



Website Fair Use Policy – Diamas Security Ltd

Website: diamasecurity.com

Version 1.0 | 16 October 2026

1. Purpose and scope

This policy sets out acceptable use of diamasecurity.com and its enquiry or other publicly available website features. It is intended to protect visitors, Diamas Security Ltd and the security and availability of the website. It applies to website users; employment, client service and supplier arrangements are governed by their separate agreements.

2. Permitted use

You may browse the website, make genuine enquiries and use information to assess our services. Use the website lawfully and respectfully, provide accurate information where requested, and submit information about another person only where you are authorised and have a lawful basis to do so. Ordinary browsing and use of accessibility tools are permitted.

3. Unacceptable use

You must not use the website to:

- Commit fraud, impersonate another person or misrepresent an affiliation with Diamas.
- Send unlawful, threatening, discriminatory, abusive or defamatory material.
- Submit spam, unsolicited promotions or material that infringes privacy or intellectual property rights.
- Introduce malware or malicious code, attempt unauthorised access, obtain credentials or bypass security controls.
- Disrupt the website through denial-of-service activity, excessive automated requests or other interference.
- Harvest personal information or extract content in a manner that infringes rights, circumvents access restrictions or materially impairs the service.
- Conduct intrusive security testing without prior written authorisation from Diamas.

4. Content and branding

Website material, logos and branding belong to Diamas or their respective rights holders. You may view and save reasonable extracts for lawful personal or internal business reference, retaining relevant ownership notices. Obtain permission before commercial republication or implying our endorsement. Nothing in this policy restricts uses permitted by applicable law.



5. Enquiries and information submitted

Only provide information relevant to your enquiry. Do not send passwords, payment card details, confidential site security plans or sensitive personal information through a general enquiry form. Contact us to arrange a suitable secure channel if such information is needed.

We handle personal information in accordance with our Privacy Policy. Sending an enquiry does not by itself create a security services contract, confirm a booking or guarantee a response within a particular time. Service scope and commitments must be agreed separately.

6. Availability, information and external links

We aim to keep website information accurate and useful, but information may change. Confirm current service availability and requirements directly with us before relying on them for an operational decision.

Maintenance or technical issues may interrupt access. Links to external websites are provided for convenience; their content and privacy practices are governed by the relevant provider. This policy does not exclude any liability or rights that cannot lawfully be excluded.

7. Responding to misuse

Where misuse is suspected, we may investigate and take proportionate steps, such as removing submitted material, restricting abusive traffic or suspending access to affected features. Where appropriate and lawful, we may preserve relevant evidence and report suspected offences to the authorities.

Any handling or disclosure of personal information for these purposes must follow applicable law and our Privacy Policy. A user who believes access has been restricted in error can contact us for a review.

8. Reporting concerns

Report website misuse, a suspected vulnerability or an access problem to info@diamasecurity.com. Include the affected page, time and a brief description. Do not access other users' information or continue intrusive testing to demonstrate an issue. Arrange a secure channel before sending confidential evidence.

For personal information concerns, contact our Data Protection Lead, Siddiq Mohammed, at control@diamasecurity.com.

9. Review and changes

We may update this policy to reflect changes to the website, risks or applicable requirements. The approved version will display its effective or last updated date. Changes will apply prospectively and do not override separately agreed contractual terms or statutory rights.