Incident Response Policy

1. Purpose

This Incident Response Policy outlines Bots For That's approach to identifying, responding to, and recovering from security incidents to minimise impact and ensure transparency.

2. Scope

This policy applies to all information systems, services, and personnel involved in the handling of data processed by Bots For That.

3. Definition of an Incident

A security incident is any actual or suspected unauthorised access, use, disclosure, modification, or destruction of data; or interference with system operations.

4. Incident Response Process

Our incident response follows a structured process:
- Identification
- Containment (short- and long-term)
- Eradication of the root cause
- Recovery and system restoration
- Post-incident analysis and improvements

5. Notification Procedures

We will notify affected customers without undue delay, and within 72 hours where feasible, if personal data is compromised, in line with our Data Processing Addendum.

6. Roles and Responsibilities

The incident response team (IRT) includes technical, legal, and communications personnel. All team members are trained and their roles are documented in the IRP.

7. Testing and Review

This policy and the associated response plan are tested annually or following any major incident. Lessons learned are incorporated into future procedures.