VIVO CONTROL

SECURITY · 14 PAGES

Building Access Control and Liability — What Property Managers Need to Know

A non-legal guide to how access control audit trails affect liability exposure, insurance requirements, and incident documentation for residential and commercial properties.

14 pages · 12 min read · PDF

INTRODUCTION

Why Access Control and Liability Are Connected

Property managers usually think about access control as a security and convenience question. Insurers, attorneys, and courts tend to think about it differently: as documentation. When something goes wrong on a property — an assault, a theft, an unauthorized entry — the question that follows is rarely just "what happened." It's "what can you prove happened, and what did the property do to prevent it."

This guide is a plain-language introduction to how access control intersects with liability exposure and insurance — written for property managers and board members, not lawyers. It explains the general concepts you're likely to encounter, not how any specific law applies to your specific property. That distinction matters throughout this guide, and we'll repeat it where it counts.

> **THIS IS NOT LEGAL ADVICE**
>
> Premises liability and negligent security law vary significantly by jurisdiction, and how these concepts apply to your property depends on facts a general guide can't capture. Use this guide to understand the landscape and to have a more informed conversation with your insurance broker and legal counsel — not as a substitute for either.

Premises Liability and Negligent Security — General Concepts

Most jurisdictions recognize some version of "premises liability" — the general principle that a property owner or manager owes visitors, residents, and tenants a duty of reasonable care to keep the property reasonably safe. A specific category within this area, often called "negligent security," deals with claims that inadequate security measures contributed to a criminal act against someone on the property.

While the exact legal test varies by jurisdiction, claims in this area generally require some version of the following elements:

- **Duty** — that the property owed the injured person some duty of care, which is typically established simply by their lawful presence on the property.
- **Breach** — that the property failed to meet a reasonable standard of care, often argued by comparing the property's actual security measures to what a similar property would reasonably provide.
- **Causation** — that the breach was a substantial factor in the harm that occurred, which often turns on whether the specific type of incident was foreseeable.
- **Damages** — that the person suffered an actual, provable harm as a result.

Foreseeability is often the most contested element in these cases, and it's frequently where a property's own history — prior incidents, complaints, or known vulnerabilities — becomes directly relevant.

How "Reasonable Security" Is Generally Evaluated

Courts and insurers generally don't expect a property to be impenetrable — the standard is typically "reasonable," not "perfect." A few factors commonly come up in how that reasonableness gets assessed, in general terms:

- **Industry and area norms.** What security measures are typical for similar properties in a similar area is often a reference point, though not a guarantee of adequacy on its own.
- **Prior incidents at the property.** A documented history of similar incidents tends to strengthen an argument that a particular risk was foreseeable — and that the property should have responded to it.
- **Feasibility and cost of additional measures.** Whether a reasonable, cost-effective improvement existed and wasn't implemented is often part of the analysis.
- **Whether existing measures actually functioned as intended.** A broken gate, a non-functional camera, or an access control system with no usable log can undercut a property's argument that it had reasonable security in place — even if the equipment was purchased in good faith.

This is general background, not a checklist for compliance — the weight given to each factor varies significantly by jurisdiction and by the specific facts of a case.

The Role of the Audit Trail

This is the central idea of this guide: in most disputes involving property access, the audit trail — the record of who entered, when, and how — tends to matter more than the underlying incident itself. Two properties can experience an identical bad event and end up in very different positions depending entirely on what they can document afterward.

A property that can produce a clear, timestamped record of every entry during the relevant window is in a fundamentally different position than one that can only offer a guard's recollection or a gap in a paper log. The record doesn't just support a property's version of events — in many cases, it's the only reliable way to establish what actually happened at all.

> **WHY THIS MATTERS EVEN WITHOUT AN INCIDENT**
>
> Insurers and legal counsel generally view a property's ability to produce this kind of record as a proxy for how seriously the property takes security overall — independent of any specific event. This is one reason access control audit trails come up in insurance underwriting conversations even for properties with no incident history.

What a Strong Audit Trail Includes

- **Timestamped entry and exit records** at every access point, not just the main entrance — gaps at secondary gates are a common weakness.
- **Credential issuance and revocation history** — a clear record of when a resident's access was granted and, importantly, when it was terminated (at move-out, for example).
- **Video or photo verification tied to specific entry events,** where the platform supports it, which corroborates the access log rather than standing alone.
- **Guest and visitor access records,** including who issued a temporary credential and its valid time window.
- **System status logs,** showing whether the access control system itself was functioning normally during the relevant period — this matters directly if a claim involves an equipment failure.
- **Export capability,** since a record that exists but can't be produced in a usable format when needed provides limited practical value.

What a Weak or Missing Audit Trail Costs You

- **Inability to establish who had access** during a relevant window, which can leave a property unable to support its own account of events.
- **Difficulty demonstrating that reasonable security measures were actually in place and functioning,** as opposed to simply purchased at some point in the past.
- **Weakened position in insurance claims,** since insurers generally expect documentation to support a claim narrative, not just a description of what allegedly happened.
- **In some jurisdictions and circumstances, an adverse inference risk** — where a party's failure to preserve or produce evidence it should reasonably have had can be viewed unfavorably. Whether and how this applies is a legal question specific to your situation, not a general rule this guide can state definitively.
- **Reduced credibility in the broader reasonableness analysis** from page 4 — a property that can't produce basic access records has a harder time arguing its overall security posture was adequate.

None of this means a property without perfect records is automatically liable, or that a property with excellent records is automatically protected — but the difference in position is significant enough that closing this gap is generally worth the investment.

Insurance Implications

- **Underwriting conversations increasingly ask about access control specifics,** not just "do you have a security system" — insurers may ask about credential management, audit trail capability, and monitoring.
- **Some policies or endorsements may require specific documentation practices** as a condition of coverage for certain claim types — confirm this directly with your broker rather than assuming your current system satisfies policy requirements.
- **Claims involving access-related incidents typically require supporting documentation** from the property, and the completeness of that documentation can affect how smoothly a claim is processed.
- **Premium impact varies by carrier and market,** but demonstrable, well-documented security measures are commonly cited by brokers as a relevant factor in underwriting discussions — ask your specific broker how this applies to your policy.
- **Additional insured and certificate requirements** for vendors, including your access control provider, should be confirmed as part of any new installation contract (see our RFP Template, Section 11 for HOA-specific contract terms).

Incident Documentation Best Practices

1. **Preserve the access log immediately.** Export or otherwise secure the relevant time window's access records as soon as an incident is reported, before any routine data cycling or retention policy could affect it.
2. **Document the incident factually and promptly,** separate from any access log — who reported it, when, and what was observed, without speculation about cause or fault.
3. **Notify your insurance broker and legal counsel early,** rather than waiting until a formal claim or demand arrives — early guidance can affect what you should and shouldn't do next.
4. **Avoid altering or "cleaning up" any system logs or footage** related to the incident, even with good intentions — preserve records exactly as they exist.
5. **Keep a written record of your response,** including any corrective action taken, since a documented, prompt response is generally viewed more favorably than an undocumented one.

How Long to Keep What

Record Type	General Guidance
Standard access logs (no known incident)	Follow your platform's default retention, commonly 6–12 months, unless your insurer or counsel advises longer
Video footage tied to entry events	Often shorter than access logs due to storage cost — confirm your platform's specific retention window
Records related to a known incident or claim	Preserve indefinitely until legal counsel confirms it's no longer needed
Credential issuance/revocation history	Retain for the duration of residency plus a reasonable buffer, per your counsel's guidance
Contract and vendor documentation	Retain for the life of the contract plus applicable statute of limitations periods in your jurisdiction

Retention periods involve legal considerations (statutes of limitations, litigation holds) that vary by jurisdiction and circumstance — treat this table as a starting point for a conversation with counsel, not a final policy.

PROPERTY TYPE DIFFERENCES

Residential vs. Commercial Property Differences

Factor	Residential (HOA / Multifamily)	Commercial
Who's typically owed a duty of care	Residents, guests, and invited visitors	Employees, customers, tenants, and their visitors
Common claim types	Unauthorized entry, assault, theft in common areas	Workplace violence exposure, theft, tenant disputes over shared access
Typical decision-maker for security investment	HOA board or property management company	Building owner, property manager, or tenant (depending on lease terms)
Insurance structure	Often a master policy through the association	Frequently split between owner and tenant policies, with lease terms defining responsibility

Commercial leases in particular often allocate security responsibility contractually between landlord and tenant — confirm which party's insurance and legal exposure applies to access control specifically, since this is often less clear-cut than it appears.

Working With Your Insurance Broker and Legal Counsel

Everything in this guide is general background. Getting guidance specific to your property means bringing the right questions to the right professional.

Questions for Your Insurance Broker

- [x] Does our current policy have specific documentation requirements tied to access-related claims?
- [x] Does our access control system's audit trail capability affect our premium or coverage terms?
- [x] What certificate of insurance requirements should we impose on our access control vendor?

Questions for Legal Counsel

- [x] What does premises liability and negligent security law look like specifically in our jurisdiction?
- [x] What record retention periods should we follow given our specific risk profile and jurisdiction?
- [x] What should our incident response and documentation protocol look like, in writing?

BRING THIS TO YOUR NEXT REVIEW

Documentation Checklist and Key Takeaways

- [x] Confirmed our access control platform produces a timestamped, exportable log at every entry point, not just the main entrance
- [x] Confirmed credential issuance and revocation history is tracked, including at move-out
- [x] Reviewed our record retention practices with legal counsel, specific to our jurisdiction
- [x] Confirmed with our insurance broker whether our documentation practices satisfy policy requirements
- [x] Documented a written incident response protocol, including immediate log preservation steps
- [x] Confirmed additional insured / certificate of insurance requirements are in place for our access control vendor
- [x] Tested that our system's export function actually works, before we need it during an incident

The core idea to carry forward: the audit trail your access control system produces is not just an operational convenience — it's frequently the single most important piece of evidence in how a liability question gets resolved. Investing in a system that reliably produces one is a risk-management decision, not just a technology decision.

VIVO CONTROL

A Complete, Exportable Audit Trail — By Default

Vivo Control logs every entry, credential change, and system event automatically, with export tools built for exactly the documentation needs covered in this guide.

Book a Free Demo →

---

www.vivocontrol.com/en/demo/ · hello@vivocontrol.com ·