Incident Response Policy

dnswatchdog.io

1. Purpose

This policy describes how DNS Watchdog detects, classifies, contains, and recovers from security incidents and personal data breaches, and how we communicate with affected parties. It supports the breach notification commitments set out in the Data Protection Policy and the Data Processing Agreement.

2. Scope

This policy applies to any event that affects, or has the potential to affect, the confidentiality, integrity, or availability of:

- Personal data processed by DNS Watchdog as a controller or processor;
- Customer data, including DNS records, certificates, scan results, screenshots, and audit trails;
- Platform infrastructure, source code, or operational systems;
- Sub-processor systems used to deliver the Service.

It applies to all employees, contractors, and third parties acting on behalf of DNS Watchdog.

3. Definitions

- **Event:** Any observable occurrence in a system or network.
- **Security incident:** An event that compromises, or is reasonably suspected to compromise, the confidentiality, integrity, or availability of data or systems.
- **Personal data breach:** A security incident leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data, as defined in Art. 4(12) GDPR.
- **Reporter:** The person who first identifies and reports the incident.
- **Incident lead:** The individual responsible for coordinating the response to a specific incident.

4. Roles and Responsibilities

Role	Responsibilities
Data Protection Officer (DPO)	Overall accountability for this policy. Leads the incident response team. Decides on regulatory and data subject notifications.
Incident lead	Coordinates investigation, containment, and recovery for a specific incident. Maintains the incident timeline and decision log.
Engineering on-call	First responder for technical incidents. Performs initial triage and containment.
Legal contact	Advises on regulatory obligations, contractual notifications, and external communications.
Communications contact	Coordinates customer-facing messaging and any public statements.
All personnel	Required to report suspected incidents promptly to security@dnswatchdog.io.

The incident response team is convened by the DPO when an incident is classified at Severity 1 or 2 (see Section 6).

5. Reporting an Incident

Anyone who suspects a security incident or personal data breach must report it without delay.

- **Internal reports:** security@dnswatchdog.io and the engineering on-call channel.
- **Customer reports:** contact@dnswatchdog.io or security@dnswatchdog.io.
- **External security researchers:** security@dnswatchdog.io. We acknowledge reports promptly and follow the responsible disclosure expectations set out in the Acceptable Use Policy.

Reports should include, where known: a description of what was observed, the systems or data affected, the time the issue was first noticed, and how to reach the reporter for follow-up.

6. Severity Classification

Each incident is assigned a severity level on triage. The level may be revised as the investigation progresses.

Severity	Description	Examples
Sev 1 - Critical	Confirmed or highly likely compromise of personal data, customer data, or production credentials. Major service outage.	Confirmed unauthorised access to a production data store; compromise of provider credentials; full platform outage.
Sev 2 - High	Significant security event with material risk to data, customers, or platform integrity.	Targeted account compromise affecting one customer; loss of integrity in a non-critical service; sub-processor security incident with potential customer impact.
Sev 3 - Medium	Localised issue with limited impact, contained quickly.	Misconfiguration corrected before exploitation; phishing attempt without successful credential capture.
Sev 4 - Low	Anomaly or near miss; no demonstrable impact.	Failed brute-force attempts blocked by rate limiting; benign noisy alerts requiring review.

7. Response Process

The response process follows five phases. Phases may run in parallel where appropriate.

7.1 Identification and Triage

Within one (1) hour of a Sev 1 or Sev 2 report being received during business hours, or four (4) hours outside business hours, the engineering on-call performs initial triage and the incident lead is assigned. The incident is logged in the incident register with a unique identifier, initial severity, and a brief description.

7.2 Containment

The incident lead, working with engineering, takes immediate steps to limit further damage. Examples include rotating affected credentials, revoking sessions, disabling compromised accounts, isolating affected systems, applying emergency configuration changes, and communicating with sub-processors where their systems are involved. Evidence is preserved before destructive remediation steps where it is reasonable to do so.

7.3 Eradication and Recovery

Once contained, the incident lead coordinates removal of the underlying cause (for example, patching, removing malicious artefacts, restoring from clean backups) and verification that affected systems are operating normally. Recovery includes confirming integrity of customer data, monitoring for recurrence, and re-enabling any temporarily disabled functionality.

7.4 Notification

The DPO determines, in consultation with the legal contact, whether the incident triggers notification obligations.

- **Supervisory authority (GDPR Art. 33):** Where the incident is a personal data breach likely to result in a risk to the rights and freedoms of individuals, the DPO notifies the relevant supervisory authority (in the UK, the Information Commissioner's Office) without undue delay and, where feasible, within 72 hours of becoming aware.
- **Customers (DPA Section 4.6):** Where DNS Watchdog acts as a processor, the affected customer is notified without undue delay and in any event within 48 hours of becoming aware of a personal data breach involving their data.
- **Data subjects (GDPR Art. 34):** Where the breach is likely to result in a high risk to the rights and freedoms of data subjects, affected individuals are notified without undue delay using clear and plain language.
- **Sub-processors and partners:** Where relevant, sub-processors and other partners are notified to coordinate joint response actions.

Notification content includes, at minimum, a description of the incident, categories and approximate number of data subjects and records affected, likely consequences, the measures taken or proposed, and a contact point for further information. Where information is incomplete at the time of initial notification, updates are provided as the investigation progresses.

7.5 Post-Incident Review

For all Sev 1 and Sev 2 incidents, and for Sev 3 incidents at the discretion of the DPO, a post-incident review is held within ten (10) working days of recovery. The review captures:

- A timeline of events and response actions;
- Root cause analysis;
- What worked well and what did not;
- Specific, owned remediation actions with target dates;
- Any updates required to this policy, runbooks, or technical controls.

Review outputs are stored in the incident register and tracked to completion.

8. Detection and Monitoring

DNS Watchdog maintains the following detection capabilities to support timely identification of incidents:

- Centralised application and infrastructure logs in CloudWatch with structured fields for request tracing, with retention configured per log group.
- Error monitoring through Sentry, with non-actionable events filtered out and alerts on new and regressed errors.
- Cloud account configuration monitoring through AWS-native services for anomalous IAM activity, network changes, and access patterns.
- Billing and usage anomalies that may indicate compromise or abuse.
- External security reports and customer reports submitted to security@dnswatchdog.io.

9. Evidence Handling

During investigation, the incident lead preserves logs, configurations, and other artefacts relevant to the incident. Evidence is handled in line with the controls applicable to its classification level and retained for at least one (1) year after the incident is closed, or longer where required for legal or regulatory reasons.

10. Sub-Processor Incidents

Where a sub-processor (for example, AWS, Clerk, Stripe, Sentry, or Vercel) reports an incident affecting DNS Watchdog or its customers, the DPO assesses the impact, applies the response process described above, and discharges any onward notification obligations to customers and supervisory authorities. The current list of sub-processors is maintained in the Data Processing Agreement.

11. Testing and Training

- Tabletop exercises simulating Sev 1 and Sev 2 incidents are run at least annually with the incident response team.
- Post-incident review actions are tested where they introduce new procedures or controls.
- All personnel receive incident reporting and response training during onboarding and at least annually thereafter.

12. Records and Reporting

DNS Watchdog maintains an incident register documenting all reported incidents regardless of severity or notification outcome. The register records the incident identifier, severity, dates of detection and closure, affected systems and data categories, notifications made, and remediation actions. The register is available to supervisory authorities on request and is reviewed by the DPO at least quarterly.

13. Review

This policy is reviewed annually by the DPO, after any Sev 1 incident, and whenever there are material changes to the platform, sub-processors, or applicable legislation.

14. Contact

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