

Security and data handling

An overview of the current hosted application, its safeguards, and the decisions to complete with your IT and security teams before an evaluation uses actual utility records.

Scope
**Current hosted POLT
configuration**

Reviewed
September 7, 2026

Contact
justin@polt.systems

01 Access and permissions

An administrator creates each account; users cannot register themselves. Access to operational records requires sign-in, and permissions are enforced on the server. Passwords are hashed, sign-in attempts are rate limited, and production sessions use secure, HttpOnly cookies.

Viewer. Read, search, copy, and export records within the authorized workspace.

Operator. Viewer capabilities, plus creating and editing operational records.

Admin. Operator capabilities, plus account and reference management and record archive/restore.

Application sign-in currently uses email and password. Application MFA and enterprise SSO are not currently configured; any required identity integration must be agreed and verified before the pilot.

02 Hosting and information flow

Vercel hosts the application. Neon PostgreSQL stores the authoritative saved records. The current application and database configuration uses the US East region. Web access uses HTTPS and database connections verify TLS certificates.

Operational records. Saved logs, change history, account records, and user preferences are held in PostgreSQL. Application access is scoped to workspace membership.

Service providers. Vercel hosts the application; Neon hosts the database; GitHub Actions stores encrypted backup artifacts. Cloudflare provides domain DNS and DNSSEC. Google Workspace handles correspondence sent to POLT's contact address.

Browser data. When draft recovery is enabled, temporary unsaved drafts may remain in browser storage for up to 24 hours. They are separate from saved records and cleared on save or sign-out. Shared-device use needs an agreed draft-recovery policy.

The application has no configured third-party product analytics or AI model integration. Hosting and authentication services still process the technical information needed to operate the service. Review provider terms, locations, and data-processing requirements with your organization.

03 Record integrity and retention

Each saved edit and its history are recorded together. If another user has changed the log, POLT requires review before saving over that version. Retrying a creation request uses its original identifier to avoid creating the same records twice. Saved history includes the acting user and the change time.

Archiving preserves a record and its history. History is protected against modification through ordinary application use; it is not tamper-proof against database administrators. A utility's retention schedule, legal holds, export needs, and eventual deletion process must be agreed for its evaluation. The backup retention period is separate from the retention of operational records.

CSV export supports authorized operational results. A complete exit plan should also specify how audit history and any other required data will be supplied.

04 Backup and recovery

The hosted backup workflow is scheduled every six hours. It encrypts the database archive and its verification manifest, performs an isolated restore check, and publishes encrypted artifacts to GitHub Actions with 14-day retention. A hosted backup was downloaded and restored successfully in a documented drill on September 7, 2026.

Backup schedules can be delayed or fail. A completed drill verifies the tested snapshot; it does not establish an end-to-end recovery-time guarantee. Browser-only unsaved drafts, source code, and secrets need their own protection.

Agree acceptable data loss and recovery time, backup ownership, alert delivery, incident contacts, and a full cutover exercise before operational reliance. Continuous availability and a staffed 24/7 response are not currently committed.

05 Items for the utility's review

This overview describes the current implementation. It is not an independent security assessment, a regulatory compliance certification, or a service-level agreement. Begin demonstrations with fictional records; obtain the appropriate utility approvals before entering actual utility information.

Identity and access. Required MFA/SSO, account approval, access reviews, shared workstations, and timely account removal.

Data and assurance. Permitted records, hosting approval, data location, retention, processing agreements, and any independent testing or compliance evidence required by the utility.

Operations and support. Availability expectations, recovery objectives, security reporting, incident escalation, support hours, capacity, and change management.

Security questions or concerns: contact Justin at justin@polt.systems. Describe the issue without including passwords, sensitive operational records, or other confidential material; arrange an appropriate exchange method if needed.

Related guides

Introduction: polt.systems/intro | Pilot guide: polt.systems/pilot