensurate with the assessed risk. We are committed to resolving the issue within 90 days or less.

Please note that if we do not receive a response from you within 48 hours of our initial contact, we will not make any further attempts to re-engage with you beyond this timeframe.

7. ACKNOWLEDGEMENT OF REPORTED VULNERABILITIES

We greatly appreciate the efforts of security researchers who dedicate their time and expertise to identifying and reporting security vulnerabilities to us in accordance with this Vulnerability Disclosure Policy. Your contributions play a crucial role in helping us maintain a secure environment for our infrastructure and systems.

Our security team will carefully evaluate each submitted report based on its severity, impact, and quality. We are committed to investigating and addressing valid security vulnerabilities that are reported to us.

Please note that there may be instances where we determine that a reported vulnerability has an acceptable level of risk, and we may choose not to make changes in such cases.

While we value the contributions of security researchers, we do not operate a bug bounty or hall of fame program. Our primary focus is on acknowledging and addressing the reported vulnerabilities to ensure the security of our systems and infrastructure.

The Company reserves the right to determine the eligibility of a submitted vulnerability and to modify or discontinue any aspect of this Vulnerability Disclosure Policy at any time without prior notice. All decisions made by us regarding the handling of reported vulnerabilities are final and binding.

8. TERMS AND CONDITIONS OF VULNERABILITY DISCLOSURE

By making a report to the Company, or communicating a report to MT regarding vulnerabilities and errors, or otherwise through your participation in our Vulnerability Disclosure Program, you agree to be bound by the following terms and conditions:

- a. You will comply with the guidelines outlined in this Vulnerability Disclosure Policy and grant the Company a worldwide, royalty-free, non-exclusive license to use your submission for the purpose of addressing vulnerabilities.
- b. Only the first report of a previously unidentified issue will be considered. In the event of multiple submissions for the same vulnerability, only the earliest received report will be considered.
- c. It is your responsibility to notify us of any changes to your contact information, including your email address. Failure to provide accurate and up-to-date contact information may result in the inability to acknowledge your contribution or communicate with you regarding your submission.
- d. You agree not to disclose and/or share to any third party any information related to your report, the vulnerabilities and/or errors reported, or any other vulnerabilities or potential vulnerabilities discovered, nor the fact that vulnerabilities and/or errors has been reported to the Company.
- e. Share your report in English.
- f. You have not engaged, and will not engage, in testing/research on our systems, platforms, products and services with the intention or effect of causing damage, losses or any harm to the Company, its customers, employees, partners or suppliers.

- g. You have not used, misused, deleted, altered or destroyed, and will not use, misuse, delete, alter or destroy, any data that you have accessed or may be able to access in relation to the vulnerability and/or error discovered.
- h. You must not intentionally harm the experience or usefulness of the service to others, including degradation of services and denial of service attacks.
- i. You have not conducted and attempted to conduct non-technical attacks such as social engineering, phishing, spamming or physical attacks against our employees, users, or infrastructure.
- j. Your testing activities must not negatively impact the Company or the Company's' online environment availability or performance. You may only exploit, investigate, or target vulnerabilities against your own accounts. Testing must not violate any law or disrupt or compromise any data or access data that is not yours; intentional access of customer data other than your own is expressly prohibited.
- k. You have not tested, and will not test, the physical security of any property or, building of the Company.
- l. You have not breached, and will not breach, any applicable laws and regulations in connection with your report and your interaction with Mauritius Telecom's product or service that led to your report.
- m. You are the original finder of the vulnerability. If someone else found it and told you about it, you must get their permission before reporting it to us.
- n. MT and its partners or subsidiaries can share the information you provide in your report with others as needed.
- o. You must not to access or attempt to access any person's personal data during your testing (this includes, but is not limited to, the Company's personnel and customers and/or any other data that could be considered personal data). If you gain access to any personal data while testing, stop and alert us immediately. You agree not to store, transfer, transmit, copy, create derivative works from, or disclose any personal data and/or the Company's data (save to the extent required for you to submit your report to the Company).
- p. The Company does not guarantee that you will receive any response from us related to your report. The Company will only contact you regarding your report if the Company deems it necessary.
- q. You are making your report without any expectation or requirement of reward or other benefit, financial or otherwise, for making such report, and without any expectation or requirement that the vulnerabilities and/or errors reported are corrected by the Company.

9. REPRESENTATION OF WARRANTIES

By submitting a vulnerability report to the Company, you represent and warrant that:

- a. You are a natural person, and not a robot, automated system, or artificial intelligence.
- b. You are submitting the report in your individual capacity, or on behalf of a legal entity for which you have the authority to bind to these terms and conditions.
- c. You acknowledge that MT may require you to provide additional information to verify your identity and the authenticity of your submission. Failure to provide such information upon request may result in the rejection of your submission and disqualification from the Vulnerability Disclosure Program.
- d. You understand that the Company reserves the right to reject any submission that it believes, in its sole discretion, to be made by a robot, automated system, or artificial intelligence, or otherwise fails to comply with these terms and conditions.

MT SHALL HAVE NO OBLIGATION TO REVIEW, ACKNOWLEDGE, OR RESPOND TO ANY SUBMISSION THAT IT DETERMINES, IN ITS SOLE DISCRETION, TO BE MADE BY A NON-HUMAN RESEARCHER OR THAT OTHERWISE FAILS TO COMPLY WITH THESE TERMS AND CONDITIONS.

10. LEGAL CONSIDERATIONS

This Policy follows best practices in the security research community. However, it does not give you permission to act contrary to the law or which may cause the Company to be in breach of any of its legal obligations, including but not limited to:

- The Cybersecurity and Cybercrime Act 2021
- The Data Protection Act 2017

If you comply with the terms and conditions outlined in this Policy and act in good faith, the Company shall not initiate legal proceedings or seek criminal prosecution against security researchers who report any security vulnerability on our services or systems, where the researcher has acted in good faith and in accordance with this Policy.

11. CONFIDENTIALITY

In addition to the above, you agree to fully comply with the following confidentiality obligations:

"Confidential Information" refers to (i) all information obtained from the Company during your security testing or through any other means related to your participation in our Vulnerability Disclosure Program, and (ii) all submissions made by you to MT. Confidential Information does not include information that (a) becomes publicly available through no fault of your own and without breaching these obligations, or (b) is independently developed without using or referring to MT's Confidential Information.

You agree to (i) maintain the strict confidentiality of MT's Confidential Information, (ii) protect such Confidential Information from any unauthorized use, access, or disclosure, (iii) not disclose MT's Confidential Information to any third party, including the public, without MT's prior written consent, (iv) use MT's Confidential Information solely for the purpose of participating in MT's Vulnerability Disclosure Program and not for any other purpose, and (v) promptly notify MT's Security Team (through the designated communication channels) upon discovery of any actual or potential loss, unauthorized access, or disclosure of MT's Confidential Information.

ANY BREACH OF THESE CONFIDENTIALITY OBLIGATIONS SHALL RESULT IN AUTOMATIC DISQUALIFICATION FROM THE VULNERABILITY DISCLOSURE PROGRAM, AND MT RESERVES THE RIGHT TO PURSUE ALL AVAILABLE LEGAL REMEDIES, INCLUDING, BUT NOT LIMITED TO, SEEKING INJUNCTIVE RELIEF AND MONETARY DAMAGES, TO THE FULLEST EXTENT PERMITTED BY LAW.

**** END OF DOCUMENT ****