Information Security Policy

DOCUMENT MOG-POL-IS-001 | REV 0 | 16 OCTOBER 2026 | APPROVED

Mogas Design Limited • Company No. 15188968 • 5th Floor, 167–169 Great Portland Street, London W1W 5PF (correspondence address only)

1. Purpose and commitment

Mogas Design Limited is committed to safeguarding client engineering information, personal data, commercially sensitive records and its own business information against unauthorised access, loss, alteration, disclosure and disruption. Controls shall be proportionate to the confidentiality and safety significance of each project and to contractual, regulatory and professional obligations. This policy does not represent ISO 27001 certification.

2. Scope and operating structure

This policy applies to both directors and all independent subcontractors working on behalf of Mogas, including their approved devices, accounts and handling of Mogas/client information. Mogas is a director-led husband-and-wife consultancy (60%/40% ownership), has no salaried employees, and works primarily from a converted garden office and remotely. Subcontractors normally work from their own premises. The London address is solely a correspondence address.

3. Governance and responsibilities

The directors are jointly accountable for information security; a nominated lead director maintains the access register, checks material incidents, and reviews this policy at least annually. Each contractor must protect information entrusted to them, use only approved sharing routes, report suspected breaches immediately, and return or securely delete information on completion as instructed. Project-specific client requirements take precedence where more stringent.

4. Classification and secure handling

Information shall be treated as Public, Internal, Confidential or Client Restricted according to sensitivity and client instructions. Gas infrastructure layouts, pipeline/AGI designs, operating parameters, security arrangements, client asset records and personal data require particular care. Share only the minimum needed with authorised persons; check recipient identity and permissions before sending. Do not upload client-controlled documents to public AI tools, personal sharing sites or unapproved third-party services without explicit authorisation.

5. Accounts, authentication and permissions

Use individual accounts and strong unique passwords, managed securely, with multi-factor authentication wherever supported—especially email and cloud storage. Never share passwords or MFA codes. Apply least-privilege access: each contractor receives only the project folders they need, with access reviewed when assignments change and revoked promptly at completion. Maintain recovery methods for critical accounts securely and separately from devices; the alternative director may access accounts only through authorised delegated access or formally approved recovery, not by informal password sharing.

6. Cloud document storage and backups

Mogas uses account-based cloud/Drive document storage to support controlled remote access. If a device fails or is unavailable, an authorised director can sign in from another trusted device using their own account and prescribed authentication, restore access to approved project files and continue operations. Cloud synchronisation alone is not necessarily an independent backup. The directors shall verify that backup/version history or a separate recoverable copy is available for critical records, document retention and restoration, and periodically test recovery. Do not claim uninterrupted availability or successful backup testing without evidence.

7. Device, network and remote-working security

Devices used for Mogas work should have supported operating systems, automatic security updates, anti-malware protection where appropriate, screen locks, device encryption where available and secure backups. Avoid shared household accounts and unattended unlocked screens. Use password-protected home Wi-Fi with current router security; avoid insecure public Wi-Fi or use an approved secure connection. Report lost devices immediately. Printed confidential records must be secured and disposed of by shredding or equivalent secure means.

8. Engineering information integrity and transfers

Control drawing and report revisions, maintain clear file naming and approved issue/transmittal routes, and retain traceable review and approval status. Use controlled client portals or agreed encrypted transfer channels for sensitive deliverables. Validate source revisions before design/checking/appraisal. Never knowingly alter or bypass client access restrictions or project segregation requirements.

9. Contractor onboarding and offboarding

Before granting access, confirm appropriate competence, confidentiality and data-protection obligations and any client-required security terms. Provide relevant project/security briefings. Record granted folders/accounts and owners; remove access and request return/deletion confirmation when assignments end or contractors change. Contractors must not subcontract information handling to others without approval.

10. Incidents, breaches and business continuity

Suspected phishing, lost/stolen equipment, accidental disclosure, malware, ransomware, account compromise or missing files must be reported to a director immediately. The director shall contain the incident (such as revoking access or isolating an affected device), preserve evidence, assess affected information and advise the client promptly as required by contract. Assess personal-data breaches under UK GDPR and notify the ICO within 72 hours where the statutory reporting threshold applies, unless unlikely to result in risk to individuals; affected individuals must also be informed when legally required. Maintain an incident log, corrective actions and a documented recovery test. Refer to the Mogas Business Continuity Plan.

11. Review, monitoring and improvement

At least annually, and after a significant incident, contractual change or system change, the directors shall review account access, MFA adoption, backup/restoration evidence, device security and contractor access removal. Findings and actions shall be recorded.

Director review and approval

Approved by	Mohammed Fasiuddin, Director
Review / adoption date	16 October 2026
Next planned review	16 October 2027, or earlier if needed
Signature	Signed copy held on file – available on request.

Document status: Approved by the Director. Signed copy held on file – available on request.