

Property Portfolio Suite

A PRIVATE ESTATE OPERATING SYSTEM

Information Security Management System

A consolidated reference pack for specialist Cyber, Technology and Professional Indemnity insurance brokers, and for enterprise client procurement teams reviewing the platform under non-disclosure agreement.

Property Portfolio Suite Limited

Company No. 17411633 · Registered in England and Wales

Registered office: 66 Paul Street, London, EC2A 4NA, United Kingdom

Prepared: 21 August 2026

Correspondence: support@propertyportfoliosuite.com

CONFIDENTIAL · DISTRIBUTED UNDER NDA ONLY

Contents

This pack consolidates the three governance documents that describe how Property Portfolio Suite protects the operational record of a private residence: the platform's Information Security Policy, its Data Protection Impact Assessment, and a plain-language reference for advisers explaining where client data lives, how it is protected, and who can reach it.

The documents are shared here as a single unit because a specialist broker or procurement reviewer generally needs to read them together. Each is also maintained as a standalone file and is updated on the same review cadence.

01 Information Security Policy

02 Data Protection Impact Assessment

03 Where Your Data Lives

The pack is not a substitute for the executed Data Processing Agreement or the contractual Master Services Agreement, both of which are exchanged directly with each client. It describes the platform's design and its control environment.

SECTION 01

Information Security Policy

Property Portfolio Suite Ltd (Company No. 17411633 · registered in England and Wales · registered office: 66 Paul Street, London, EC2A 4NA)

Version 1.0 · Effective from the date of adoption · Reviewed at least annually or on material change.

1. Purpose

This policy describes the technical and organisational measures Property Portfolio Suite Ltd ("PPS Ltd", "we") maintains to protect the confidentiality, integrity and availability of information entrusted to the Property Portfolio Suite platform. It is written to be consistent with UK GDPR, the Data Protection Act 2018 and the ICO's recommended controls, and drafted in an ISO 27001-minded structure.

2. Scope

This policy applies to: - All personnel with access to production systems, data or credentials - All third parties (sub-processors) with processing access, governed by written data processing terms - All environments: production, staging/preview, and local development

3. Roles and responsibilities

- **Data Controller:** PPS Ltd (in respect of PPS Ltd's own corporate data)
- **Data Processor:** PPS Ltd (in respect of client-uploaded estate data)
- **Information Security Owner:** the sole director of PPS Ltd (until such time as a separate DPO/CISO is appointed)
- **Sub-processors:** listed on [/sub-processors](#) and governed by their own data processing terms

4. Access control

- **Authentication:** username + password + mandatory two-factor authentication for every account. 2FA cannot be disabled.
- **Password requirements:** minimum length enforced, hashed with bcrypt at rest, never logged in plaintext.
- **Session lifecycle:** idle timeout after 15 minutes of no deliberate interaction (click, keystroke, scroll or tap). Warning modal at 12 minutes.

- **Role-based access control:** five roles (Owner, Admin, IT, Portfolio Manager, House Manager, PA, Family Member, Contractor). Every read and every write is authorised against a permissions matrix.
- **Restricted-tier content:** pins classified `restricted` are stripped from API responses by default, even for the property owner. Access requires a two-step reveal (password + one-time code emailed to the registered address), granting a 3-minute unlock window scoped to a single floor plan.
- **Admin access to production data:** only the platform operator holds direct database credentials. All admin actions in the app UI are logged.

5. Cryptography

- **In transit:** TLS 1.2+ for every client-server connection. HSTS enabled. HTTPS-only.
- **At rest:** MongoDB storage encrypted at the hosting layer. Passwords bcrypt-hashed. Session tokens signed with a rotating secret.
- **Key management:** platform-provided keys, rotated on incident or on personnel change. JWT secret held in environment variables, never in source control.
- **Sensitive-content export:** PDF exports that include Restricted-tier content carry a per-page watermark (viewer identity, timestamp, export code) and a front-cover confidentiality notice.

6. Logging and audit

- **Immutable audit log:** every sensitive action written to `activity_log`. Includes authentication events, password changes, code reveals, PDF exports, permission changes, and export codes.
- **Retention:** audit records retained for the client's active engagement plus 7 years, then destroyed.
- **Notification to the estate's Principal** on: any Sensitive/Hardened PDF export, any restricted-pin reveal, any change to permissions, any password reset.

7. Third-party processors

The definitive list is maintained at `/sub-processors` (public). Each processor is engaged under written data processing terms compliant with UK GDPR Article 28. No new processor is added without a documented review.

8. Data lifecycle

- **Retention** during active engagement: full data retained.
- **On engagement termination:** client-controlled export offered; data marked for deletion; irrevocable deletion completed within 90 days unless a specific legal hold applies.
- **Backups:** encrypted, retained for 30 days on rolling basis, purged on schedule.
- Full detail in `data-retention-policy.md`.

9. Incident response

Every information security incident is handled under the process documented in `incident-response-runbook.md`. Notification obligations under UK GDPR (72-hour ICO notification for breaches likely to result in risk to individuals) are treated as binding.

10. Development practices

- **Source control:** private repository, no client data or credentials in source.
- **Environments:** production isolated from preview/development. Production data does not flow into non-production environments.
- **Change management:** all production changes deployed via a controlled release path with rollback capability.
- **Dependency management:** third-party libraries reviewed on inclusion and monitored for advisories.

11. Physical security

PPS Ltd holds no on-premises client data. All production data resides with the hosting sub-processor named on `/sub-processors`, in facilities certified to industry-standard physical security controls (ISO 27001 / SOC 2 at the infrastructure layer).

12. Review

This policy is reviewed at least annually and after any material change to systems, processing or personnel. Review dates and material changes are logged.

Last reviewed: [date to be recorded on first adoption] **Next scheduled review:** 12 months from adoption

SECTION 02

Data Protection Impact Assessment (DPIA)

Property Portfolio Suite Ltd

Assessment for the Property Portfolio Suite platform. This is a live document; sections are refined as processing changes.

1. Description of the processing

Nature: A software platform on which owners of significant private residences, and the household staff and advisers they authorise, record and manage information about their estates. Processing includes storage, retrieval, editing, sharing under role-based permissions, PDF export, and audit logging.

Scope: Data uploaded voluntarily by the client and their nominated users, comprising property records, floor plans, infrastructure locations (including security equipment), contractor networks, service histories, maintenance and cost records, compliance documents, and access instructions.

Context: Clients are high-net-worth and ultra-high-net-worth private individuals. The information is not the client's own personal data in the ordinary sense; it is the operational record of their private estate. Sensitivity is elevated for security-related items (alarms, CCTV, safes) and access-related items (keys, codes, contractor identities).

Purposes: To provide the client with a single organised record of their estate, to enable authorised staff to operate the estate without holding informal records elsewhere, and to produce paper exports (proposals, briefs, contractor packs) as required by the client.

2. Necessity and proportionality

- **Lawful basis:** contract (Article 6(1)(b)) — processing is necessary to deliver the service the client has engaged.
- **Data minimisation:** only categories the client uploads are stored. No enrichment, no third-party data acquisition, no advertising or profiling.
- **Purpose limitation:** data is used only to deliver the platform to the client. Not shared with any party outside the sub-processors listed on [/sub-processors](#).
- **Storage limitation:** retention aligned with the client's engagement plus a defined post-termination period (see [data-retention-policy.md](#)).
- **Accuracy:** the client and their authorised users edit and delete data at will.

3. Risks to individuals

The subjects of the data are (a) the property owner and (b) household staff, contractors and advisers whose contact details appear in the record.

Risk	Likelihood	Severity	Combined
Unauthorised disclosure of security equipment locations via PDF export	Low	High	Medium
Unauthorised in-app disclosure of restricted content by a legitimate user	Low	High	Medium
Data breach at the platform layer (compromise of MongoDB / hosting layer)	Low	High	Medium
Data breach at a sub-processor	Low	High	Medium
Insider access misuse by PPS Ltd personnel	Very low	High	Low-Medium
Contractor / staff contact details disclosed beyond intended audience	Low	Medium	Low
Loss of access continuity (availability failure)	Low	Low-Medium	Low

4. Measures to reduce risk

Every identified risk is addressed by one or more of:

- **Restricted-tier classification** with a two-step reveal (password + emailed code + 3-minute window) for anything that would materially harm the estate if disclosed.
- **PDF export sensitivity gate:** cover page, per-page watermark identifying the exporter, ownership-role check, audit trail entry, and immediate notification to the estate's Principal for any Sensitive-or-above export.
- **Role-based access control** with a documented permissions matrix.
- **Encryption at rest and in transit.**
- **Mandatory two-factor authentication** on every account.
- **Immutable audit log** for every sensitive action.
- **Idle-session timeout** (15 minutes of no deliberate input).

- **Sub-processor due diligence** and written data processing terms with each.
- **Incident response runbook** with 72-hour ICO notification.
- **Retention/deletion procedure** on engagement termination.

5. Residual risk

After the above measures, the residual risk is assessed as **Low** for each category. No processing activity is classified as high-risk after mitigation.

6. Consultation

- Sub-processors have been reviewed at engagement.
- No consultation with the ICO is deemed necessary as no high-risk residual is present.

7. Sign-off

Assessed by: Sole director of PPS Ltd **Date:** to be recorded on first adoption **Next review:** on any material change to processing, or 12 months from adoption, whichever is sooner.

SECTION 03

Where Your Data Lives

Property Portfolio Suite Ltd · Reference document for prospective clients, advisers and their solicitors.

A factual, no-marketing account of where information you place in the platform is stored, how it is protected, and who can reach it.

Storage

- **Primary datastore:** MongoDB, operated by the platform's hosting sub-processor.
- **Location:** hosting facilities within the United Kingdom or European Economic Area (as declared by the hosting sub-processor). No routine transfer of data outside the UK/EEA occurs.
- **Redundancy:** replicated across multiple availability zones at the hosting layer.

Encryption

- **In transit:** every connection between a client's device and the platform is protected by TLS 1.2 or higher. HTTP Strict Transport Security is enforced. The domain is served with a valid certificate.
- **At rest:** MongoDB storage is encrypted at the hosting layer using industry-standard algorithms (AES-256).
- **Passwords:** hashed with bcrypt. Never stored or logged in plaintext.
- **Session tokens:** signed with a rotating secret held in environment variables, never in source control.
- **Sensitive PDFs:** exports that include Restricted-tier content are watermarked per page and preceded by a confidentiality cover page.

Backups

- **Frequency:** automated daily.
- **Retention:** 30-day rolling window.
- **Encryption:** backups encrypted at rest by the hosting sub-processor.
- **Restoration:** tested on a schedule; restoration procedures are documented in the incident response runbook.

Access

- **You and your nominated users:** full access to your own estate record, under role-based permissions you control.
- **PPS Ltd personnel:** the sole director of PPS Ltd holds administrator credentials required to operate the platform. Administrative actions in the app UI are logged. Direct database access is used only for platform operations or incident response, never for ordinary browsing of client data.
- **Sub-processors:** engaged strictly for the operational function they provide (hosting, payments, email delivery). No sub-processor is permitted to use client data for its own purposes.
- **Third parties beyond sub-processors:** none. Data is not shared, sold or licensed to anyone else.

Sub-processors

The definitive current list is at [/sub-processors](#) on the public site. Each is engaged under written data processing terms compliant with UK GDPR Article 28.

Audit trail

Every sensitive action is written to an immutable audit log: - Sign-in and sign-out - Password changes and resets - Two-factor challenge results - Restricted-content reveals (per plan, per user, with expiry) - PDF exports (with export code, viewer identity, and sensitivity breakdown) - Permission changes - Data deletions

Audit records are retained through the client's engagement plus 7 years, then destroyed.

On termination of your engagement

- You are offered a full export of your record.
- Your data is marked for deletion.
- Deletion is completed, from primary storage and from backups on the next rotation, within 90 days unless a specific legal hold applies.

Contact

Any question about this document, or about your data, may be directed in writing to support@propertyportfoliosuite.com.

Last reviewed: [date to be recorded on first adoption]