campfire.

Certifications & Compliance

CERTIFIED

SOC 1 Type II – Certified & Current

Controls relevant to financial reporting. Type II means our controls were tested continuously over a full audit period, not just at a single point in time.

SOC 2 Type II – Certified & Current

Covers all five Trust Service Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy. Independently audited over time, not just a snapshot. Continuously verified.

UNDERWAY

ISO 27001 – Audit Year 1 Underway

The international standard for Information Security Management Systems. We have entered our first formal audit year and are on track for full certification by end of 2026.

ALIGNED

GDPR, CIS Controls & NIST CSF – Framework Aligned

Our security program is built in alignment with globally recognized frameworks—GDPR for data privacy, CIS Controls for prioritized security best practices, and NIST CSF for risk-based cybersecurity governance.

Your data is safe with Campfire.

We hold ourselves to the highest independent security standards. Not as a checkbox, but as a commitment to every customer who trusts us with their data.

AUDIT TYPE

Continuous — not point-in-time

VERIFICATION

Independent third-party auditors

REPORTS AVAILABLE

Upon request under NDA

Security Practices

MULTI-FACTOR AUTHENTICATION
Enforced across all systems and privileged access points

LEAST-PRIVILEGE ACCESS
With quarterly reviews and prompt deprovisioning on departure

ENCRYPTION AT REST & IN TRANSIT
AES-256 and TLS 1.2+ for all sensitive data

FORMAL RISK ASSESSMENT
Program with a maintained risk register and documented treatment plans

VENDOR & THIRD-PARTY RISK MANAGEMENT
With due diligence for all critical suppliers

DOCUMENTED INCIDENT RESPONSE PLAN
With tested procedures and defined escalation paths

BUSINESS CONTINUITY & DISASTER RECOVERY PLANS
Tested at least annually

CONTINUOUS MONITORING & LOGGING
Of systems, user activity, and security events

ANNUAL SECURITY AWARENESS TRAINING
For all staff, with phishing simulations

FORMAL CHANGE MANAGEMENT
With peer review and documented approval workflows

VULNERABILITY MANAGEMENT & PATCHING
With SLAs defined by severity classification

DATA CLASSIFICATION & RETENTION POLICIES
Governing handling of all customer data

ENDPOINT PROTECTION & MDM
Deployed across all corporate devices