Cybersecurity Policy (Castle Capital LLC)

Last Updated: October 19, 2025

Effective Date: October 19, 2025

Policy Owner: Founders (Merritt & Marcus)

1. Overview & Scope

This policy documents Castle Capital LLC's current, minimal security controls appropriate for a two-person startup operating a single cloud VPS and select SaaS tools. It reflects the present state to avoid overstatements and establishes a short, practical roadmap to improve security over time.

2. Roles & Accountability

- Security Lead: Marcus (engineering, keys, server hardening, backups).
- Operations/Compliance Lead: Merritt (policies, access reviews, vendor checks, incident coordination).
- Both founders are required to follow this policy and approve exceptions in writing (email is sufficient).

3. Systems in Scope

- Single cloud VPS (production + admin). No network segmentation, DMZ, or VPN.
- SSH key–based administration only.
- Public web service currently served over HTTP (no TLS).
- SaaS used for docs, repo hosting, and task tracking.
- No on-prem office network, Wi-Fi, or mobile device management.
- No crypto/digital-asset custody or trading.

4. Access Controls (Passwords & Sessions)

- Password policy: minimum 8 characters; unique password per service; use of a reputable password manager is required.
- Email Verification for MFA
- Session lifetime: up to 24 hours. Re-authentication required for account-level changes.
- Account provisioning/de-provisioning performed by Security Lead with same-day revocation upon role change or exit.
- No shared accounts; if unavoidable (rare), credentials are stored in the password manager and rotated when access changes.

5. Authentication & Remote Administration

- Administrative access via SSH keys only; passwords disabled for remote shell.
- Key generation: 4096-bit RSA or modern Ed25519; private keys stored only on founder laptops.
- Git and CI access limited to founder accounts.

6. Data Handling & Encryption

- Data at rest on the VPS uses AES-128 (cloud provider default).
- Data in transit for public endpoints currently uses HTTP (no TLS). Sensitive credentials and tokens are not transmitted over HTTP where avoidable.
- Secrets (API keys/tokens) are stored in an encrypted password manager and injected into services via environment variables; do not commit secrets to source control.
- Backups and snapshots are encrypted by the cloud provider per its default settings.

7. Logging & Monitoring

- Application and server logs written to local files and rotated regularly.
- Retain logs for 30 days unless space requires earlier rotation.

8. Backups & Recovery

- Daily VPS snapshot; retain 28 daily / 32 weekly copies when feasible.
- Restore test performed at least twice a year or after major changes.
- RTO target: next business day; RPO target: last daily snapshot.

9. Change Management

- All changes tracked in git.
- At least one other founder reviews code changes that affect authentication, authorization, or data handling.
- Emergency fixes are documented after the fact in the task tracker.

11. Vendor & SaaS

- Use reputable providers with baseline security (HTTPS by default, access controls, documented backups).
- Review billing/admin access quarterly; remove unused admins and OAuth grants.
- Store only minimum necessary data in SaaS tools.

12. Policy Review & Exceptions

- Review semi-annually or upon major changes (new vendor, new data type, or new surface exposed).
- Exceptions must be approved by both founders via email and documented in the task tracker.