HSRC GROUP™ Responsible Disclosure Policy

At HSRC GROUP™, the security of systems is a top priority. We have a material interest in the ability to maintain adequate security of our systems and IT infrastructure for ourselves and our customers.

Through this Responsible Disclosure Policy, we allow for the safe, secure and responsible disclosure of weaknesses in our information technology infrastructure which can be exploited to perform unauthorized actions within a system (vulnerabilities). The purpose of this policy is to enable the vulnerability to be reported responsibly and to be remediated or patched in order to retain the integrity, continuity and security of our services.

If you are a security researcher and you encounter a vulnerability, we would like to cooperate with you to fix the vulnerability before this can be misused.

Report

Please send the report to **HSRC GROUP™** or **Email: export1@hsregionalcaribe.co Tel: +57 323 7967920**

Do's:

- Report the vulnerability as quickly as reasonably possible to minimize the risk of others finding and taking advantage of it
- Report it in a manner that safeguards the confidentiality of the report so others cannot gain access to the information
- Provide sufficient information to reproduce the problem so it can be resolved. To the extent possible, please include: type of vulnerability/issue; service, product or URL affected; special configuration/requirements to reproduce the issue; information necessary to reproduce the issue; impact of the vulnerability together with an explanation of how an attacker could find it and exploit it.

Don'ts:

- Reveal the vulnerability or problem to others until it is resolved.
- Build your own backdoor in an information system with the intention of then using it to demonstrate the vulnerability, because doing so can cause additional damage and create unnecessary security risks.
- Utilize a vulnerability further than necessary to establish its existence.
- Copy, modify or delete data on the system. An alternative for doing so is making a directory listing of the system.
- Make changes to the system.
- Repeatedly gain access to the system or share access with others.
- Use brute force attacks, attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties to gain access to the system.

Next Steps:

We will respond to your report within 5 business days with our evaluation of the report and an expected resolution date.

If you have followed the instructions above, we will not take any legal action against you concerning the report. We will not pass on your personal details to third parties without your permission unless it is necessary to comply with a legal obligation. Reporting under a pseudonym or anonymous is possible.

We will keep you informed of the progress towards resolving the problem.

In the public information concerning the reported problem, we will give your name as the discoverer of the problem (unless you desire otherwise).

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved.

No Rewards

Currently, no monetary compensation is offered or provided in connection with reporting vulnerabilities. This policy is not intended to encourage hacking attempts in connection with **HSRC GROUP™** information technology infrastructure, but to provide a responsible manner through which security vulnerability reports can be communicated and remediated.

Questions

If at any time you have questions about the above procedure, feel free to reach out to **HSRC GROUP™** or **Email: export1@hsregionalcaribe.co Tel: +57 323 7967920**

This policy is based on guidance issued by the National Cyber Security Center of the Colombian Ministry of Justice and Security and the guidance issued in by Colombian Public Justice Department. **END OF DOCUMENT.**