Compania Națională "Loteria Română" S.A.



# POLITICĂ DE DIVULGARE RESPONSABILĂ A VULNERABILITĂȚILOR DE SECURITATE

## 1. Dispoziții generale

Loteria Română S.A. (denumită în continuare „Loteria Română"), cu sediul în București, Str. Poenaru Bordea, nr. 20, în calitate de operator național în domeniul jocurilor de noroc, recunoaște importanța securității cibernetice și încurajează raportarea responsabilă a eventualelor vulnerabilități identificate în infrastructura sa IT.

Prezenta politică stabilește cadrul legal în care persoanele interesate (denumite în continuare „Raportori") pot notifica, în mod voluntar și responsabil, vulnerabilități de securitate identificate în sistemele digitale gestionate de Loteria Română.

## 2. Domeniul de aplicare

Politica se aplică tuturor serviciilor digitale și sistemelor informatice deținute, operate sau controlate de Loteria Română, inclusiv, dar fără a se limita la: site-ul web oficial, platforme online de jocuri, aplicații mobile și infrastructura asociată.

## 3. Activități permise și nepermise

### 3.1 Activități permise:

În scopul identificării și raportării de vulnerabilități de securitate, Loteria Română permite, în mod limitat, următoarele activități tehnice:

- Testare neintruzivă a aplicațiilor web pentru identificarea vulnerabilităților de tip XSS, CSRF, SQL injection, etc.;
- Scanări pasive (fără impact operațional) ale interfețelor publice;
- Observarea comportamentului aplicațiilor fără interacțiune cu date reale sau conturi ale utilizatorilor.

### 3.2 Activități interzise:

Sunt strict interzise următoarele activități:

- Exfiltrarea, modificarea sau ștergerea datelor;
- Accesarea neautorizată a conturilor sau datelor personale;
- Atacuri de tip Denial-of-Service (DoS/DDoS);
- Inginerie socială, phishing sau manipularea angajaților ori a utilizatorilor;
- Introducerea de malware sau alte coduri malițioase;
- Exploatarea efectivă a vulnerabilității înainte de remedierea sa de către Loteria Română.

## 4. Obligațiile Raportorului

Raportorul:

- se obligă să acționeze cu bună-credință și cu respectarea principiilor eticii în securitate cibernetică;
- va furniza Loteriei Române detalii tehnice clare și complete despre vulnerabilitatea identificată (inclusiv, dacă este cazul, pașii de reproducere și capturi de ecran);
- nu va divulga public informațiile privind vulnerabilitatea înainte de remedierea sa sau fără acordul expres, în scris, al Loteriei Române;
- se obligă să nu utilizeze în niciun fel vulnerabilitatea descoperită în scopuri personale sau comerciale.

**5. Măsuri și garanții**

Atât timp cât Raportorul respectă prezenta politică, Loteria Română:

- nu va iniția acțiuni legale sau administrative împotriva acestuia;
- va analiza raportul într-un termen rezonabil, de regulă nu mai mult de 30 de zile de la primirea notificării;
- poate, la discreția sa, recunoaște public contribuția Raportorului și/sau oferi o formă de recompensă onorifică sau simbolică (fără caracter contractual sau obligatoriu).

**6. Modalitatea de raportare**

Orice raport de vulnerabilitate se va transmite prin e-mail, la adresa oficială: security@loto.ro

Raportul trebuie să conțină: descrierea detaliată a vulnerabilității, pașii de reproducere, adresele URL implicate (dacă este cazul), și datele de contact ale Raportorului (opțional, pentru comunicare ulterioară).

**7. Limitări și exonerări**

Prezenta politică:

- nu constituie un angajament juridic din partea Loteriei Române de a recompensa sau colabora cu Raportorul;
- nu reprezintă o autorizație de penetrare extinsă a sistemelor informatice;
- poate fi modificată oricând, fără notificare prealabilă.

**8. Jurisdicție și lege aplicabilă**

Această politică este guvernată de legislația română în vigoare. Orice dispută referitoare la aplicarea sau interpretarea acestei politici va fi soluționată de instanțele competente din România.

**9. Informarea publicului în cazul unui incident de securitate**

În cazul în care o vulnerabilitate raportată sau un incident de securitate produce un impact semnificativ asupra confidențialității, integrității sau disponibilității sistemelor sau datelor gestionate de Loteria Română, se vor lua următoarele măsuri:

**9.1 Notificarea autorităților competente:**

Loteria Română va notifica autoritățile competente conform prevederilor legale aplicabile, inclusiv:

- Autoritatea Națională pentru Securitatea Cibernetică (DNSC) – conform legislației NIS/NIS2;
- Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) – dacă sunt afectate date cu caracter personal, conform Regulamentului (UE) 2016/679 (GDPR).

**9.2 Informarea persoanelor afectate:**

În cazul în care un incident afectează în mod direct drepturile și libertățile persoanelor fizice, Loteria Română va informa persoanele vizate în cel mai scurt timp posibil, într-o manieră clară și accesibilă.

Informațiile comunicate vor include:

- natura vulnerabilității sau a incidentului;
- potențialele riscuri și impact estimat;
- măsurile luate pentru remediere și protecție;
- recomandări pentru persoanele afectate (ex: schimbarea parolei, monitorizarea activității contului etc.).

**9.3 Transparență publică:**

În cazuri semnificative, Loteria Română poate publica, la momentul oportun și în urma unei evaluări interne, un comunicat oficial pe site-ul propriu (www.loto.ro) și/sau prin canale oficiale (ex: presă, rețele sociale), care va include detalii relevante despre natura și consecințele incidentului, fără a compromite securitatea operațională sau ancheta în desfășurare.