Vulnerability Disclosure Policy (CVD)

This policy outlines Promote International AB's commitment to security and provides guidelines for security researchers to conduct discovery activities and submit vulnerability reports to us in a responsible manner.

1. Introduction

At Promote International AB, we value the work of the security community. If you believe you have found a security vulnerability in our platform or services, we encourage you to let us know as soon as possible. We will investigate all legitimate reports and do our best to quickly fix the issue.

2. Guidelines

We ask that you follow these guidelines when participating in our vulnerability disclosure program:

- **Do not** perform any activity that may disrupt our services (e.g., DoS/DDoS).
- **Do not** access, modify, or delete data that does not belong to you.
- **Do not** use social engineering, phishing, or physical security attacks against our employees or offices.
- **Keep it confidential:** Provide us with a reasonable amount of time to fix the issue before sharing any information publicly.

3. Scope

The following systems are in scope for this policy:

- www.promoteint.com
- *.promotelogin.com (Our primary SaaS platform)
- Our public-facing APIs

Any third-party services (e.g., AWS, Akamai, Google Workspace) are OUT OF SCOPE. Please report any issues regarding those services directly to the respective provider.

4. How to Report

Please submit your findings to:

security@promoteint.com

Include a detailed description of the vulnerability, the steps to reproduce it, and any potential impact.

5. Our Commitment

If you follow these guidelines when reporting an issue to us:

- **Legal Action:** We will not pursue or support any legal action related to your research.
- **Responsiveness:** We will acknowledge receipt of your report within 3 business days.
- **Recognition:** If the vulnerability is valid and unique, we will offer to recognize your contribution (e.g., a 'Thank You' on our site).

6. Rewards

Currently, Promote International AB does not operate a paid Bug Bounty program. However, we value every report and are committed to clear and open communication with researchers who help us stay secure.