

How BRIEFED protects your program's records

A summary for security, IT and procurement reviewers. BRIEFED is pre-duty briefing and shift-change software for air medical and flight programs, operated by Compendium360, LLC.

Architecture and hosting

Platform

Runs on Cloudflare's global network: Cloudflare Workers (application), Cloudflare D1 (database) and Cloudflare Pages (web app).

Encryption in transit

All connections use HTTPS (TLS). Browsers are instructed to use HTTPS only (HSTS).

Delivery

A web application (installable to the home screen) on phones, tablets and computers. Nothing is installed on your servers.

Backups and recovery

Point-in-time recovery of the database to any minute within the last 30 days (Cloudflare D1 Time Travel).

Organization separation

Separate spaces

Each organization has its own address. Every record carries its organization and every query is limited to it.

Sessions bound to the organization

A sign-in issued for one organization is rejected at any other organization's address.

Identity and access

Invitation-only accounts

People are added by your administrators. Invitation links are single-use, expire, and only a hash of each link is stored.

Password storage

Passwords and PINs are never stored. Only salted PBKDF2-SHA256 hashes (100,000 rounds) are kept, compared in constant time.

Brute-force protection

Repeated failed sign-ins per address and per account are throttled and logged.

Role-based access

Roles and reporting lines are defined by your administrators. Managers see only the people beneath them; pilots see their own records.

Quick PIN sign-in

A 4-digit PIN works only on a device where the person has already signed in with their password, and is locked after repeated failures.

Session control

Administrators can sign one person, or their whole team, out of every device. Disabled accounts lose access immediately.

Logging and monitoring

Audit trail

Sign-ins, failed sign-ins, invitations, role and account changes, and brief submissions are recorded with time, account and network address.

Record integrity

Every brief is time-stamped and tied to the account that submitted it, with the pilot, aircraft, base and shift.

Application security

Web protections

Security headers on every page, protection against being embedded by other sites (clickjacking), and restrictive content policies on administrative pages.

Input handling

Database queries are parameterized; submitted data is validated and size-limited.

Updates

Fixes and improvements reach every device automatically, with a one-tap refresh.

Vulnerability reports

Reported through a private ticket at [briefed.flights/support](#) ("Report a security issue").

Data

Data collected	Account details (name, username, role, optional email), base and aircraft assignments, briefs (weather snapshot, aircraft status, crew names, risk score, med crew acknowledgment), and audit records.
Ownership and export	Your organization's data belongs to your organization. Briefs export as PDF; briefings, bases, people and alerts export as CSV.
Use of data	Used only to provide the service. Not sold, and not used for advertising.
Analytics	First-party, cookie-free usage analytics only.
Third-party data sources	Weather and hazards from the NWS Aviation Weather Center and the FAA (NOTAMs, TFRs, WeatherCams).

Questionnaires and further documentation. We're happy to complete your organization's security or vendor questionnaire. Open a ticket at [briefed.flights/support](#) and choose "Support question" or "Report a security issue".