Cyber Vulnerability Disclosure Policy

Last modified: June 30, 2022

INTRODUCTION

Pollard Banknote Limited and its subsidiaries ("Pollard" or the "Company") are leading lottery partners to more than 60 lotteries worldwide, providing high quality instant ticket products, licensed games, retail merchandising solutions, and a full suite of digital offerings, ranging from game apps to comprehensive player engagement and iLottery solutions, including strategic marketing and management services.

Together, we are committed to the identification and remediation of cyber vulnerabilities that affect our information technology environments, including our systems and networks, and our digital products and services. The purpose of this policy is to document a process for the reporting of cyber vulnerabilities.

We encourage you to contact us at vulnerabilityreporting@pbl.ca to report potential cyber vulnerabilities in our systems.

LEGAL POSTURE

Pollard will openly accept cyber vulnerability reports and agrees not to pursue legal action against individuals who:

- Notify us as soon as possible after discovering a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a cyber 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.
- Provide us a reasonable amount of time to resolve the issue before disclosing it publicly.
- 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.

HOW TO SUBMIT A VULNERABILITY REPORT

We accept cyber vulnerability reports at vulnerabilityreports@pbl.ca.

If a cyber vulnerability is discovered, you must provide a detailed summary of the cyber vulnerability, including the following:

- Description of the vulnerability and its potential impact;
- Product, version, and configuration of any software or hardware potentially impacted;
- Step-by-step instructions to reproduce the issue;

- Proof-of-concept; and
- Suggested mitigation or remediation actions, as appropriate.

By submitting a cyber vulnerability report, we will presume that you have read, understand and agree to the guidelines described in this policy, and consent to having subsequent communications with us stored on Pollard's information systems. Personal data submitted in a cyber vulnerability report will not be retained by Pollard, other than contact information that will only be retained in order to coordinate with you.

By submitting a cyber vulnerability report, you acknowledge that you have no expectation of payment and that you expressly waive any future pay claims against Pollard or its subsidiaries related to your submission.

WHAT YOU CAN EXPECT FROM POLLARD

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- Within seven (7) days, we will acknowledge that your report has been received.
- To the best of our ability, we will confirm the existence of the cyber vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.

If we are unable to resolve communication issues or other problems, Pollard may bring in a neutral third party to assist in determining how best to handle the vulnerability.

ACTIVITIES OUTSIDE THE SCOPE OF THIS POLICY

Pollard does not authorize, permit, or otherwise allow (expressly or impliedly) any person, including any individual, group of individuals, consortium, partnership, or any other business or legal entity, to engage in any security research or vulnerability or threat disclosure activity on or affecting Pollard systems that is inconsistent with this policy or the law. If you engage in any activities that are inconsistent with this policy or other applicable law, you may be subject to criminal and/or civil liabilities.

MODIFICATION OR TERMINATION OF THIS POLICY

Pollard may modify the terms of this policy or terminate the policy at any time.

QUESTIONS

Questions regarding this policy may be sent to vulnerabilityreporting@pbl.ca. We also invite you to contact us with suggestions for improving this policy.