EquipCheck
Security & Privacy Overview
Version 1.0 — 11 May 2025

1 | Company Profile

Item	Detail
Legal Entity	**EquipCheck Inc.**
Headquarters	United States — fully-remote organization
Primary Product	Cloud-based inventory-tracking platform for professional and NCAA Division I athletic teams
Contact (Security & Privacy)	**support@equipchecksoftware.com**

2 | Governance & Written Policies

EquipCheck operates a documented **Information-Security Management System (ISMS)**. All policies live in a private Git repository; revisions require executive sign-off and are reviewed on a fixed cadence.

Policy / Standard	Scope	Review Cadence
Information-Security Policy	High-level principles & roles	Annual
Data-Classification & Handling Standard	Storage, transmission, destruction rules	Annual
Access-Control / Least-Privilege Standard	Provisioning, MFA, quarterly role review	Quarterly
Secure-Development Guidelines	Code review, dependency management	Release-based
Change-Management Standard	PR workflow, impact tiers, rollback steps	Annual
Incident-Response Plan (IRP)	Detect, contain, eradicate, recover; 72 h customer notice	Annual live tabletop
Business-Continuity & Disaster-Recovery Plan	Weekly backups, 12-month retention	Semi-annual restore test
Privacy & Data-Protection Policy	U.S. privacy alignment, 30-day post-termination deletion	Annual

3 | Hosting & Architecture

Topic	Detail
Cloud Provider & Region	**Google Cloud Platform — us-central1 (Iowa)**
Compute Model	100 % serverless (Cloud Run & Cloud Functions) inside a private VPC

Topic	Detail
Data Storage & Back-ups	Google Cloud Datastore/Firestore (AES-256 encryption at rest); weekly encrypted backups to Cloud Storage retained 12 months
Network & Transit Security	TLS 1.2+ on all external endpoints; internal service-to-service calls use Google-managed mTLS
Administration	Google Workspace SSO + mandatory MFA; no corporate VPN required
CI/CD	Pull-request workflow with manual deploy during maintenance windows; automated pipeline planned

4 | Data Inventory & Usage

Data Element	Stored?	Notes
Player/Staff name, email, phone	Yes	Classified *Confidential*
Player size information	Yes	Confidential
Inventory item name, size, quantity	Yes	Internal
Payment, biometric, health data	No	—

Internal Use — Data is accessed only to operate the service or to troubleshoot a customer request.
Analytics — Only aggregate, de-identified metrics (no direct identifiers) are retained indefinitely.
Staging / Test — Uses synthetic data; production data is never copied to lower environments.

Retention & Destruction

Live customer data is deleted **within 30 days** of contract termination or written request. Back-ups containing that data expire automatically **12 months** after creation.

5 | Security Controls

Area	Control
Authentication	Native username/password + optional SMS or email MFA
Least-Privilege	Role-based IAM; quarterly access review
Encryption	In transit (TLS 1.2+) / At rest (AES-256, Google-managed keys)
Vulnerability Management	SCC mis-config & dependency alerts; patches applied during maintenance windows
Penetration Testing	Not yet performed; third-party test available on request
Employee Background Checks	Completed before any production access is granted
Training	No separate role-based program—scope of privileged personnel is small; annual module planned for Q2 2026

6 | Incident Detection & Response

- **Real-time Detection** – Google Cloud Security Command Center, Audit-Log alerting, uptime/error probes, and anomaly metrics feed a unified alert channel with pager escalation.
- **Documented IRP** – Four-phase checklist (identify → contain → eradicate → recover), severity matrix, communication templates, 72 h customer-notification SLA.
- **Investigation Resources** – CTO and on-call engineer handle triage and forensics via Cloud logs and BigQuery; Google Cloud IR specialists and external consultants under retainer for major events.
- **Customer Communications** – Initial notice < 72 h, periodic updates, and a full root-cause report within 10 business days.

---

7 | Audit & Risk Management

- **Quarterly Internal Audit** – Covers *all* assets, services, and processes that handle customer data: policy currency, IAM roles, SCC findings, backup restores, change-tickets, incident logs.
- **Scope Exclusions** – Non-production marketing assets and synthetic-data test environments (no customer data).
- **Third-Party Audits** – Not yet commissioned. Reliance on GCP's SOC 2/ISO 27001 attestations plus internal audits is deemed sufficient today; SOC 2 Type I pursuit is planned when customer scale requires (within ~18 months).
- **Formal Risk-Assessment Framework** – Not in place; compensating controls are continuous SCC monitoring and quarterly audits. A written NIST-aligned methodology will be adopted by **Q2 2026**.

---

8 | Human-Resources Security

Access to production data is restricted to a **small, trusted subset** of personnel. Controls:

- Pre-employment background screening
- Signed confidentiality & IP-assignment agreements
- MFA-protected least-privilege IAM roles
- Same-day access revocation checklist on off-boarding

A formal HR security program (onboarding/off-boarding SOP, annual role-based training) will be documented by **Q2 2026**.

---

9 | Vendor & Sub-Processor Management

Provider	**Function**	**Assurance**
Google Cloud Platform	Hosting, storage, IAM	SOC 2 Type II, ISO 27001
Amazon SES (AWS)	Transactional email	SOC 2 Type II, ISO 27001

With only two mature providers, a full vendor-risk program is not yet warranted. Due-diligence reviews of certifications and security bulletins are performed annually; a formal assessment questionnaire and contract checklist will be introduced by **Q4 2025**.

---

10 | Change Management

All infrastructure and application code reside in Git.

- **Standard, High-Impact, and Emergency** categories dictate review depth, approval path, rollback plan, and deployment timing.
- Pull-request discussions plus Cloud-Audit-Log entries form the immutable audit trail.
- Emergency fixes undergo post-change review within 24 h.

11 | Customer Commitments & Notifications

Commitment	Value
Encryption	TLS 1.2+ in transit; AES-256 at rest
Backup Retention	12 months
Data Deletion	≤ 30 days after contract end
Customer Incident Notice	≤ 72 h
Post-Incident Report	≤ 10 business days

12 | Summary of Key Statements

- EquipCheck has a **formal ISMS** with written policies covering data handling, access control, incident response, business continuity, and change management.
- **Quarterly internal audits** cover *all* systems that handle customer data; external audits will be pursued as scale demands.
- Customer data stays **encrypted at rest and in transit**, stored only in U.S. GCP regions, and is **deleted 30 days** after contract termination.
- **Incident Response Plan** guarantees customer notification within **72 hours** of any confirmed breach.
- Vendor footprint is limited to GCP and Amazon SES, each holding **SOC 2 Type II** and **ISO 27001** certifications.
- Formal risk-assessment, vendor-management, and role-based-training programs will be fully documented **by 2026** as the company grows.

For additional details or to request redacted copies of specific policies under NDA, contact **support@equipcheck.com**.