1 Scope

This Vulnerability disclosure policy applies only to vulnerabilities within Allwyn UK products and services.

Not all products and services under The National Lottery brand are operated by Allwyn UK. We are the operator of The National Lottery in the UK and, for the avoidance of doubt, this vulnerability disclosure policy only applies to the products and services operated by Allwyn UK.

We recommend reading this vulnerability disclosure policy fully before you report a vulnerability and always act in compliance with it.

Although Allwyn UK does not offer monetary rewards for disclosure, we really value and appreciate those who take the time and effort to report vulnerabilities to us.

2 Reporting a Vulnerability

If you've identified a security vulnerability impacting Allwyn UK, please feel free to let us know by email security@national-lottery.co.uk as soon as you can, but please note:

- If you need to share sensitive information, please do not include it in your initial message - we will provide a secure communication method in our reply to you.
- This email address should only be used to report security vulnerabilities. We won't be able to respond to emails on other matters sent to this email address.

3 What to expect

After submitting your vulnerability report to us, you will receive an email acknowledging receipt of your report, usually within 5 working days. We will aim to keep you informed of our progress.

The Security team will then triage the reported vulnerability, and respond as soon as possible to ask for further information, if required.

When the reported vulnerability is resolved, or any remediation work is to be scheduled, the Security team will notify you, and may invite you to confirm the solution covers the vulnerability adequately.

4 Vulnerability reporting guidelines

You must not:

- Break any applicable law or regulations.
- Access unnecessary, excessive or significant amounts of data.
- Modify data in Allwyn UK systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt or report any form of denial of service, e.g meaning that simply overwhelming a service with a high volume of requests.
- Disrupt services or systems.
- Submit reports detailing non-exploitable vulnerabilities, or reports indicating that the services do not fully align with "best practice", for example missing security headers.

- Submit reports detailing TLS configuration weaknesses, for example “weak” cipher suite support.
- Communicate any vulnerabilities or associated details other than by means described in the published security.txt.
- Social engineer, ‘phish’ or physically attack the Allwyn UK staff or infrastructure.
- Demand financial compensation in order to disclose any vulnerabilities.

You must:

- Always comply with data protection laws (Data Protection Act 2018 and UK GDPR) and must not violate the privacy of the organisation’s users, staff, contractors, services or systems. You must not, for example, share, redistribute or fail to properly secure data retrieved from the systems or services.
- Securely delete all data retrieved during your research as soon as it is no longer required or within 1 month of the vulnerability being resolved, whichever occurs first (or as otherwise required by data protection law).

5 Legalities

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause Allwyn UK to be in breach of any of its legal obligations.