

Information security policy

OWNER: AMRIT KHAREL, DIRECTOR, UK OPERATIONS

LAST REVIEWED: SEPTEMBER 2026

NEXT REVIEW: SEPTEMBER 2027

Purpose

This policy sets out how Kyros Software Ltd (Co. 16915277) protects its information assets, systems and data. It applies to all staff, contractors and third parties with access to company systems.

Scope

All information assets including source code, client data, internal documentation, cloud infrastructure, development environments and communication systems.

Objectives

- Protect confidentiality, integrity and availability of information assets
- Meet contractual and regulatory obligations, including UK GDPR and the Data Protection Act 2018
- Align to NCSC guidance and Cyber Essentials principles
- Maintain client confidence in our handling of their data

Roles and responsibilities

Director (**Amrit Kharel**) — overall accountability for information security, risk acceptance, policy approval and incident escalation.

All staff and contractors — comply with this policy, report incidents promptly, complete security awareness training annually.

Asset management

All hardware, cloud accounts and SaaS subscriptions are recorded in an asset register.

Assets are classified as Public, Internal or Confidential.

Confidential data (client data, credentials, personal data) receives the highest level of protection.

Access control

Access is granted on a least-privilege, need-to-know basis.

Multi-factor authentication is required for all cloud services, source code repositories and production infrastructure.

User accounts are reviewed quarterly and revoked promptly on departure.

Shared credentials are prohibited. Secrets are stored in a secrets manager.

Administrative access to production systems is limited to named individuals.

Secure development

Code is peer-reviewed before merge.

Dependencies are monitored for known vulnerabilities.

Secrets are never committed to source control.

Production deployments follow a documented release process.

Endpoint security

All devices used for company work run supported operating systems with automatic updates enabled.

Firewalls are enabled on all endpoints.

Full-disk encryption is enabled on all devices.

Only approved software is installed on work devices.

Incident management

Any suspected security incident is reported immediately to the Director.

The Director assesses severity and contains the incident.

Where personal data is involved, the data protection policy applies (including 72-hour ICO notification where required).

A root cause analysis is completed and lessons learned are documented.

Affected clients are notified without undue delay where their data may be impacted.

Acceptable use

Company systems are for business use. Limited personal use is permitted provided it does not compromise security.

Unapproved cloud storage, messaging or file-sharing services must not be used for company or client data.

Staff must lock screens when leaving devices unattended.

Physical security

As a remote-first company, physical security controls focus on home working environments:

Work devices must be kept secure and not left unattended in public places.

Confidential documents must be stored securely and shredded when no longer needed.

Visitors must not have unsupervised access to work devices.

Review

This policy is reviewed annually or following a significant security incident. The next review is due September 2027.