Vulnerability Reporting Policy

CSC is committed to maintaining the highest levels of client service, confidence, and security. CSC encourages responsible reporting of vulnerabilities that are found in systems or applications. CSC will work with security researchers to verify and address any potential vulnerabilities that are reported to us.

Reporting a potential security vulnerability:

- Privately and securely, share details of the suspected vulnerability, including preferred contact information, by sending an email to **informationsecurity@cscglobal.com** with the subject "Potential Security Vulnerability."
    - CSC encourages the use of encrypted email.
- Please include an appropriate level of detail including the steps needed to reproduce the issue, applicable screenshots, time and method of discovery, and other details that could facilitate CSC's identification of the problem.

CSC prohibits you from:

- Conducting vulnerability testing or penetration testing without CSC's prior written approval.
- Publicly sharing the suspected vulnerability, or related details, until CSC has released a fix.
- Compromising the availability, security, or privacy of CSC systems and services.
- Accessing, or attempting to access, modify, download, or copying data that does not belong to you.

CSC security commitment:

Upon receipt of the suspected vulnerability, and subject to the above requests, CSC will:

- Respond in a timely manner and acknowledge receipt of the suspected vulnerability
- Provide an estimated timeframe for addressing the vulnerability, based on severity and impact, once a reasonable investigation has taken place
- Provide notification to you when the vulnerability has been remediated

CSC pledges not to initiate legal action against researchers as long as they adhere to this policy. Thanks for submitting a vulnerability report and collaborating with us to improve security!