ORRJO.

SECURITY

Information Security Policy

Last updated 22 May 2026 • Approved by the CEO • Next review: 22 May 2027

C

Confidentiality

Information is accessible only to authorised individuals.

I

Integrity

The accuracy and completeness of information is maintained.

A

Availability

Information is accessible to authorised users when required.

Purpose

Information collected, analysed, stored, communicated, and reported on by ORRJO may be subject to theft, misuse, loss, and corruption. Information may also be put at risk by poor education, weak training, or breach of security controls. Incidents of this kind can give rise to financial loss, reputational damage, non-compliance with legislation, and contractual breach.

This Information Security Policy sets out the high-level controls ORRJO Ltd applies to protect its own information assets and the information entrusted to ORRJO by its clients. It sits

alongside ORRJO's Privacy Policy, Acceptable Use Policy, Data Protection Policy, and Information Risk Management Policy.

1. Scope

This policy and its supporting controls, processes, and procedures apply to:

- All information used at ORRJO, in any format (digital, paper, audio, video)
- Information processed by other organisations on ORRJO's behalf
- All individuals with access to ORRJO information or technology, including employees, contractors, interns, clients, suppliers, and any third party providing information processing services to ORRJO

2. Objectives

ORRJO's information security objectives are:

- Information risks are identified, managed, and treated to an agreed risk tolerance
- Authorised users can securely access and share information to perform their roles
- Physical, procedural, and technical controls balance user experience and security
- Contractual and legal obligations relating to information security are met
- Client delivery, business administration, and internal product activity considers information security from the outset
- Individuals accessing ORRJO information are aware of their information security responsibilities
- Incidents affecting information assets are resolved promptly and learnt from to improve controls

3. Controls

ORRJO takes a risk-based approach to the controls below. The controls are aligned to ISO/IEC 27001 Annex A and reviewed annually.

3.1 Information security policies

A set of lower-level controls, processes, and procedures supports this high-level policy. The supporting documentation is approved by the Operations Team, published internally, and communicated to staff and relevant external parties.

3.2 Organisation of information security

ORRJO operates a CEO-accountable, proportionate governance model suited to a UK-based B2B agency. The CEO has ultimate accountability for information risk. The Director of Operations and the Head of Operations together act as ORRJO's information governance group, reviewing information risk and security activity at least quarterly. Department heads act as Information Asset Owners for the assets under their remit. The Information Security function is held by the Head of Operations, supported by external advisers on a risk-prioritised basis.

3.3 Human resources security

Right-to-work, identity, and reference checks are completed before joining. All staff sign a confidentiality undertaking and complete security awareness training within 30 days of joining, refreshed annually. Access is revoked promptly on leaving.

3.4 Asset management

All information assets are documented, owned, and classified according to legal requirements, business value, criticality, and sensitivity. Classification determines handling, storage, retention, and disposal.

3.5 Access control

Access is granted on a least-privilege basis, driven by business need and the classification of the information. Multi-factor authentication is mandatory for all business systems where supported. Privileged access is granted sparingly, time-bound, and reviewed quarterly. A formal joiner-mover-leaver process governs all access changes.

3.6 Cryptography

ORRJO.

Data at rest in ORRJO-managed systems is encrypted using AES-256 or equivalent. Data in transit is encrypted using TLS 1.2 or higher. Cryptographic keys are managed by approved key management services and rotated on a defined schedule.

3.7 Physical and environmental security

Information processing facilities are housed in secure areas with defined security perimeters. Cloud infrastructure is provided by ISO 27001 and SOC 2 certified providers. Endpoints are full-disk encrypted, screen-locked when idle, and remotely wipeable.

3.8 Operations security

Documented procedures for critical operations, lightweight change control proportionate to risk, anti-malware controls on all managed endpoints, logging and monitoring of security-relevant events on business systems, and ongoing vulnerability management. Patches to operating systems, browsers, and security-relevant software are applied within risk-tiered timeframes.

3.9 Communications security

Network controls protect information within ORRJO networks. Secure transfer is provided for information moving in and out of ORRJO, in line with classification. Email security includes SPF, DKIM, and DMARC.

3.10 System acquisition, development, and maintenance

Security requirements are defined as part of the requirements for any new system or material change. Development, test, and production environments are separated. Code changes are reviewed before deployment.

3.11 Supplier relationships

Information security requirements are considered when engaging suppliers. Data Processing Agreements are in place with every supplier processing personal data. Supplier security posture is reviewed proportionate to the risk of the data they hold.

3.12 Incident management

Actual and suspected security incidents must be reported immediately to hello@orrjo.com with the subject "Security Incident". Incidents are investigated, contained, and remediated, with lessons fed back into the control set. Where a personal data breach has occurred, the affected client is notified

within 24 hours in line with the signed Services Agreement, and the ICO within 72 hours where required by UK GDPR.

ORRJO.

3.13 Business continuity

Arrangements protect critical business processes from major system failures or disasters. Business impact analysis is undertaken for ORRJO's critical services. Backups are routine, tested, and held in line with retention requirements. Recovery time and recovery point objectives are defined and reviewed.

3.14 Compliance

The design, operation, and management of ORRJO information systems comply with statutory, regulatory, and contractual security requirements, including UK GDPR, the Data Protection Act 2018, PECR, the Computer Misuse Act 1990, and ORRJO's contractual commitments to clients. Compliance is evidenced through internal review (annual minimum, led by the Director of Operations), supplier security confirmations on engagement, and external assessment of critical systems on a risk-prioritised basis.

4. Roles and responsibilities

- The **CEO (Gareth Sandler)** approves this policy, is accountable for information risk at the highest level, and acts as ORRJO's Data Protection and Privacy lead
- The **Director of Operations (Melissa Wilson)** owns the policy, leads the annual review, and is responsible for governance, supplier security, and policy implementation
- The **Head of Operations (Cara Doran)** holds the Information Security lead function, manages day-to-day controls, and coordinates incident response
- **Every department head** acts as Information Asset Owner for the assets within their remit (for example, the Head of Operations owns client delivery systems; the Head of Marketing owns marketing platforms; the Head of Lead Generation owns outbound platforms; the Head of Client Success owns client communication channels)
- **Every member of staff, contractor, and supplier** is responsible for following this policy in their own work

5. Reporting a concern

ORRJO.

If you believe an information security incident has occurred, or you have a concern about ORRJO's controls, email hello@orrjo.com with the subject line "Security Incident". We acknowledge within five working days and act within timelines proportionate to severity.

6. Review

This policy is reviewed annually by the Operations Team and approved by the CEO. The next review is due on or before 22 May 2027. Material changes are communicated to staff and, where relevant, to clients.

7. Contact

ORRJO Ltd
86-90 Paul Street, London EC2A 4NE
Companies House: 13925853
VAT: GB 406 990 969
Email: hello@orrjo.com

OTHER ORRJO POLICIES

ORRJO.

- Privacy Policy
- Terms of Service
- Acceptable Use Policy
- Modern Slavery Statement
- Equality and Diversity
- All policies

ORRJO.

The B2B growth agency that builds brand, creates demand, and books meetings as one integrated system.

Services

ORRJO Intelligence

Creative Studio

Demand Generation

Lead Generation

Resources

Original Research

Methodology

Free Tools

Blog

Company

About

Case Studies

Pricing

Careers

Legal

All Policies

Privacy

Terms

Acceptable Use