

Security Starts With Boundaries.

ThinkHOA security is not only about passwords and login screens. It is about protecting **association-specific governance intelligence** so each HOA's records, history, precedent, and decision context stay separated, traceable, and trustworthy.

What ThinkHOA is protecting

- Governing documents, amendments, rules, policies, and resolutions
- Meeting minutes, prior board actions, and association precedent
- Open matters, governance questions, and decision history
- Controlled legal and regulatory authority with source provenance

Core principle

A private HOA's governance history should never be blended into another HOA's workspace. Security begins with the integrity of the association boundary.

SECURITY ARCHITECTURE

Protect the workspace. Preserve the reasoning.

ThinkHOA security combines access control, data scoping, provenance, and governance transparency. The objective is not just defense—it is trustworthy decision-making.

A

Association-level data separation

Each HOA has its own documents, matters, history, and governance context.

U

Controlled user access

Access can be restricted by account, user, association, and role.

P

No cross-association private precedent

Association A's private board history should not appear in Association B.

L

Controlled legal intelligence

Applicable law can be maintained separately from private HOA records.

S

Source provenance

Important sources can retain source, jurisdiction, effective date, and version.

H

Preserved history

Prior documents and decisions remain available for audit and historical reference.

T

Traceable conclusions

Users should be able to see why a governance conclusion was reached.

Q

Human oversight

Questionable classification or hierarchy issues can be reviewed rather than guessed.

BOUNDARY

Keep each HOA in its own lane

Security begins by maintaining a clean boundary around the association workspace.

1 Separate workspace

Each HOA has its own document set, decision history, and matter context.

2 Scoped intelligence

Association-specific memory should remain tied to the correct HOA.

PROTECTION

Who can see what

Protection is about controlling visibility and limiting the spread of private governance information.

1 Role-based access

The right people see the right association information—and only that information.

2 Controlled authority

Public legal authority can be maintained separately from private association records.

BEYOND

Trust requires more than login security

A governance AI system should make important reasoning visible and reviewable.

1 Traceable answers

The source of a conclusion should be visible rather than hidden inside a response.

2 Preserved history

Past versions, prior decisions, and unresolved issues should remain available for context.

Security must answer four questions

1

WHO IS
ALLOWED
TO SEE
THIS?

2

WHICH
ASSOCIATION
DOES IT
BELONG TO?

3

WHAT
SOURCE
PRODUCED
THE
CONCLUSION?

4

CAN
THE
USER
TRACE
IT
BACK?

ThinkHOA security promise

The source of an important governance conclusion should be visible rather than hidden inside an AI answer.

What “secure” means in practice

- **Boundaries:** keep data scoped to the correct association workspace.
- **Protection:** restrict access based on role and association context.
- **Integrity:** preserve provenance, versioning, and historical context.
- **Trust:** let users see why a recommendation can—or cannot—be trusted.

Context first. Then the answer.

Security in governance AI is not just defense. It is the foundation for transparent, defensible decision-making.