Data Classification Policy

dnswatchdog.io

1. Purpose

This policy defines the classification levels DNS Watchdog applies to data it processes, and the minimum security controls required for each level. It supports our Data Protection Policy by linking the categories of data described there to concrete handling, access, and protection requirements.

2. Scope

This policy applies to all data processed by DNS Watchdog Ltd., regardless of format or location. It covers data held in production systems, development and staging environments, third-party services used as sub-processors, employee devices, and any physical records. It applies to all employees, contractors, and third parties acting on behalf of DNS Watchdog.

3. Roles and Responsibilities

- **Data Protection Officer (DPO)** owns this policy, reviews it annually, and resolves classification disputes. The DPO can be contacted at dpo@dnswatchdog.io.
- **Data owners** (typically the engineering or operations lead responsible for a system) are accountable for classifying the data their system processes and ensuring the relevant controls are in place.
- **All personnel** are responsible for applying the controls described in this policy to data they handle and for reporting suspected misclassification or mishandling to the DPO.

4. Classification Levels

DNS Watchdog uses four classification levels. Where a single data set contains items at multiple levels, the highest applicable level applies to the whole set.

4.1 Public

Information that has been approved for unrestricted distribution and whose disclosure poses no risk to DNS Watchdog, our customers, or third parties.

Examples: Published marketing content, blog posts, published legal policies, public documentation, sub-processor lists, public records of the company.

4.2 Internal

Non-sensitive information intended for use within DNS Watchdog. Unauthorised disclosure is unlikely to cause material harm but is not appropriate.

Examples: Internal documentation and runbooks, non-sensitive operational metrics, team communications, internal architectural diagrams that do not include credentials or customer data.

4.3 Confidential

Information whose unauthorised disclosure, alteration, or destruction would cause harm to DNS Watchdog, our customers, or data subjects. Most personal data and customer data falls into this category.

Examples: Customer account data (names, email addresses, organisation details), DNS records and zone data, certificate metadata, port scan results, website screenshots and AI analysis output, IP intelligence data, audit trail entries, billing and subscription data, application logs, error reports.

4.4 Restricted

Information whose unauthorised disclosure or compromise would cause severe harm, including direct compromise of customer infrastructure, loss of platform integrity, or regulatory breach. Restricted data is the most tightly controlled category.

Examples: DNS provider API credentials, AWS account credentials and IAM access keys, encryption keys (KMS keys, application secrets), Sentry DSN, authentication tokens and session secrets, full payment card data (handled directly by Stripe; never received or stored by DNS Watchdog), database master credentials, cryptographic material.

5. Handling Controls

The table below sets out the minimum controls for each classification level. Higher levels inherit the controls of all lower levels.

Control	Public	Internal	Confidential	Restricted
Encryption at rest	Optional	Required	Required (AES-256 / AWS-managed KMS)	Required (AWS KMS SecureString or equivalent customer-managed encryption)
Encryption in transit	Required	Required	Required (TLS 1.2+)	Required (TLS 1.2+)
Access control	Open	Authenticated employees and contractors	Role-based, least privilege, tenant-scoped	Named individuals only, time-bound where possible, MFA enforced
Logging and audit	Not required	Standard application logs	Access and change logs retained per the Data Protection Policy	All access logged; logs reviewed for anomalies
Storage in third-party services	Permitted	Permitted with sub-processor agreement	Permitted only with sub-processor agreement and DPA in place	Permitted only in approved secret stores (AWS SSM Parameter Store SecureString, Stripe vaulting); never in source code, tickets, chat, email, or general-purpose document storage
Inclusion in logs and error reports	Permitted	Permitted	User identifiers permitted; request bodies and sensitive payloads excluded	Prohibited; filtered out of logs, error reports, and stack traces

Control	Public	Internal	Confidential	Restricted
Sharing outside DNS Watchdog	Permitted	Need-to-know basis under NDA	Only with the data subject, the data controller, or as required by law	Only as strictly necessary to deliver the Service or comply with a legal obligation
Disposal	No requirement	Standard deletion	Secure deletion; lifecycle policies and retention periods apply	Secure deletion plus key destruction where applicable; cryptographic erasure preferred

6. Application to Platform Components

The classification levels above map to the platform as follows.

System or store	Primary classification	Notes
Marketing site (https://dnswatchdog.io)	Public	Static content; no customer data
Application DynamoDB tables (records, zones, providers, audit)	Confidential	Tenant-isolated by `scope_id`; AWS-managed encryption at rest
Archive DynamoDB table	Confidential	Same controls as active tables; up to 3 years retention
Screenshot S3 bucket	Confidential	SSE-S3 (AES-256) with bucket key; CloudFront delivery over HTTPS
SSM Parameter Store (provider credentials, application secrets)	Restricted	SecureString with AWS KMS encryption; access restricted to specific service roles

System or store	Primary classification	Notes
CloudWatch Logs	Confidential	Structured logging excludes credentials, request bodies, and other Restricted content
Sentry error reports	Confidential	User identifiers may appear in error context; non-actionable events filtered out before submission
Stripe (billing)	Confidential (subscription data); Restricted (payment card data, held by Stripe)	DNS Watchdog does not receive or store payment card numbers
Clerk (identity)	Confidential	Authentication and identity data only

7. Roles, Access, and Provisioning

Access to Confidential and Restricted data is granted on a least-privilege, need-to-know basis. Access provisioning, review, and revocation are described in the platform's access management procedures, which are reviewed at least annually.

- New access requests for Restricted data require approval from the data owner and the DPO.
- Access to production Confidential and Restricted data is reviewed at least every six months.
- Access is revoked promptly when an individual leaves DNS Watchdog or changes role such that access is no longer required.

8. Incident Handling

Suspected unauthorised access, disclosure, or loss of Confidential or Restricted data must be reported immediately to security@dnswatchdog.io and handled in accordance with the Incident Response Policy.

9. Training

All personnel with access to Confidential or Restricted data complete data protection training as part of onboarding and at least annually thereafter. Training covers the classification levels, handling controls, and incident reporting procedures defined in this policy.

10. Review

This policy is reviewed annually by the DPO, or sooner if there are material changes to the platform, processing activities, or applicable legislation.

11. Contact

- **Data Protection Officer:** dpo@dnswatchdog.io
- **Security issues:** security@dnswatchdog.io
- **Postal address:** DNS Watchdog Ltd., Data Protection Officer, 167-169 Great Portland Street, 5th Floor, London W1W 5PF, United Kingdom