

## Security Information Document

### Golden Draw Weekly

Operated by Tattersall's Sweeps Pty Ltd

ABN: 99 081 925 662

Level 1, 411 Collins Street, Melbourne, Victoria 3000, Australia

---

### Effective Date: 29 April 2025

Tattersall's Sweeps Pty Ltd, operator of Golden Draw Weekly, is committed to maintaining the highest standards of security to protect our users, their data, and the integrity of our online lottery platform. This Security Information Document outlines the measures implemented to ensure a secure and trustworthy experience for all participants in accordance with Australian legal and regulatory requirements.

---

## Website Encryption and Secure Socket Layer (SSL) Usage

Golden Draw Weekly employs industry-standard encryption protocols to safeguard all data transmitted between users and our platform. Our website utilises Transport Layer Security (TLS) with a minimum of 256-bit encryption, ensuring that all sensitive information, including personal details and financial transactions, is securely encrypted.

- **SSL Certificates:** We maintain valid and up-to-date SSL certificates issued by a trusted Certificate Authority. These certificates are regularly renewed and configured to enforce secure connections.
- **HTTPS Enforcement:** All pages on the Golden Draw Weekly website are accessible exclusively via HTTPS, preventing unauthorised interception of data.
- **Secure Payment Gateways:** All payment processing is conducted through PCI DSS-compliant third-party providers, ensuring secure handling of credit card and other financial information.

Users are encouraged to verify the presence of the padlock icon and "https://" in their browser's address bar when accessing our platform.

---

## Account Security and User Responsibilities

Golden Draw Weekly prioritises account security through robust authentication mechanisms and user-driven safeguards.

- **Password Requirements:** Users must create strong, unique passwords with a minimum length of 12 characters, incorporating a mix of uppercase, lowercase, numbers, and special characters.
- **Two-Factor Authentication (2FA):** We offer optional 2FA via SMS or authenticator apps to add an additional layer of security to user accounts.
- **Session Management:** User sessions are automatically terminated after a period of inactivity, and suspicious login attempts trigger account lockouts and user notifications.

### User Responsibilities:

- Users must maintain the confidentiality of their login credentials and refrain from sharing account details with third parties.
- Users are required to promptly report any suspected unauthorised access or compromised accounts to our support team at [support@goldendrawweekly.com.au](mailto:support@goldendrawweekly.com.au).
- Users should ensure their devices are protected with up-to-date antivirus software and avoid accessing their accounts on public or unsecured networks.

Tattersall's Sweeps Pty Ltd is not liable for losses resulting from a user's failure to adhere to these security practices.

---

## Data Storage and Internal Access Controls

Golden Draw Weekly adheres to strict data storage and access protocols to protect user information in compliance with the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs).

- **Data Storage:** All user data is stored on secure servers located within Australia, managed by ISO 27001-certified data centres. Data is encrypted at rest using AES-256 encryption standards.
- **Access Controls:** Access to user data is restricted to authorised personnel on a need-to-know basis. All staff undergo regular security training and are bound by confidentiality agreements.
- **Data Minimisation:** We collect and retain only the data necessary to provide our services, including name, contact details, date of birth, and payment information, as outlined in our Privacy Policy.
- **Data Retention:** Personal data is retained only for as long as required to fulfil legal, regulatory, or operational purposes, after which it is securely deleted or anonymised.

Regular reviews of our data storage practices ensure ongoing compliance with Australian privacy laws.

---

## Fraud Prevention and Anti-Money Laundering Compliance (AUSTRAC)

Golden Draw Weekly is registered with the Australian Transaction Reports and Analysis Centre (AUSTRAC) and complies with the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

- **Identity Verification:** All users are required to verify their identity prior to participating in lottery draws or withdrawing funds. This includes submitting government-issued identification and proof of address, which are validated against third-party databases.

- **Transaction Monitoring:** Our platform employs automated systems to monitor transactions for suspicious activity, including unusual patterns or high-value transfers. Suspected cases are escalated for manual review and reported to AUSTRAC where required.
- **Fraud Detection:** We utilise machine learning algorithms and behavioural analytics to detect and prevent fraudulent activities, such as account takeovers or payment fraud.
- **Know Your Customer (KYC):** Comprehensive KYC procedures are in place to ensure the legitimacy of all participants, protecting both users and the platform from financial crime.

Users found to be engaging in fraudulent or illegal activities will have their accounts suspended and may be reported to relevant authorities.

---

## Security Audits and Penetration Testing

To maintain the integrity of our platform, Golden Draw Weekly conducts regular security audits and penetration testing.

- **Independent Audits:** Our systems are audited annually by third-party cybersecurity firms certified under ISO 27001 and adhering to OWASP standards. These audits assess vulnerabilities across our website, databases, and internal networks.
- **Penetration Testing:** Quarterly penetration tests are performed to identify and address potential weaknesses in our infrastructure. Both automated and manual testing methodologies are employed to simulate real-world cyber threats.
- **Continuous Monitoring:** We maintain 24/7 monitoring of our systems for unauthorised access attempts, malware, or other security threats, with alerts routed to our dedicated cybersecurity team.

Findings from audits and tests are promptly addressed, and updates are applied to mitigate identified risks.

---

## Incident Response and Notifiable Data Breaches Scheme

Golden Draw Weekly has a comprehensive incident response plan to address potential security incidents, in line with the *Notifiable Data Breaches Scheme* under the *Privacy Act 1988* (Cth).

- **Incident Response Team:** Our dedicated team is trained to respond swiftly to security incidents, with clear protocols for containment, investigation, and remediation.
- **User Notification:** In the event of a data breach likely to result in serious harm, affected users will be notified within 30 days, as required by law. Notifications will

include details of the breach, its impact, and steps users can take to protect themselves.

- **Regulatory Reporting:** All eligible data breaches are reported to the Office of the Australian Information Commissioner (OAIC) and AUSTRAC, where applicable.
- **Post-Incident Review:** Following any incident, we conduct a thorough review to identify root causes and implement measures to prevent recurrence.

Users can contact our Data Protection Officer at [dpo@goldendrawweekly.com.au](mailto:dpo@goldendrawweekly.com.au) for inquiries or to report suspected security incidents.

---

**Last Updated: 29 April 2025**

Tattersall's Sweeps Pty Ltd reserves the right to update this Security Information Document as necessary to reflect changes in our practices, technology, or legal requirements. Users will be notified of material changes via email or through a prominent notice on our website.

---

**Footer**

© 2025 Tattersall's Sweeps Pty Ltd. All Rights Reserved.