

# Access Control Policy

## Augustine Realty Company

|                 |                                                          |
|-----------------|----------------------------------------------------------|
| Document        | Access Control 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 roles |
| Parent document | Information Security Policy v1.0                         |

### 1. Purpose and scope

This policy defines who may access Augustine Realty Company systems and data, on what basis, how that access is granted and removed, how it is reviewed, and how non-human (machine-to-machine) access is authenticated. It applies to all Company systems — Augustine Portal, Augustine Net Worth, the production database, the hosting platform, and every third-party service — and to every person and service that reaches them.

### 2. Principles

1. **Deny by default.** Access is refused unless it has been explicitly granted. Missing or unset configuration results in *no* access, never in open access.
2. **Least privilege.** A person or service receives the narrowest set of permissions that lets them do their job, and no more.
3. **Zero trust.** No request is trusted because of where it came from (§3).
4. **Accountability.** Every account belongs to exactly one identifiable person. Shared logins are prohibited.
5. **Separation of duties.** Read access and the ability to change data are distinct grants (§4).

### 3. Zero trust access architecture

The Company operates a zero-trust model. There is **no trusted internal network** and no VPN perimeter whose crossing confers access.

- **Every request is authenticated at the application layer**, on every request, regardless of origin. Authentication is not inferred from network location, IP address, or the fact that a previous request in the session succeeded.
- **Enforcement is structural, not per-page.** All private routes sit inside a route group whose layout performs the authentication check, so a route added later is protected the moment it exists rather than when someone remembers to add a guard. There is no unauthenticated view of any financial or resident record.
- **Session validity is re-evaluated continuously.** A user who is deactivated or deleted is refused on their next request; the session token alone is not sufficient proof of a live entitlement.
- **Identity is verified before enrolment.** Sign-in requires a verified email address, and both password registration and federated (Google OAuth 2.0) sign-in are additionally restricted to an explicit allowlist of permitted addresses. An unset allowlist denies everyone.

- **Every hop is encrypted and authenticated.** Browser to application, application to database and application to third-party API all require TLS 1.2 or higher with credentials presented on each call. Nothing is reachable without credentials by virtue of being "inside".
- **The infrastructure has no standing open ports.** Applications run as managed serverless workers; the database accepts only TLS connections authenticated with a credential held in the platform secret store.
- **Least-privilege scoping is enforced in the data layer.** Records are scoped to the requesting identity — for example a property owner sees only properties where they are the recorded owner — so authorisation is not merely a hidden navigation link.

## 4. Role-based access control (RBAC)

Permissions are attached to **roles**, and roles are assigned to users. No permission is granted to an individual outside a role.

**Augustine Net Worth** — two roles, because the entire surface is a single household balance sheet:

| Role   | May do                                                                                                     |
|--------|------------------------------------------------------------------------------------------------------------|
| OWNER  | Read everything; create, edit and delete assets, loans and valuations; connect and revoke bank connections |
| VIEWER | Read only. Intended for an accountant or a lender performing diligence. Cannot mutate any record.          |

**Augustine Portal** — roles reflect genuinely different relationships to the business, and the boundaries between them are enforced, not cosmetic:

| Role                      | May do                                                                                                                                                                           |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Staff roles (incl. OWNER) | Administer applications, leases, maintenance and residents, within the staff portal                                                                                              |
| CONTRACTOR                | See only work assigned to them                                                                                                                                                   |
| TENANT                    | See only their own tenancy, invoices, documents and maintenance requests                                                                                                         |
| PROPERTY_OWNER            | See only their own properties and their own money. Deliberately excluded from staff routes — this is a landlord whose property the Company manages, not a member of the Company. |

Role checks are applied server-side on every protected action. Hiding a control in the interface is never treated as an access control.

## 5. Provisioning, modification and deprovisioning

- **Joiner.** Access is requested from and approved by the Owner, granted at the lowest role that fits the job, and issued only after the person has read this policy and the Information Security Policy. Each account is created for one named individual.
- **Mover.** When a person's responsibilities change, their role is changed to the new one and the previous entitlements are removed at the same time. Accumulated permissions are not permitted.
- **Leaver.** Access is revoked on the **same day** the engagement ends: the account is deactivated (which takes effect on the next request), the person is removed from the sign-up allowlist, and any credential they held — third-party service logins, API keys — is rotated.

## 6. Periodic access reviews and audits

Access reviews are performed **quarterly** by the Owner (Security Officer), and additionally after any personnel change or security incident. Each review is recorded — date, reviewer, systems covered, findings, actions taken — and the record is retained for at least two years.

Each review covers:

1. **User accounts and roles** in Augustine Portal and Augustine Net Worth — is every account still needed, and is every role still the minimum required?
2. **The sign-up allowlist** — does it still contain only current, authorised addresses?
3. **Administrative access** to the hosting platform, the database provider, the domain registrar, the email provider, the version-control organisation, and the Plaid dashboard.
4. **Non-human credentials** — API keys, OAuth clients and encryption keys: which exist, what each is for, when it was last rotated, and whether it is still in use (§7.4).
5. **Active bank connections** — is every connected institution still one the business intends to read?
6. **Audit records** — a review of the append-only audit log and platform logs for access anomalies.

Any account, role or credential that is no longer required is removed during the review, not deferred.

## 7. Non-human (service) authentication

Machine-to-machine access never uses a human's credentials and never uses a shared static password.

### 7.1 TLS everywhere

All service-to-service traffic uses **TLS 1.2 or higher** with server certificate validation. Certificates for Company domains are issued and rotated automatically by the hosting provider. Plaintext HTTP is not used for any call carrying credentials or data, and there is no fallback path that downgrades.

### 7.2 OAuth 2.0

Federated user authentication uses **Google OAuth 2.0** with a registered client and an explicit allowlist of authorised redirect origins. A request from an unauthorised origin is refused by the identity provider before it reaches the Company's systems. The Company never receives or stores the user's Google password.

### 7.3 API credentials and tokens

- **Plaid** is authenticated with a client ID and a per-environment secret, presented over TLS on every call. Secrets are held in the Cloudflare secret store, never in source control or configuration files.
- **Plaid access tokens** obtained per bank connection are **encrypted at rest with AES-256-GCM** before they touch the database, using a key held only in the secret store. There is exactly one place in the codebase where a plaintext bank token exists in memory, and it does not write to disk.
- **The database** is reached with a credential held as a platform secret over a TLS-only connection.
- **Inbound webhooks are not trusted.** Webhook bodies are never treated as authorisation; the system re-fetches from the provider's authenticated API rather than acting on posted content, and a per-connection cooldown limits abuse.

### 7.4 Credential lifecycle

Every non-human credential has a named purpose and an owner. Credentials are rotated on a defined schedule, immediately on suspected compromise, and immediately when a person with access to them departs. Unused credentials are revoked at the quarterly review.

## 8. Authentication requirements for people

- Passwords are stored only as **bcrypt** hashes and are never recoverable or displayed.
- Federated sign-in via Google is preferred where available, and the Google account used for administrative access must itself have **multi-factor authentication enabled**. MFA is required on every third-party administrative console (hosting, database, registrar, Plaid dashboard, version control).
- Email addresses must be verified before an account is usable.
- Sessions are held in signed tokens, are re-validated against account status on each request, and expire.
- Credentials are never shared between people, never sent over email or chat, and never committed to source control.

## 9. Privileged access

Administrative access to production — the hosting account, the database, the secret store and the Plaid dashboard — is limited to the Owner. Granting it to anyone else requires the Owner's written approval, is time-boxed, is recorded in the access review record, and is revoked when the reason for it ends.

## 10. Physical and endpoint access

Any device used to reach production systems or Restricted data must have full-disk encryption, automatic screen lock, an active OS firewall, and current security updates. Devices are not left unattended and unlocked. Company data is not stored on devices belonging to anyone outside the Company.

## 11. Exceptions and enforcement

Any exception to this policy must be requested in writing, approved by the Owner, recorded with a compensating control and an expiry date, and reviewed at the next quarterly access review. Violations may result in immediate revocation of access and termination of the engagement.

---

### Approved by

Austin Clough — Owner, Augustine Realty Company

Signature: \_\_\_\_\_ Date: \_\_\_\_\_