Privacy and Security Summary for Golfers and Clubs/Organisations

This document outlines how DotGolf, the Platform Provider of the new Golf Australia CONNECT Platform, protects the personal information of Australian golfers through robust privacy and security controls.

Built on Proven Technology.

DotGolf's core technology for Golf Australia CONNECT is already used today by 2 million golfers and over 5,000 clubs in various worldwide territories including New Zealand, England, Wales, Ireland and Scotland.

Committed to Golfer Privacy.

- Built with 'privacy by design' (DotGolf has worked with Golf Australia to embed privacy considerations into Golf Australia CONNECT at each design and development stage).
- Golfers can control and limit the visibility of their personal information to other golfers.
- DotGolf has an express contractual obligation to Golf Australia to comply with all relevant privacy laws, including the Australian Privacy Act, its Australian Privacy Principles and Notifiable Data Breaches scheme.
- DotGolf maintains appropriate cyber insurance to support Golf Australia CONNECT.
- View DotGolf's Privacy Policy at **https://www.dotgolf.co.nz**.

Hosted on Proven Infrastructure.

- Hosted in Amazon Web Services' ISO 27001-certified Australian data centres featuring 24/7 physical security, including CCTV and biometric access control.
- Amazon Web Services is a leading cloud infrastructure provider used by organizations including the Commonwealth Bank of Australia, NASA, and Qantas.
- Security and Compliance responsibilities are managed between DotGolf and Amazon Web Services under the 'AWS Shared Responsibility Model'.

Notable Security Controls.

- Enforced HTTPS (TLS 1.2+) encryption for all Internet traffic.
- Enforced password strength policies for all golfers and club administrators.
- Enforced multi-factor authentication (**MFA**) for Golf Australia users and helpdesk. Pending consultation between Golf Australia and clubs/organisations, DotGolf will also progressively enable MFA for club administrators.
- Enforced network segmentation and web application firewall (**WAF**) to protect all Internet-accessible services from unauthorised access and cyber attacks.
- Comprehensive logging and monitoring to detect and respond to suspicious activities.
- Security patches, updates and mitigations are regularly assessed and applied.
- Regular penetration testing and security audits performed by security experts.
- Comprehensive incident response and disaster recovery plans for service continuity.
- Integrated with leading payment processors, including Stripe and Windcave. DotGolf's PCI-DSS compliance documents are available to clubs/organisations upon request.

Questions about DotGolf's Privacy and Security Controls?

Please contact DotGolf – hello@dotgolf.co.nz.