



Prestigious HOA Portal

PROPERTY MANAGEMENT SERVICES

SERVICE LEVEL AGREEMENT

SLA v1.0

Uptime, support, security, and data-protection commitments
between Prestigious Property Management Services LLC
and its customers.

Effective date: [fill on signing] Version: 1.0 · February 2026 Between: Prestigious Property Management Services LLC ("Provider") and the client identified in the executed Order Form ("Customer").

1 · Definitions

Term	Meaning
Service	The Prestigious HOA Portal SaaS application at the Customer's designated URL and its supporting APIs, mobile web app, and PWA.
Business Hours	Monday–Friday, 08:00–18:00 US/Eastern, excluding US federal holidays.
Non-Business Hours	All other hours, including weekends and holidays.
Uptime	Percentage of minutes in a calendar month during which the Service responds to a <code>GET /api/healthz</code> probe with HTTP 200 within 2000 ms.
Downtime	Any minute during which the Service fails the Uptime probe, excluding Scheduled Maintenance and Excluded Events (§ 8).
Incident	An unplanned interruption to the Service, degradation of performance, or unavailability of a documented feature.
RTO	Recovery Time Objective — the maximum acceptable time to restore Service following a disaster.
RPO	Recovery Point Objective — the maximum acceptable window of data loss following a disaster.

2 · Availability Commitment

2.1 MONTHLY UPTIME TARGET

Provider will use commercially reasonable efforts to maintain the following monthly uptime for the production environment (`portal.prestigiouspm.net`):

Tier	Monthly Uptime	Max downtime / month
Standard (included)	99.5 %	~3 h 39 m
Business (add-on)	99.9 %	~43 m
Enterprise (custom)	99.95 %	~21 m

Uptime is measured by an external probe striking `/api/healthz` every 60 seconds from at least two geographic regions. A minute is counted as "down" only when both probes fail.

2.2 SERVICE CREDITS

If monthly uptime falls below the tier commitment, Customer is entitled to a service credit against the next monthly invoice:

Achieved Uptime	Credit (% of monthly fee)
< 99.5 % (Standard) or < 99.9 % (Business) or < 99.95 % (Enterprise)	10 %
< 99.0 % (Standard) or < 99.5 % (Business) or < 99.9 % (Enterprise)	25 %
< 98.0 % (Standard) or < 99.0 % (Business) or < 99.5 % (Enterprise)	50 %
< 95.0 % (any tier)	100 %

Credits must be requested in writing within 30 days of the qualifying event. Credits are the sole and exclusive remedy for any Uptime failure.

3 · Support & Incident Response

3.1 SEVERITY DEFINITIONS

Severity	Definition	Example
P0 — Critical	Production is fully down or a security incident is in progress. Data loss or corruption suspected.	Login broken for all users; PII exposure suspected.
P1 — High	A core module is broken for all users OR a single-community outage of critical functionality.	Payments failing site-wide; rent charges not posting.
P2 — Medium	A feature is degraded or broken for a subset of users, and a workaround exists.	SMS inbox slow to refresh; PDF export producing incorrect totals.
P3 — Low	Cosmetic issue, question, or feature request.	Typo, styling glitch, "how do I..."

3.2 RESPONSE & RESOLUTION TARGETS

Response time = first substantive human reply. Resolution target = the deadline by which Provider will either restore service, deploy a fix, or provide a documented workaround.

Severity	Response (Business Hours)	Response (Non-Business Hours)	Resolution Target
P0	15 minutes	30 minutes (24/7)	4 hours
P1	1 hour	4 hours	1 business day
P2	4 business hours	Next business day	5 business days
P3	1 business day	Next business day	Next release

Business and Enterprise tiers extend P0 and P1 response to 24/7 with named on-call engineers and a direct phone line.

3.3 SUPPORT CHANNELS

Channel	Availability	Purpose
Email support@prestigiouspm.net	24/7 (P0/P1)	Primary channel — all severities
In-app support widget	24/7	Feature Qs, non-urgent bugs
Slack shared channel	Business Hours (Business+)	Real-time collab
Phone / SMS on-call	24/7 (Enterprise)	P0 escalation

Provider will not open new tickets from social media, third-party review sites, or vendor forums — those are read-only.

3.4 ESCALATION PATH

1. T1 support — receives ticket, triages, patches / documents workaround
2. T2 engineering — escalated after 30 min (P0) or 2 h (P1)
3. On-call CTO — escalated after 2 h (P0) or same business day (P1)
4. Executive — Customer may request executive escalation after 4 h (P0) without resolution

4 · Scheduled Maintenance

4.1 STANDARD MAINTENANCE WINDOWS

Type	Window	Notice
Routine (config, minor deploys)	Any time, zero-downtime	None required — zero user-facing impact
Standard (major deploys, dependency upgrades)	Sunday 03:00–05:00 US/Eastern	≥ 72 hours advance email + banner
Extended (DB migrations, region moves)	Sunday 02:00–06:00 US/Eastern	≥ 7 days advance email + banner
Emergency (security patches, critical bugs)	Any time	Best-effort — post-hoc RCA within 5 business days

4.2 EXCLUSIONS FROM UPTIME CALCULATION

Scheduled Maintenance windows and Emergency Maintenance under 30 minutes are excluded from Downtime calculations for Section 2. Emergency Maintenance exceeding 30 minutes is counted as Downtime.

5 · Data Protection

5.1 BACKUP

Provider maintains encrypted MongoDB backups of Customer data with the following schedule:

Backup	Frequency	Retention	Storage
Automated snapshot	Every 6 hours	7 days	AWS S3 (encrypted at rest, versioned)
Nightly full	Daily @ 02:00 UTC	30 days	AWS S3, cross-region replica
Weekly full	Sunday @ 02:00 UTC	90 days	AWS S3 Glacier Deep Archive
Monthly full	1st of month	12 months	AWS S3 Glacier Deep Archive

5.2 RECOVERY OBJECTIVES

Scenario	RTO	RPO
Application server failure	≤ 15 minutes	0 (no data loss)
Regional MongoDB failure	≤ 2 hours	≤ 6 hours
Regional AWS outage	≤ 4 hours	≤ 6 hours
Multi-region catastrophic loss	≤ 24 hours	≤ 24 hours

Restore drills are executed quarterly against the most-recent snapshot; drill results are shared with Customer on request.

5.3 DATA PORTABILITY & DELETION

- Export: Customer may export all their data (residents, leases, ledger, docs, audit log) at any time via `/admin/audit` (CSV), `/admin/reports` (PDF), and `/admin/data-export` (full JSON dump). No fee.
- Deletion on termination: Provider will delete all Customer data from active systems within 30 days of contract end, and purge from all backups within 90 days, providing a written attestation of deletion on request.
- Right to be forgotten (CCPA/GDPR): Individual data-subject deletions honoured within 30 days of a verified request.

5.4 DATA RETENTION (IN-SERVICE)

Data category	Retention
Financial records (charges, payments, statements)	7 years (regulatory)
Audit log (hash-chained, tamper-evident)	7 years
Communications (SMS threads, emails)	3 years
Access credentials / guest pass history	1 year
Vendor W-9 / COI documents	Duration of relationship + 7 years
Session logs	90 days

6 · Security Commitments

Provider maintains the following technical + organisational controls (verified by internal audit; SOC 2 Type I in progress, Type II targeted Q4 2026):

6.1 APPLICATION SECURITY

- Encryption in transit — TLS 1.2+ enforced with HSTS in production
- Encryption at rest — MongoDB AES-256 (Emergent-managed), S3 AES-256 backups
- Authentication — JWT (HS256, 24 h TTL), bcrypt (cost ≥ 12), auth-endpoint rate limiting (10 attempts / minute / IP)
- Password policy — ≥ 10 chars, letter + digit, breach-corpus blocklist
- CSRF — Bearer-first + `SameSite=None` + no unauth'd state writes
- XSS — React auto-escaping + strict CSP (`X-Content-Type-Options: nosniff` , `X-Frame-Options: DENY` , `Referrer-Policy: strict-origin-when-cross-origin` , restrictive Permissions-Policy)
- SSRF — Admin webhook rules resolve DNS + block private/loopback/link-local ranges before dispatch; `follow_redirects=False` on outbound calls
- Bot mitigation — Cloudflare Turnstile on public sign-up
- Rate limiting — Redis-backed, cross-pod; auth endpoints 5–10 req/min/IP; global 200 req/min/IP

6.2 MULTI-TENANT ISOLATION

- Every collection scoped by `property_id` . Every read/write goes through a helper that enforces the requesting user's `property_ids` — direct DB access is not exposed.
- Admin actions cross-property require explicit access; portfolio views only visible to owners of all included properties.
- Impersonation (admin $\rightarrow$ resident) is JWT-scoped 30 minutes, audit-logged with actor triple, and never allowed admin $\rightarrow$ admin/owner.

6.3 OBSERVABILITY & INCIDENT DETECTION

- Sentry — All backend errors + frontend crashes reported with PII scrubbing enabled
- Structured audit log — SHA-256 hash-chained, tamper-evident, exportable
- Uptime monitoring — External probes against `/api/healthz` every 60s
- Anomaly alerts — Login spike, failed-auth spike, AI cost budget, background-job stall
- Log retention — 90 days hot, 1 year cold

6.4 PERSONNEL SECURITY

- Every engineer with production access completes background check + annual security training
- Access to production data is role-scoped (SRE / on-call / observability); non-emergency changes go through PR + code review
- MFA enforced on all admin consoles (AWS, Emergent, Stripe, GitHub, GHL)
- Offboarding: access revoked within 4 business hours of separation

6.5 SECURITY INCIDENT RESPONSE

Provider commits to the following on discovery of a confirmed security incident:

Step	Deadline
Internal escalation to CTO + counsel	30 minutes
Preliminary scope assessment	4 hours
Notification to affected Customers (email + phone)	24 hours
Regulatory notification (if applicable)	Per statute (typically 72 h GDPR / 60 d HIPAA / state law)
Post-incident RCA + remediation plan	5 business days

7 · Change Management

- Major releases (breaking API changes, UI redesigns): ≥ 14 days notice + changelog + optional preview window
- Minor releases (new features): Rolled out weekly; changelog posted at [/changeLog](#)
- Patch releases (bug fixes, security): Rolled out continuously (canary $\rightarrow$ 10 % $\rightarrow$ 100 %)
- Deprecations: ≥ 90 days notice for any deprecated API or feature
- Sunset: A deprecated feature remains available in read-only mode for ≥ 30 days before removal

8 · Excluded Events (Force Majeure)

Provider is not liable for downtime caused by:

- Customer's own network, ISP, VPN, DNS misconfiguration, or device
- Customer's misuse of the API (e.g., exceeding rate limits, invalid credentials)
- Third-party dependencies outside Provider's reasonable control — specifically named:
 - Emergent Platform / Kubernetes host — infrastructure hosting SLA passes through
 - Cloudflare — edge + Turnstile
 - Stripe — payments + Financial Connections
 - AWS S3 — object storage
 - Resend — transactional email
 - GoHighLevel — SMS
 - DocuSign — envelope signatures
- Force majeure (natural disaster, war, pandemic, government action, ISP outages)

- Scheduled maintenance windows disclosed per § 4
- Beta / preview features clearly labelled as such in the UI or docs

Third-party pass-through: If a Stripe outage causes a payments failure counting as Downtime, Provider will file for and pass through any Stripe service credit to Customer. Provider maintains an incident-status page at status.prestigiouspm.net that mirrors upstream vendor status.

9 · Reporting & Transparency

9.1 MONTHLY SERVICE REPORT

Within 10 business days after each calendar month, Provider will publish a report at status.prestigiouspm.net/reports containing:

- Actual monthly uptime (%)
- Incident count by severity
- MTTR (mean time to resolve) per severity
- Any credits earned by Customer
- Notable events + RCAs

9.2 REAL-TIME STATUS PAGE

Public status page at status.prestigiouspm.net :

- Component-level health (API, DB, payments, email, SMS)
- Live incident timeline with updates every 30 min during active incidents
- Historical uptime chart (90 days)
- Subscribe to email + webhook notifications

9.3 ANNUAL REVIEWS

Customer is entitled to one (Business tier) or two (Enterprise tier) 90-minute annual reviews with the Provider's CTO covering:

- Prior-year uptime vs. commitment
 - Roadmap alignment
 - Security posture summary
 - Renewal negotiation
-

10 · Support-Included Scope

Support covers:

- Login / authentication / password reset
- Data corruption or loss
- Financial calculation errors (rent, late fees, statements, 1099s)
- Third-party integration failures (Stripe, Resend, GHL, DocuSign)
- Documented feature not working as described
- Security concerns
- Performance degradation (see § 11)

Support does NOT cover:

- Custom feature development (billable separately)
- Training beyond onboarding + provided manuals (billable via Professional Services)
- Third-party service configuration outside our platform (e.g., customer's own Stripe account setup — we document, don't operate)
- Data entry / data cleanup (unless caused by a Provider bug)
- Advice on customer's legal, tax, or regulatory questions

11 · Performance Targets

Metric	Target (p95)
API GET (cached)	≤ 200 ms
API GET (uncached)	≤ 800 ms
API POST / PATCH	≤ 1200 ms
Page-load (LCP, warm browser cache)	≤ 2.5 s
Search + AI query	≤ 5 s
PDF export (statement / packet, up to 50 pages)	≤ 20 s
Bulk CSV import (up to 5 000 rows)	≤ 60 s

Sustained breach of a p95 target for > 30 min qualifies as a P1 Incident.

12 · Fair-Use & Rate Limits

Endpoint class	Limit
Auth (/auth/*)	5–10 / minute / IP
General API	200 / minute / IP
AI-backed endpoints (Claude Sonnet 4.5)	10 / minute / JWT + \$50 / month / property (soft ceiling)
Bulk import	3 concurrent jobs / property
Broadcast SMS	5 000 / day / property (higher on request + carrier approval)
Broadcast Email	20 000 / day / property

Overage above soft ceilings triggers a courtesy email — hard blocks are only applied when abuse is suspected.

13 · Confidentiality & Data Handling

Fully governed by the executed Data Processing Addendum (DPA) and Master Subscription Agreement (MSA). Highlights:

- Provider is a Processor under GDPR / Service Provider under CCPA
- Sub-processors listed at prestigiouspm.net/legal/subprocessors — 30-day advance notice on any change
- Customer data is never used to train AI models beyond that Customer's own workspace
- Provider will notify Customer within 24 h of any legal process compelling disclosure

14 · Business Continuity

- Redundancy: Application deployed across ≥ 2 Kubernetes pods (auto-scaling to 6 under load), MongoDB primary + secondary + arbiter, Redis with AOF persistence
- Backup site: MongoDB replica in a second AWS region (cross-region replication for backups)
- BCP drill: Quarterly disaster-recovery drill (full restore of latest backup into isolated environment, verified against a scripted test suite)
- Vendor concentration limits: No single third-party vendor exceeds 20 % of Provider's cost base (except Emergent hosting + AWS)

15 · Termination

- Convenience: Either party may terminate with 30 days' written notice at the end of any monthly billing cycle
- Cause: Termination for uncured material breach with 30 days' notice + right to cure
- Data return: Customer may export all data any time before termination + within 30 days after (via [/admin/data-export](#))
- Post-termination: Provider retains data for 30 days ("winding-down" grace period) then permanently deletes; backups purged within 90 days total

16 · Changes to This SLA

Provider may update this SLA once per calendar year with ≥ 60 days notice; Customer may terminate without penalty if any change materially reduces the commitments in §§ 2, 3, 5, 6, 8.

17 · Governing Law

Governed by the laws of Florida, exclusive jurisdiction in Palm Beach County, Florida. Disputes escalated via good-faith negotiation → mediation → binding arbitration (AAA Commercial Rules).

Appendix A · Contact Directory

Function	Channel
PO hotline (Enterprise)	(561) 926-2292
PO email (all tiers)	p0@prestigiouspm.net (auto-escalates on-call)
General support	support@prestigiouspm.net
Security disclosures	security@prestigiouspm.net
Billing	billing@prestigiouspm.net
Legal / DPA	legal@prestigiouspm.net
Status page	status.prestigiouspm.net

Appendix B · Tier Comparison

Uptime	99.5 %	99.9 %	99.95 %
P0 response	15 min BH / 30 min NBH	15 min 24/7	5 min 24/7
P1 response	1 h BH / 4 h NBH	30 min 24/7	15 min 24/7
Support channels	Email + widget	+ Slack	+ phone + named CSM
Backup RPO	6 h	6 h	1 h
Annual review	—	1 × 90 min	2 × 90 min + quarterly touchpoint
SOC 2 report	On request (from Q4 2026)	Included	Included
Named on-call engineer	—	—	Yes
Dedicated staging env	—	Optional	Included

Signed for Provider: ____ Name: ____ Title: _____ Date: _

Signed for Customer: ____ Name: ____ Title: _____ Date: _