

Vulnerability Management Policy

Augustine Realty Company

Document	Vulnerability Management Policy
Version	1.0
Effective date	2 August 2026
Owner	Austin Riley Clough, CEO (acting Security Officer) — augustinerealtycompany@gmail.com
Review cycle	Annually
Parent document	Information Security Policy v1.0

1. Purpose and scope

This policy defines how Augustine Realty Company finds, prioritises and fixes security vulnerabilities across three surfaces: **application dependencies**, **production infrastructure**, and **the endpoints** (laptops and workstations) used by personnel and contractors to reach either.

2. Scanning

2.1 Application dependencies

- **Continuous automated scanning** of every dependency in both application repositories through GitHub Dependabot alerts, configured in `.github/dependabot.yml`. Alerts are raised against the CVE feed as soon as an advisory is published, not on a scan schedule.
- **Weekly automated update pull requests** for npm dependencies and GitHub Actions, so that patching is a routine merge rather than an emergency.
- `npm audit` is run before each production deployment; a release is not shipped with an unreviewed high or critical advisory.

2.2 Production infrastructure

Production runs entirely on managed, serverless platforms — Cloudflare Workers for compute and Neon for PostgreSQL. There is no Company-managed operating system, virtual machine, container image or open network port in production, so the host-level patching surface belongs to those providers, who patch it continuously and publish their compliance attestations. What remains in the Company's control, and is therefore scanned and reviewed, is: the application code and its dependencies (§2.1), the runtime compatibility date, the platform configuration (bindings, secrets, routes), and the third-party integrations. Platform security advisories from Cloudflare, Neon and Plaid are monitored.

2.3 Endpoints

Every laptop or workstation used to reach production or Restricted data runs **Microsoft Defender Antivirus with real-time protection and cloud-delivered protection enabled**, which performs continuous malware and threat scanning, and **Windows Update with automatic updates enabled** for operating-system and driver patches. Full-disk encryption (BitLocker), an enabled host firewall, and automatic screen lock are required on the same devices. The Owner verifies this configuration on every device at the quarterly access review, and no device outside this standard is permitted to hold Company data.

3. End-of-life software

Software that has reached, or is within **six months** of, its end-of-life or end-of-support date is treated as a vulnerability in its own right and is scheduled for upgrade or replacement. This is checked at each quarterly review and covers: the Node.js runtime and Workers compatibility date, the Next.js and React major versions, the PostgreSQL major version, and the operating system on every endpoint. Running unsupported software in production is not permitted without a documented, time-boxed exception approved by the Owner.

4. Risk rating and remediation SLA

Vulnerabilities are rated using **CVSS v3.1 base score**, adjusted for whether the affected code path is actually reachable in our deployment.

Severity	CVSS	Remediate within
Critical	9.0 – 10.0	24 hours
High	7.0 – 8.9	7 days
Medium	4.0 – 6.9	30 days
Low	0.1 – 3.9	90 days, or at the next routine dependency update

The clock starts when the alert is raised, not when it is read. Any vulnerability that is actively exploited in the wild is treated as Critical regardless of its score.

Where a fix is not available within the SLA, the Owner records a **compensating control** — disabling the affected feature, restricting the reachable path, or pinning to a safe version — together with a review date. An SLA breach without a recorded compensating control is not an acceptable state.

5. Verification and records

Every remediation is verified: the alert must close, and the deployed version must be confirmed to contain the fix. The **quarterly access review** record includes a vulnerability summary — what was open, what was fixed, what remains open with which compensating control — and is retained for at least two years.

6. Externally reported vulnerabilities

Reports from outside the Company are accepted at augustinerealtycompany@gmail.com and are acknowledged within **3 business days**. They are triaged and remediated under the same SLA as internally discovered issues, and the reporter is told what was done.

Approved by

Austin Riley Clough — CEO, Augustine Realty Company

Signature: _____ Date: _____