GREEKHOURS

Trust Pledge

What GreekHours does with a chapter's data, who can see it, and what happens if something goes wrong. Every statement verified against the live system.

Version 2.0 · Verified against production September 8, 2026 · For chapter officers, advisors, and national and campus stakeholders

The eight commitments

1. **Collect only what hour tracking needs, never sell it.**
2. **Location verifies a session, never tracks you.** Only during a session. Raw location deleted after 120 days. Never in a shared report.
3. **No passwords, ever.** Sign in with Apple, Google, or Microsoft.
4. **Encrypted in transit and at rest.** TLS 1.2+; database and backups encrypted on Microsoft Azure.
5. **Access scoped by role and by chapter.** Five chapter roles, each scoped to their area of responsibility. No chapter sees another's data.
6. **Your data is yours.** Share with names removed or as totals. Delete any time. Deletion requests acknowledged in 5 business days.
7. **AI stays in bounds.** Support assistant runs on Azure. Conversations deleted after 120 days. Content not used to train models.
8. **We monitor, respond, and tell you.** Security reports assessed within 1 business day. Chapter contacts notified within 72 hours of a confirmed incident.

Sharing compliance outside the chapter

> Read-only links in three levels: Full Detail, Anonymized Detail (no names, random per-report labels), or Summary Only (totals). Every level excludes location and financial detail. Links expire and can be revoked.

Enterprise application

GreekHours is a native iOS and Android app, a web admin portal, and API services running on an enterprise-grade Microsoft Azure environment with privacy and security controls built in: a **web application firewall**, **security alerting**, and **continuous monitoring** across the service, on top of encryption in transit and at rest.

What GreekHours is

An app that tracks study, service, and chapter hours for Greek organizations, verifies study sessions by location, and gives officers reports they can trust. This page is a summary; the full Trust Pledge adds the fact sheet, third-party list, retention schedule, and evidence list.

Common questions

What does it collect? Name, sign-in identity, chapter and role, hours, and location during a session.

Does it track location? Only during a study session. Never outside one.

Who can see the data? Officers in the chapter, within their role. No other chapter.

Can compliance be shared without exposing people? Yes, with names removed or as totals.

What if there is a security problem? Assessed within one business day; affected chapters told within 72 hours of confirmation.

How data is protected

No stored passwords; sign-in through Apple, Google, or Microsoft. HTTPS/TLS in transit. Database, photos, and backups encrypted at rest on Microsoft Azure. Access limited by role and scoped so one chapter cannot see another's data. Backups roll over every 7 days, so deleted data is gone within a week.

Access scoped by role and chapter

Five chapter roles control who sees what: Student (own hours), Study Admin, Service Admin, and Event Admin (their area of responsibility), and Chapter Admin (the whole chapter). Chapter data is scoped so one chapter can never reach another's.

Where to check

greekhours.com/privacy · greekhours.com/security · security@greekhours.com · and the full GreekHours Trust Pledge.

An operational trust summary for chapter decision support, not a legal contract. Campus-specific requirements route through the school. Does not replace legal review required by a university, national organization, or advisor.