VULNERABILITY REPORTING POLICY

ENFINITE SOLUTIONS LIMITED

P.O Box 21405 – 00100,
Nairobi, Kenya.
www.enfinitesolutions.com
info@enfinitesolutions.com

VERSION 1.0.0

VERSION HISTORY				
VERSION	**APPROVED BY**	**REVISION DATE**	**DESCRIPTION OF CHANGE**	**AUTHOR**

PREPARED BY	Judy Wambui	**TITLE**	VP OF PRODUCTS	**DATE**	15/01/2022
APPROVED BY	George N. Njoroge	**TITLE**	CEO	**DATE**	01/02/2022

At Enfinite Solutions Limited, trust is our #1 value and we take the protection of our customers' data very seriously. We are committed to ensuring the security of our applications by protecting our customers' personal and/or corporate data.

This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

The Enfinite security team acknowledges the valuable role that independent security researchers play in Internet security. As a result, we encourage responsible reporting of any vulnerabilities that may be found in our site, applications or systems. Enfinite is committed to working with security researchers to verify and address any potential vulnerabilities that are reported to us.

As a policy, Enfinite does not offer compensation for reported issues.

Authorization:
If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized. We will work with you to understand and resolve the issue quickly, and Enfinite 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 in accordance with this policy, we will make this authorization known.

Guidelines:
Under this policy, "research" means activities in which you:

1. Notify us as soon as possible after you discover a real or potential security issue.
2. Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
3. 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.
4. Do not disclose any unresolved vulnerability to the public.
5. 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, or proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

Testing for security vulnerabilities:
Whenever a Trial or Beta Edition is available, please conduct all vulnerability testing against such instances. Always use test or demo accounts when testing our online services.

Reporting a potential security vulnerability:
In order to help us triage and prioritize submissions, we recommend that your reports:

1. Describe the location the vulnerability was discovered and the potential impact of exploitation.
2. Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
3. Be in English, if possible.

Privately share details of the suspected vulnerability with Enfinite by sending an email to info@enfinitesolutions.com. The details of the suspected vulnerability will help the Enfinite security team validate and reproduce the issue.

Enfinite does not permit the following types of security research:
While we encourage you to discover and report to us any vulnerabilities you find in a responsible manner, the following conduct is expressly prohibited:

1. Performing actions that may negatively affect WakiliCMS or its users (e.g. Spam, Brute Force, Denial of Service)
2. Accessing, or attempting to access, data or information that does not belong to you
3. Destroying or corrupting, or attempting to destroy or corrupt, data or information that does not belong to you
4. Conducting any kind of physical or electronic attack on Enfinite personnel, property, or data centers
5. Social engineering any Enfinite service desk, employee, or contractor
6. Conduct vulnerability testing of participating services using anything other than test accounts (e.g. Beta or Trial Edition instances)
7. Violating any laws or breaching any agreements in order to discover vulnerabilities

The Enfinite security team commitment:

We ask that you do not share or publicize an unresolved vulnerability with/to third parties. If you responsibly submit a vulnerability report, the Enfinite security team and associated development organizations and personnel will use reasonable efforts to:

1. Respond in a timely manner, acknowledging receipt of your vulnerability report
2. Provide an estimated time frame for addressing the vulnerability report
3. Notify you when the vulnerability has been fixed

We are happy to thank every individual researcher who submits a vulnerability report helping us improve our overall security posture at Enfinite.