4

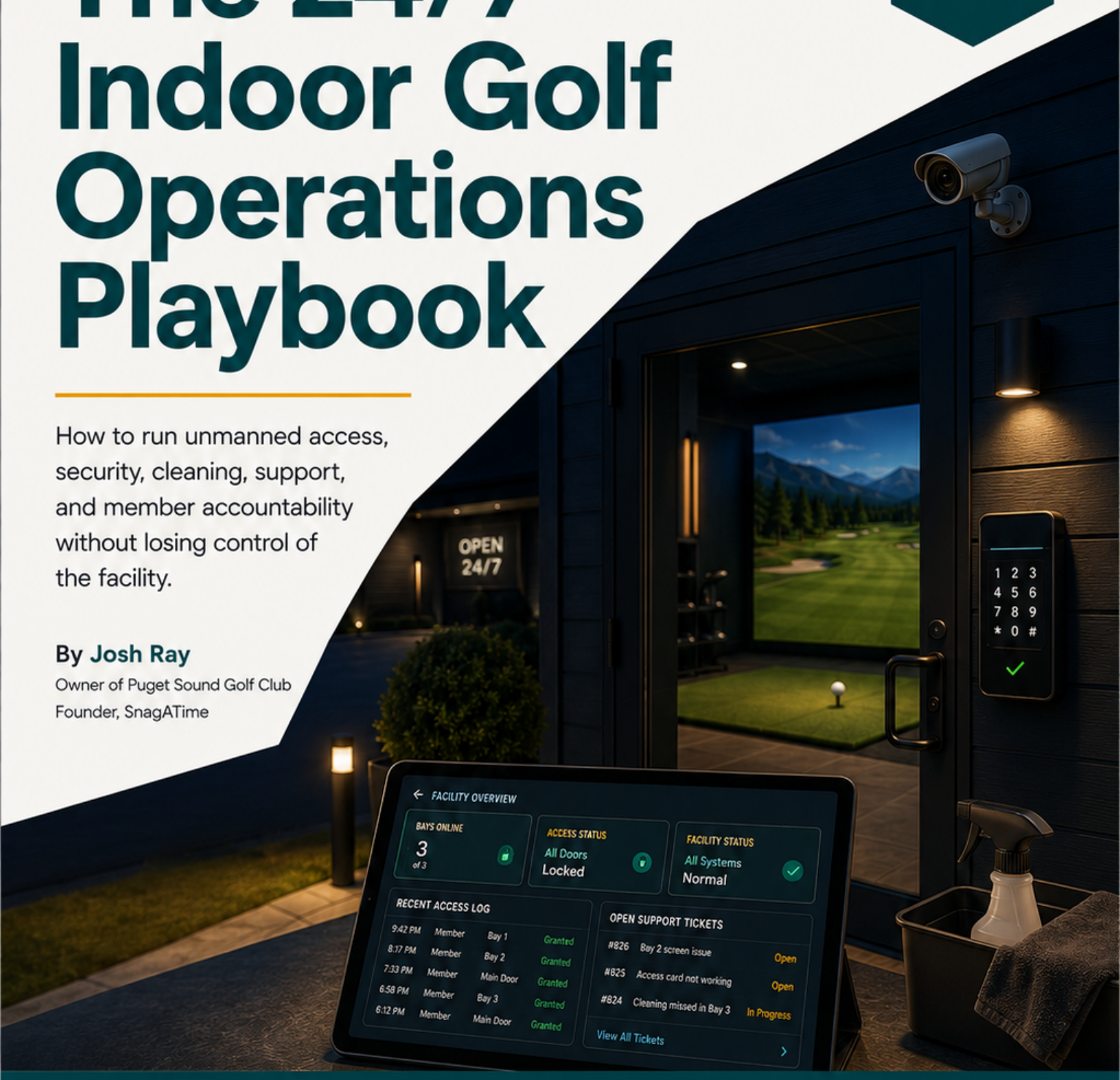
The 24/7 Indoor Golf Operations Playbook

How to run unmanned access, security, cleaning, support, and member accountability without losing control of the facility.

By Josh Ray

Owner of Puget Sound Golf Club

Founder, SnagATime



CONTROL ACCESS

MONITOR SECURITY

HANDLE SUPPORT

KEEP IT CLEAN

Foreword: 24/7 is not a door code

The most dangerous version of a 24/7 indoor golf facility is the one that thinks access control is the whole model.

Customer books. Customer pays. A code is sent. The door opens. Customer plays.

That is the happy path.

The real 24/7 operation is everything around it:

- payment before access
- waiver before access
- customer identity
- reservation-specific or customer-specific entry
- access logs
- camera coverage
- insurance approval
- simulator startup and reset
- door failure
- no-shows and late cancels
- guest control
- cleaning
- damage
- theft
- remote support
- incident follow-up
- weekly review

Unmanned does not mean unmanaged.

It means the work shifts from the front desk to the operating system.

This guide is for operators who want the benefits of extended access without losing control of the facility. It is not a promise that every facility should be 24/7. Some should not. But if you are going to offer unmanned, semi-automated, or extended-hours access, the lock is only one part of the decision.

The real question is whether the business can stay accountable when no staff member is standing in the room.

Executive summary: the eight 24/7 gates

Before offering unmanned or extended-hours access, operators should clear eight gates.

1. Insurance alignment

Ask the insurer directly whether unmanned operation is covered.

Confirm whether shared codes are allowed, whether cameras are required, whether waivers are required, whether alcohol or food changes the answer, and whether 24/7 public access is treated differently from member-only access.

At minimum, the broker conversation should touch general liability, property and equipment coverage, business interruption, workers' compensation if staff or contractors are involved, cyber/payment exposure if relevant (POS systems, stored customer data, recurring billing tokens), and liquor liability if alcohol is present. For the broader insurance checklist, see the Indoor Golf Startup Playbook, Chapter 9.

Operators should also treat 24/7 access as a carrier-narrowing factor. In the startup playbook, one risk-management operator described 24/7 operations as reducing the number of willing insurers by roughly 75% in that operator's market. Treat the exact percentage as anecdotal, but treat the direction as real: unmanned access usually makes underwriting harder, not easier.

Do not assume. Get the operating model reviewed before you sell it.

2. Traceable entry

A shared keypad code is operationally convenient but weak for accountability.

Better patterns include customer-specific credentials, reservation-bound access, and logs that tie entry to a customer account.

The operator should be able to answer: who entered, when they entered, why they were allowed in, and whether access expired when it should have.

3. Payment and waiver before entry

Access should not be granted until the reservation is paid and required waiver status is complete.

This matters for cash control, risk management, insurance conversations, and customer support. A facility that allows unpaid or unwaived entry is not automated. It is exposed.

4. Camera and incident workflow

Cameras are not just security theater.

They support incident review, insurance conversations, remote troubleshooting, customer accountability, and owner peace of mind.

The question is not only "do we have cameras?" It is "what happens when something happens?"

5. Bay reset plan

The bay must be usable without staff in the room.

That means startup, shutdown, simulator reset, launch-monitor reset, projector/display behavior, PC behavior, clear customer instructions, and a remote fallback when something breaks.

6. Support coverage

24/7 does not mean the owner never gets called.

It means the support workflow is explicit: what customers try first, when they contact support, who responds, when credits/refunds are issued, and what gets logged after the session.

7. Cleaning and maintenance rhythm

Unmanned hours still create wear.

Balls move. Tees break. Mats shift. Screens age. Customers spill things. Trash fills. Bathrooms need attention. Door hardware and cameras need review.

Cleaning and maintenance have to be part of the 24/7 model, not a chore squeezed around it.

8. Guest control

Guest access is not only a pricing question. It is an accountability question.

The facility should define who may bring guests, whether guests must be named, whether guests must sign waivers, whether guests can enter without the booking customer present, and who is responsible if something breaks.

Chapter 1: Decide which kind of extended-access model you are building

There are several versions of extended-access indoor golf.

They are not the same risk profile.

They are not the same software problem.

They are not the same insurance conversation.

Members-only 24/7

Members receive access privileges as part of a recurring membership.

This model works best when:

- customers are known
- usage is recurring
- rules are clear
- booking windows are disciplined
- no-show penalties are enforceable
- access logs tie to member accounts
- guests are controlled
- the facility has a clear incident process

Members-only access is often the cleanest place to start because the operator has a known customer base and recurring relationship.

The risk is complacency. A "known member" can still damage equipment, bring unauthorized guests, share credentials, or stay past a reservation. Membership does not replace accountability.

Public 24/7

Public 24/7 means a new customer can book and enter without staff.

This creates more revenue surface, but it also raises the operational bar. The facility must be more confident in identity, payment, waiver capture, camera coverage, instructions, support, and access expiration.

Public 24/7 can work, but it is rarely the safest first version.

If the operator cannot confidently support a first-time customer at 10:30 p.m., public 24/7 is not ready.

Hybrid extended hours

Hybrid extended hours means the facility is staffed during some windows and unmanned during others.

Common patterns:

- staffed public hours, member-only late-night access
- staffed evenings/weekends, automated off-peak access
- instructor or event blocks staffed, practice hours unmanned
- trusted-member 24/7 access before broader rollout

This is often the practical middle ground. It lets the operator learn where customers get confused before expanding access.

Semi-automated staffed model

Semi-automated staffed facilities may not offer true 24/7 access, but they automate booking, payment, waivers, bay assignment, reminders, and check-in.

This can be a strong first step.

It reduces front-desk burden and reveals which workflows are ready for unmanned access later.

The lesson: do not treat "24/7" as one switch. Treat it as a phased rollout.

Alcohol is usually a separate stop sign

Alcohol deserves its own decision before any unmanned access launch.

Most operators should assume unmanned alcohol service is not insurable until a broker says otherwise in writing. Many carriers will not cover it at all, and many will also scrutinize or exclude unmanned BYOB because the operator still controls the premises even if the facility is not selling the alcohol. Liquor liability, dram-shop exposure, underage drinking, intoxicated driving, and injury/property-damage claims can change the entire risk profile.

If alcohol is central to the business model, keep it in staffed hours unless counsel, the landlord, licensing authorities, and the insurance broker have reviewed the exact workflow.

Chapter 2: The access-control workflow

Access control should answer five questions:

1. Who entered?
2. When did they enter?
3. Were they allowed to enter?
4. Was entry tied to a reservation or membership?
5. Can access be revoked?

The weakest model is a shared code that rarely changes.

Shared codes are tempting because they are simple. But they create real problems:

- code sharing
- former members retaining access
- guests entering without identity
- unclear incident responsibility
- weak reservation-level audit trail
- weaker insurance posture
- no clean way to revoke one person without changing the code for everyone

The stronger model is reservation-specific or customer-specific access.

The exact hardware matters less than the workflow:

1. Customer books.
2. Customer pays.
3. Customer signs waiver.
4. Customer receives access instructions.
5. Credential activates near reservation time.
6. Credential expires after the reservation window.
7. Entry is logged.
8. Failed access has a support path.

The operator should know whether access is tied to the person, the reservation, the membership, or the door itself.

Those are different controls.

For example, a member credential that works every day from 5 a.m. to midnight is very different from a reservation credential that activates 15 minutes before a booking and expires 15 minutes after. Many facilities that market extended member access still cap the usable window at 19-21 hours for cleaning, maintenance, or risk control.

Neither is automatically wrong. But the operator should choose deliberately.

Access-control questions to answer before launch

- Can one customer share access with another?
- Can access be revoked instantly?
- Does access expire automatically?
- Are access logs easy to review?
- Can the operator see failed access attempts?
- What happens if the lock loses power or internet?
- What is the manual fallback?
- Is there battery backup?
- Is there cellular failover or another internet fallback?
- Is there a manual key override or emergency-entry process?
- Does emergency egress remain code-compliant if the access system fails?
- Does the landlord approve the hardware?
- Does the insurer approve the workflow?
- Who maintains the lock and door hardware?

If the access system cannot answer these questions, it is not ready to carry the operating model.

Chapter 3: Payment, waivers, and identity

The safest access flow is simple:

No payment, no waiver, no access.

That rule sounds obvious until the operator starts handling edge cases.

What if a member's card fails but the booking is already on the calendar? What if a customer books for three guests? What if someone signs a waiver once and then brings a different person later? What if a corporate event organizer books under one account? What if a guest is injured but never created an account?

These are not abstract problems. They are the normal messiness of running a customer facility.

A waiver is useful only if it is tied to the right person at the right time.

For 24/7, waiver workflow should:

- happen before access
- attach to the customer account
- capture timestamp and version
- support renewal when terms change
- cover guests if guests are allowed
- block booking or access when incomplete
- preserve a record the operator can retrieve later

Identity matters because the facility needs to know who is in the space.

If one member books and four unknown guests enter, the operator should know whether that is allowed, how guests are covered, and who is responsible if something breaks.

Guest policy is part of risk control

Many operators think of guests as a pricing issue.

They are also an accountability issue.

A strong guest policy should define:

- whether guests are allowed
- whether guests must be named
- whether guests must sign waivers
- whether guests count against membership privileges
- whether the booking customer is responsible for guest conduct
- whether guests can enter without the member present
- what happens if guest rules are violated

If the policy is not enforceable, it is not really a policy.

Chapter 4: Cameras, monitoring, and privacy expectations

Cameras should cover the areas where accountability matters.

Common coverage zones:

- entrance
- lobby/common area
- bay areas
- simulator equipment
- storage or restricted areas
- hallways
- door/access hardware
- point-of-sale or beverage areas if relevant
- parking lot or exterior approach if appropriate and allowed

Avoid blind spots where the most expensive equipment lives.

Cameras are only useful if the operator knows:

- how long footage is retained
- who can access footage
- how incidents are reviewed
- how footage is exported
- whether footage supports insurance needs
- how privacy expectations are communicated
- whether local rules affect video placement and audio capture

For many small facilities, 30-90 days is a common video-retention planning range, but the right answer depends on storage, camera count, incident risk, insurer requirements, and local rules. If an incident is reported, preserve the

relevant clip instead of letting normal retention overwrite it.

Audio requires extra caution. Most commercial systems disable audio capture by default because recording conversations without consent is illegal in many states and legally sensitive almost everywhere. Consult counsel before enabling audio, especially in all-party consent states, sometimes called two-party consent states.

The goal is not to make customers feel watched.

The goal is to run an accountable facility without staff present every hour.

That requires a balance. Customers should know cameras are present, but the facility should not feel hostile. Signage, house rules, and onboarding copy should make the purpose clear: safety, facility protection, and support.

Monitoring is not the same as staring at cameras

Most small operators are not watching live footage all day.

The practical workflow is event-based:

- access alert
- support message
- equipment issue
- damage report
- cleaning concern
- unauthorized-entry suspicion
- incident review

The operator needs a way to quickly find the right time window, review the relevant camera angle, document what happened, and decide what policy or process needs to change.

Camera footage is not the operating system. It is evidence for the operating system.

Chapter 5: Bay automation and reset

The bay has to work when the customer arrives.

This is where many 24/7 models become harder than expected.

Booking the room is easy. Making the simulator reliable without staff is the real work.

Operators should document:

- what should be powered on
- what should be powered off
- where the simulator software starts
- how a customer selects a course or range
- how to reset a frozen app
- how to reconnect a launch monitor
- how to handle projector/display issues
- what customers should not touch
- how to restart the PC if needed
- when to contact support

Every automated system needs a fallback.

If the PC is asleep, what happens?

If the projector does not wake, what happens?

If the launch monitor disconnects, what happens?

If the customer exits the simulator software, what happens?

If the previous customer leaves the software in a strange state, what happens?

Write the answers before opening.

The bay reset ladder

A useful bay reset ladder has four levels.

Level 1: Customer self-help

The customer can follow a short instruction card or on-screen note. This should handle common issues such as selecting the right bay, starting a range session, finding the mouse/keyboard, or following basic restart steps.

Level 2: Remote operator action

The operator can remote into the PC, restart software, power-cycle a device, unlock the door, or message the customer with specific instructions.

Level 3: Credit/reschedule

If the session cannot be saved quickly, the operator has a clear credit or refund policy.

Level 4: Physical repair

If equipment needs on-site service, the bay is removed from inventory until fixed.

The mistake is treating every issue like Level 4. That burns the owner out.

The other mistake is pretending Level 4 never happens. It does.

Chapter 6: House rules that customers actually follow

Unmanned operations need rules customers can understand quickly.

Rules should cover:

- reservation start/end behavior
- early entry
- overstaying
- guest limits
- food and drink
- alcohol, if allowed
- club and ball use
- cleanup expectations
- damage reporting
- camera disclosure
- emergency procedure
- support contact
- no-show and late-cancel policy
- penalties for misuse

Good rules are short, visible, and repeated in the right places:

- booking page
- booking confirmation
- reminder email/text
- waiver flow
- door instructions
- bay signage
- post-session message

Do not rely on one long rules page that nobody reads.

The best rule systems are layered. Customers get the right instruction at the moment they need it.

Rules should be enforceable

Avoid rules that sound good but cannot be enforced.

Weak rule:

"Please be respectful."

Better rule:

"Your reservation ends at the scheduled time. Please leave the bay clean and exit within 10 minutes so the next group can start on time. Repeated overstays may result in loss of booking privileges."

The second rule gives the customer a behavior, a reason, and a consequence.

That is what an unmanned facility needs.

Chapter 7: Cleaning and maintenance rhythm

Cleaning is one of the easiest places to underplan.

The facility needs a rhythm for:

- trash
- bathrooms
- balls
- tees
- mats
- screens
- clubs, if provided
- seating
- spills
- HVAC comfort
- door/access hardware
- cameras
- PCs and peripherals
- signage
- lost and found

The more hours the facility is open, the more intentional the cleaning loop has to be.

If the operator wants to avoid staff, cleaning still has to happen. It may be owner-performed, contractor-performed, or staff-performed, but it is not optional.

Daily, weekly, monthly

Create a maintenance cadence before the facility gets busy.

Daily checks

- trash
- bathrooms
- loose balls
- broken tees
- mat movement
- obvious spills
- door/access function
- bay readiness
- support-ticket follow-up

Weekly checks

- screen wear
- mat wear
- cable condition
- projector/display alignment
- PC updates/restarts
- camera coverage
- supply inventory
- signage condition
- recurring customer complaints

Monthly checks

- access-log review
- incident trend review
- insurance or compliance reminders
- guest-policy review
- membership misuse review
- replacement-part planning
- deep clean
- preventive maintenance

The point is not to create paperwork. The point is to prevent small misses from becoming customer churn.

Chapter 8: Support process

A support process should define:

- customer self-help steps

- support channel
- response expectations
- emergency escalation
- refund/credit rules
- incident documentation
- follow-up timing
- equipment repair ownership

Customers are more forgiving when they know what to do.

The worst support experience is silence. The second worst is confusion.

For unmanned facilities, support copy is part of the product.

Set support expectations honestly

If the operator cannot respond instantly at 1 a.m., do not imply 1 a.m. live support exists.

Instead, define what customers can expect:

- emergency instructions
- common self-help fixes
- how to report an issue
- when the operator responds
- how credits are handled
- what issues qualify for refund or reschedule

The support promise should match the operating reality.

Overpromising support creates frustration. Underexplaining support creates panic.

The goal is calm clarity.

Chapter 9: Incident categories

Not every problem needs the same response.

Group incidents by severity before launch.

Low severity

Examples:

- customer confusion
- missing tees
- projector remote misplaced
- simulator software on the wrong screen
- minor booking question
- small cleanup miss

Response:

- self-help instructions
- follow-up message

- small credit only when appropriate
- update instructions if the issue repeats

Medium severity

Examples:

- bay not playable
- door access failure
- launch monitor disconnect
- projector failure
- customer cannot complete session
- repeated no-show or overstay
- guest-policy issue

Response:

- remote support
- credit/refund decision
- maintenance ticket
- incident log
- customer follow-up
- rule or automation review

High severity

Examples:

- injury
- theft
- property damage
- unauthorized entry
- alcohol incident
- emergency services
- suspected policy violation with safety implications

Response:

- emergency process
- owner/operator notification
- camera review
- insurance documentation
- customer follow-up
- policy review
- access restriction if appropriate

The goal is to avoid inventing the response while the problem is happening.

When the categories are clear, the operator can respond faster and more consistently.

Chapter 10: Roll out 24/7 in phases

Operators do not have to launch full public 24/7 access immediately.

A safer rollout:

1. **Staffed public hours only.**
2. **Automated booking and payment during staffed hours.**
3. **Member-only extended access.**
4. **Trusted-member 24/7 access.**
5. **Public extended access if insurance, support, and operations are ready.**

Trusted-member access typically means established members with at least 60-90 days of tenure or multiple billing cycles, no incident history, a verified waiver, a working payment method, and a clear understanding that access can be revoked if rules are violated.

Each phase should have a review point:

- support tickets
- door/access failures
- no-shows
- damage incidents
- cleaning issues
- refund/credit volume
- customer confusion
- owner intervention time
- guest-policy violations
- insurer or landlord concerns

If a phase creates too much manual work, fix the system before expanding access.

Do not confuse revenue potential with readiness

Opening more hours creates more sellable inventory.

But the question is not only whether customers will book it.

The question is whether the facility can support it without damaging the experience, increasing risk, or consuming the owner's life.

Extended access should earn its way into the model.

If late-night bookings are rare, high-support, and low-margin, the operator may be better off with member-only access or shorter extended hours.

If early-morning members are reliable, low-support, and loyal, that access may be worth protecting.

Use actual usage data, not only the idea of 24/7.

Chapter 11: Documentation customers actually use

Documentation should be short, visual, and placed where the customer needs it.

Create:

- booking confirmation instructions

- arrival instructions
- door/access instructions
- bay startup card
- simulator reset card
- house rules
- emergency instructions
- support contact
- checkout/cleanup checklist

Avoid long manuals.

Customers at 10 p.m. need fast answers:

- How do I get in?
- Which bay am I in?
- How do I start?
- What if it freezes?
- What do I do when I leave?

If the instructions cannot be followed by a first-time customer under mild stress, simplify them.

The best documentation is redundant

The same critical instruction should appear in more than one place.

For example, access instructions may belong in:

- confirmation email
- reminder text
- member portal
- door signage
- support page

Bay reset instructions may belong:

- near the keyboard
- on a laminated card
- in a short video
- in the support message template

Redundancy is not clutter if it prevents support calls.

Chapter 12: What not to automate too early

Automation is powerful, but premature automation can create brittle systems.

Do not over-automate:

- rare edge cases
- complex food/beverage flows
- exceptions that need judgment

- hardware that fails unpredictably
- customer education that signage can solve
- policies that are still changing

Start with the high-frequency, high-value flows:

- booking
- payment
- waiver
- access
- reminders
- cancellation/no-show rules
- basic reset instructions

Then add deeper automation after real usage exposes the patterns.

Manual first, then automate

If an operator cannot describe the workflow manually, automation will not fix it.

For example:

- How should a no-show be handled?
- When should a customer get a credit?
- Who can bring guests?
- What happens if a member overstays?
- When should access be revoked?
- Which issues require camera review?

Answer those questions first.

Then automate the repeatable parts.

Chapter 13: The 24/7 readiness scorecard

Before enabling unmanned access, score each category from 1 to 5.

The scorecard maps onto the eight executive-summary gates, with two gates split into finer-grained categories: Gate 3 becomes Payment and Waivers, and Gate 4 becomes Cameras and Incident process.

Use 2 and 4 as between-rung scores.

Category	1 - Not ready	3 - Partially ready	5 - Ready
Insurance	not reviewed	broker conversation started	model reviewed and documented
Access control	shared code only	customer credentials but limited audit	reservation/customer-specific access with logs
Payment	payment can lag access	most bookings prepaid	payment required before access
Waivers	manual or inconsistent	digital waiver exists	waiver blocks booking/access if missing
Cameras	partial coverage	key areas covered	critical areas covered with review workflow
Bay reset	owner intervention common	some self-help steps	documented self-help and remote fallback

Category	1 - Not ready	3 - Partially ready	5 - Ready
Support	ad hoc texts/calls	support channel exists	clear support flow and credit policy
Cleaning	informal	assigned but reactive	daily/weekly/monthly rhythm
Guest control	unclear	policy exists	policy is enforced and tied to booking
Incident process	improvised	categories exist	documented response by severity

If any category is a 1, pause.

If the average is below 3, do not expand access yet.

If the scores are mostly 4s and 5s, the facility may be ready for a controlled rollout.

The scorecard is not bureaucracy. It is a way to see whether the operating model has caught up with the access model.

Chapter 14: Launch checklist

Before enabling 24/7 access, verify:

- insurer has reviewed the operating model
- landlord allows after-hours customer access
- access logs are working
- waivers block access when incomplete
- payment is required before access
- cameras cover critical areas
- footage review workflow is defined
- support number/channel is tested
- simulator reset flow is tested
- remote support access is working
- emergency instructions are posted
- cleaning schedule is assigned
- incident process is documented
- no-show/cancellation rules are enforced
- guest policy is written and enforceable
- customer instructions are clear on mobile
- door failure fallback exists
- refund/credit policy is written
- weekly review process is scheduled

If any item is fuzzy, do not call the facility hands-off yet.

The launch checklist should be reviewed again after the first 30 days of extended access.

Chapter 15: Weekly operator review

Unmanned facilities need a weekly operating rhythm.

Review:

- access failures
- support messages
- refunds and credits
- no-shows
- late cancels
- camera incidents
- damage reports
- cleaning misses
- simulator resets
- member complaints
- public first-time-customer confusion
- guest-policy issues
- overstays
- door or lock issues

Then decide:

- what instruction needs to improve
- what rule needs to change
- what automation needs a fallback
- what maintenance needs scheduling
- what customer segment needs more education
- what access privileges should change
- what should be removed from self-service

This is how 24/7 stays managed even when staff are not in the room.

The weekly review also protects the owner from drift.

Small issues compound when no one reviews them. A broken instruction creates support calls. Support calls create credits. Credits hide lost revenue. Lost revenue hides a workflow problem.

The weekly review catches the pattern before the customer experience degrades.

Chapter 16: The 24/7 operating worksheet

Use this worksheet before expanding access.

Access model

- Staffed hours:
- Unmanned hours:
- Member-only access windows:
- Public access windows:
- Trusted-member pilot group:
- Guest policy:
- Alcohol/food policy:

Insurance and permissions

- Broker reviewed model?
- Landlord approved after-hours access?
- Cameras required?
- Waivers required?
- Shared codes allowed?
- Alcohol changes coverage?
- Written notes stored?

Access workflow

- Payment required before access?
- Waiver required before access?
- Customer-specific credential?
- Reservation-specific credential?
- Access expiration window:
- Failed-access alert:
- Manual fallback:

Facility control

- Entrance cameras:
- Bay cameras:
- Equipment-zone cameras:
- Footage retention:
- Footage review owner:
- Door hardware maintenance owner:

Bay readiness

- Startup instructions:
- Reset instructions:
- Remote PC access:
- Projector/display fallback:
- Launch-monitor fallback:
- Bay out-of-service process:

Support

- Support channel:
- Emergency instructions:
- Response expectation:
- Credit/refund rule:
- Incident log location:
- Customer follow-up owner:

Cleaning and maintenance

- Daily cleaning owner:
- Weekly maintenance owner:
- Monthly review owner:
- Supplies checked:
- Screen/mat review:
- Camera/access review:

Go/no-go

- Any readiness category scored 1?
- Average score below 3?
- First rollout phase:
- Review date:
- Stop/rollback trigger:

Closing: unmanned is still operated

The best 24/7 facilities are not unmanaged.

They are carefully managed through systems.

The customer may not see staff. But the business still needs rules, support, monitoring, cleaning, insurance alignment, and a calendar that protects the model.

If you want 24/7 to work, do not start with the lock.

Start with the operating system.

Source Notes

- The Indoor Golf Startup Playbook: /resources/2026-indoor-golf-startup-playbook/
- The Indoor Golf ROI & Capacity Playbook: /resources/2026-indoor-golf-roi-capacity-playbook/
- SnagATime operator experience with automated booking, access, memberships, bay control, cleaning, and support workflows.
- Justia 50-state recording-laws survey for audio-recording consent context: https://www.justia.com/documents/50-state-surveys-recording-calls-and-conversations.pdf
- Seneca Security, security-camera retention overview and 30-90 day retention planning range: https://senecasecurity.com/learn/how-long-do-security-camera-recordings-last/
- Eventure Insurance, liquor-liability requirement overview for alcohol-service and BYOB insurance context: https://www.eventureinsurance.com/articles/liquor-liability-requirements
- NFPA 101 Life Safety Code free-access page for means-of-egress and access-control context: https://link.nfpa.org/all-publications/101/2018
- Insurance-specific sections are operational education only and should be reviewed with a qualified broker before publication.