

Information Security Policy

Augustine Realty Company

Document	Information Security Policy
Version	1.0
Effective date	2 August 2026
Owner	Austin Clough, Owner (acting Security Officer)
Review cycle	Annually, and on any material change to systems or vendors
Applies to	All personnel, contractors and systems of Augustine Realty Company

1. Purpose

This policy establishes how Augustine Realty Company ("Augustine", "the Company") **identifies, mitigates and monitors** information security risks relevant to its business. It is the top-level document of the Company's information security programme and is operationalised through the procedures named in each section and through the companion **Access Control Policy**.

The Company operates two internal software systems:

System	Purpose	Sensitive data held
Augustine Portal (augustineportal.com)	Public site, resident portal, property-owner portal, staff portal	Applicant and resident PII, lease and payment records, maintenance photos
Augustine Net Worth	Private balance-sheet tool for the Company's own portfolio	Asset valuations, loan balances, bank account balances and transactions obtained via Plaid

2. Scope

This policy covers all information assets owned or processed by the Company: application source code, production systems, databases, third-party services, credentials, and the workstations used to administer them. It applies to every person with access to those assets, including contractors.

3. Roles and responsibilities

The Company is a small organisation. Security accountability is therefore explicit rather than distributed:

- **Owner / Security Officer** — accountable for this policy, for the risk register, for approving access, for vendor selection, and for incident response. Performs the quarterly access review.
- **All personnel** — responsible for following this policy, for protecting credentials issued to them, and for reporting suspected incidents to the Security Officer without delay.
- **Contractors** — bound by the same requirements as a condition of access; access is time-boxed and removed at the end of the engagement.

4. Risk management

4.1 Identify

The Company maintains a **risk register** listing each identified risk, the asset it threatens, its likelihood and impact, the treatment decision, and the control that addresses it. Risks are identified from:

- **Asset and data inventory review** — what data exists, where it is stored, who can reach it, and what its classification is (§5).
- **Vendor review** — every third party that processes Company or resident data (§8).
- **Change review** — every material change to authentication, data storage, external integrations or hosting is assessed before release.
- **Incidents and near-misses** — every incident produces a register entry.

The register is reviewed **at least annually** and on any material change.

4.2 Assess and mitigate

Each risk is rated *high* / *medium* / *low* on likelihood and impact and given one treatment: **mitigate** (apply a control), **avoid** (do not do the thing), **transfer** (insurance or contract), or **accept** (documented, with the Owner's explicit sign-off and a review date). Acceptance is never implicit.

Standing mitigations currently in force:

Risk	Control in force
Bank access tokens exposed by a database leak	Tokens are encrypted at rest with AES-256-GCM before insert; the key lives only in the platform secret store, never in the database or the repository. An authenticated cipher is used so a tampered value fails closed rather than decrypting to garbage.
Unauthorised sign-up to a financial system	Registration and OAuth sign-in are restricted to an explicit email allowlist. Unset means closed — the system denies all by default rather than opening up on a missing variable.
A private route shipped without an auth check	Authentication is enforced by a route-group layout that wraps every private route, not per page, so a newly added route is protected the moment it exists.
Excess data access via the banking integration	Only the <code>transactions</code> product is requested from Plaid. <code>auth</code> and <code>transfer</code> — which confer the ability to move money — are deliberately not requested.
Credential leakage through source control	No secret is committed. Environment and local variable files are excluded from version control; all production secrets are held in the Cloudflare secret store.
Financial data exposed to search engines	The Net Worth application is served with <code>noindex</code> , <code>nofollow</code> and is not published on a guessable custom domain. This is hygiene, not the boundary — the boundary is authentication.
Data loss	Managed Postgres (Neon) point-in-time recovery; restores are tested (§10).

4.3 Monitor

- **Platform observability is enabled** on production workers; request and error logs are retained by the hosting provider and reviewed after any incident, deploy failure, or anomaly report.

- **Application audit records** — significant actions (lease changes, application decisions, password resets, bank connection and revocation) are written to an append-only audit record so that "who did this, and when" can be answered truthfully.
- **Failures are surfaced, not swallowed.** Error handling on primary paths raises rather than silently continuing; decryption failures, missing credentials and malformed stored values are logged as errors.
- **Vendor security advisories** for the platforms listed in §8 are monitored, and dependency updates are applied on a routine cadence.

5. Data classification and handling

Class	Examples	Handling
Restricted	Bank access tokens, API secrets, encryption keys, password hashes	Encrypted at rest; never logged; never in source control; access limited to the Owner.
Confidential	Resident and applicant PII, lease and payment records, account balances and transactions	Access on a least-privilege, role-scoped basis; TLS in transit; retained only as long as required.
Internal	Source code, configuration, operational documentation	Private repositories; access limited to personnel and engaged contractors.
Public	Marketing pages, listings, published policies	No restriction.

Restricted data is **never** written to application logs. Error messages returned from third-party APIs are truncated and only ever the response — never the request, which contains the secret.

6. Access control

Access is governed by the companion **Access Control Policy**, which defines the Company's zero-trust posture, role-based access control model, joiner/mover/leaver procedure, quarterly access reviews, and non-human (service) authentication standards. That document forms part of this policy.

7. Encryption and key management

- **In transit** — TLS 1.2 or higher is required for every connection: browser to application, application to database, and application to every third-party API. There is no plaintext transport path.
- **At rest** — the managed database provider encrypts storage volumes. Additionally, bank access tokens are encrypted at the application layer with AES-256-GCM using a unique random 96-bit IV per record, so that a database backup on its own does not yield usable banking credentials.
- **Passwords** are never stored. They are hashed with **bcrypt**; verification is by hash comparison only.
- **Keys and secrets** are generated with a cryptographically secure random source, stored in the Cloudflare secret store, and are rotatable. Widening access-related configuration requires a deliberate secret update rather than a merged code change.

8. Third-party and vendor management

The Company relies on the following sub-processors. Each was selected in part on its published security posture, each is reached over TLS, and each holds only the data it needs:

Vendor	Purpose	Data it sees
--------	---------	--------------

Plaid	Bank account balances and transaction history	Bank credentials are entered by the user at their own bank, on Plaid's screen — the Company never sees or stores them. The Company holds only an encrypted access token.
Cloudflare	Application hosting, secret storage, TLS termination, DDoS/WAF protection	All application traffic
Neon	Managed PostgreSQL	Application database
Google	OAuth 2.0 sign-in	Authentication assertions only; no password is shared with the Company
Resend	Transactional email (verification)	Email addresses and message content
Innago	Property-management system of record (Portal only)	Resident and lease records

New vendors are reviewed by the Owner before adoption; the review covers what data the vendor would receive, its authentication model, its published security and compliance documentation, and whether the integration can be scoped more narrowly. Vendor access is revoked when an integration is retired.

9. Secure development

- Source is held in private version control; production deployment is from that source only.
- Changes affecting authentication, access control, cryptography, or external data sharing are reviewed before release.
- Automated tests run on the codebase, including tests covering the sign-up allowlist and route-access gating.
- Input from users is validated at trust boundaries with schema validation before use; database access is through a parameterised query builder, not string concatenation.
- Dependencies are kept current and reviewed for known vulnerabilities.
- No secret, credential, or real customer data is used in development or test environments; Plaid is exercised against its **sandbox** environment during development.

10. Backup and continuity

The production database is a managed service with automated backups and point-in-time recovery. Restore capability is verified at least annually. Because the systems are internal business tools rather than customer-facing revenue systems, the recovery objectives are: **RTO 24 hours, RPO 24 hours**. Application code and infrastructure configuration are reproducible from version control.

11. Incident response

1. **Report** — anyone who suspects an incident notifies the Security Officer immediately. There is no penalty for a report that turns out to be nothing.
2. **Contain** — revoke the affected credential, token or session; rotate keys; disable the affected account or integration. Bank connections can be revoked individually.
3. **Assess** — determine what data was involved, over what window, and whether any third party's data is affected, using platform logs and the application audit record.

4. **Notify** — affected individuals, and where applicable Plaid and other affected vendors, are notified without undue delay and in accordance with applicable North Carolina and federal breach-notification law.
5. **Recover and learn** — restore service, then record the root cause and the corrective control in the risk register.

12. Personnel and endpoints

- Access is granted only after the person has read this policy and the Access Control Policy.
- Workstations used to administer production must have full-disk encryption, automatic screen lock, an active OS firewall, and current security updates.
- Access is removed **on the same day** a person's engagement ends.

13. Acceptable use

Company systems and data are used for Company business. Restricted and Confidential data is not copied to personal accounts, personal devices, or unapproved third-party services. Credentials are not shared between people.

14. Policy review and exceptions

This policy is reviewed at least annually by the Owner and updated on any material change to systems, vendors or applicable law. Any exception must be requested in writing, approved by the Owner, recorded in the risk register with a compensating control, and given an expiry date.

Approved by

Austin Clough — Owner, Augustine Realty Company

Signature: _____ Date: _____