INFORMATION SECURITY POLICY STATEMENT

Discount Domain Name Services Pty Ltd (DDNS) commits to its customers that it will conduct certain objectives in relation to the services provided. These commitments are documented and reviewed by management to ensure that the operations, reporting, and compliance objectives are aligned with DDNS' mission to maintain Information Security. DDNS is committed to continual improvement of our Information Security Management System. This is recorded through various polices, procedures, security documents and a terms of service that are available to customers via DDNS' public-facing website.

Specific security, availability, and confidentiality commitments include the following:

- Maintain technical and organizational measures, internal controls, and data security routines to protect customer data
- Protection of data at rest and in transit
- Protection of information systems from unauthorised access, use, modification, disclosure, destruction, threats, or hazards
- Continuous communication of the DDNS' service availability
- Ability to recover and restore customer data in the event of a business disruption or disaster
- Maintain customer data as confidential and not disclose information to any unauthorised party
- Customer data is retained for a period of five years, following the termination of the customer agreement and then removed from DDNS' systems

DDNS has also established system requirements that support the achievement of the Information Security Policy relevant to the security, availability, and confidentiality trust services categories and relevant laws and regulations. These requirements are communicated internally via the information security policies and procedures and regular security awareness training documentation, and externally via DDNS' public-facing website.

These requirements include, but are not limited to, defined processes around the following:

- Employees undergo background checks prior to employment and renewed at least every 3 years
- Employees undergo security awareness training upon hire, and annually thereafter
- Roles and responsibilities for DDNS employees who have access to confidential data and the responsibility for protecting the information and information systems
- Access control policies for employees with access to DDNS' production environment and source code such that access levels are approved prior to credentials being issued, reviewed at predefined intervals, and based on legitimate business need based on the principle of least privilege
- Software development lifecycle (SDLC) policies for any changes to the production environment to ensure that key processes and security checks are consistently performed from change initiation through release
- Risk assessment practices to assist in identifying and managing potential internal or external risks that could negatively affect DDNS' critical business processes and our ability to provide reliable services to our customers
- Incident management processes to address data breaches and security events related to DDNS' products and services in an efficient and timely manner
- Disaster recovery and business continuity plans to prepare DDNS in the event of extended service outages caused by factors beyond our control and to restore services to the widest extent possible in a minimal timeframe

Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed; how the system is operated; how the internal business systems and networks are managed; and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of DDNS' systems.

Rod Keys
Chief Executive Officer

Certified System™
ISO27001

Version 1.2
Last Reviewed: January 2026