



CERF ELN

CERF for Business

Lab-Ally LLC · cerf-notebook.com · +1 (614) 407-4547

CERF for Business

CERF (Collaborative Electronic Research Framework) is a secure, centrally managed knowledge asset platform built for any organization where records, documents, and decisions need to be traceable, defensible, and available forever.

How much time does your organization waste emailing documents to different team members, searching for the latest version of important files, trying to figure out who last edited a document, and who currently has access to what? If your organization needs a reliable, centralized store for all of its knowledge assets — and you cannot trust fragmented commercial tools to protect your confidential information long-term — CERF can help.

CERF replaces the fragmented, non-compliant tools most organizations rely on today — SharePoint, shared drives, email attachments, Dropbox, Google Drive, and paper notebooks — with a single, compliant, centrally managed system that your organization can depend on for decades.

WHO IS CERF FOR?

CERF is designed for any organization where data integrity, long-term accessibility, regulatory compliance, intellectual property protection, and data sovereignty matter.

Who	How CERF Serves Them
Biomedical & Pharma R&D;	IP-intensive, regulated environments requiring compliant experimental records, signed workflows, SOP management, and audit-ready data.
Engineering & Construction	Project records, design revision histories, contractor sign-off trails, inspection documentation, and specification version control.
Financial Services	Client records, transaction documentation, compliance filings, and the complete audit trail regulators expect.
Legal & Professional Services	Matter files, agreements, correspondence, dispute records, and engagement documentation — versioned, access-controlled, and permanently retrievable.
Real Estate & Property	Transaction records, inspection histories, ownership documentation, lease agreements, and contractor records.
Insurance	Claims files, underwriting records, actuarial documentation, regulatory compliance records, and policy histories.

Medical Device & HealthTech	Design history files, verification records, risk management documentation, and FDA submission packages.
Any Auditable Organization	Government contractors, defense suppliers, and any organization whose records may be examined by regulators, auditors, or counterparties in litigation.

SECURITY & ACCESS CONTROL

Your Files. Your Network. Your Rules.

With CERF, all of your most important documents can be kept on a single server inside your secure network — or on a cloud host of your choice. Either way, your organization retains complete top-down management awareness: you know exactly who has access to what, who has read or modified a file, where it was accessed from, when it was edited, and what every previous version looked like.

CERF enforces fine-grained, role-based access controls down to the level of individual records. Unauthorized users cannot even see that a resource exists in search results — let alone open or download it. Every access event, every login attempt, and every modification is captured in a tamper-proof, computer-generated audit trail that cannot be deleted or altered from within CERF.

CERF fully supports FISMA (Federal Information Security Management Act) requirements and has been deployed at government research institutions and defense contractors. For the most sensitive environments, CERF can operate on a completely air-gapped local area network with no internet connectivity whatsoever.

- **Role-based access — nine levels:** from Read Only through Annotator, Editor, Manager, and System Administrator, assigned at the workgroup level and enforced on every record.
- **Single-session enforcement:** no user can be logged in from multiple locations simultaneously. Session tokens are unique and expire on timeout or logout.
- **Immutable audit trail:** every action timestamped, attributed, and permanently recorded. Available for export at any time for agency review, litigation discovery, or internal investigation.
- **Air-gap capable deployment:** CERF makes no required internet calls. Deploy on a sealed LAN with zero external exposure, indefinitely.
- **Multi-factor authentication:** optional, administrator-enforced TOTP MFA for all user logins, compatible with Google Authenticator, Microsoft Authenticator, and Bitwarden.
- **Cryptographic file integrity:** hash verification on every file check-in detects any tampering between the workstation and the server.

INTELLECTUAL PROPERTY

Your IP Is Only as Strong as Your Records.

Intellectual property is created in moments — but protected over years, through documentation. A patent application, a trade secret defence, or an inventorship dispute is ultimately decided by whose records are more complete, more credible, and more tamper-proof. CERF was built to be exactly that record.

From the first sketch to the final filing, every version of every document in CERF is permanently retained with a cryptographically signed timestamp, a unique identifier, and a complete edit history. CERF establishes an unbroken chain of custody for your organization's creative and technical work — the kind of record that holds up in a derivation proceeding, a patent interference dispute, or a trade secret misappropriation case.

- **Timestamped invention records:** every file carries a computer-generated, cryptographically signed timestamp from the moment of creation, establishing a defensible priority date for invention disclosure.
- **PKI digital signatures:** CERF uses the U.S. federal government's Digital Signature Algorithm (DSA). Signed records carry a unique cryptographic hash that cannot be transferred, falsified, or retroactively applied.
- **Complete version lineage:** every iteration of every document is retained permanently, with full authorship attribution. The creative and decision-making process is reconstructable from day one.
- **Trade secret access controls:** granular workgroup permissions ensure sensitive IP is accessible only to authorized individuals. The audit trail proves who accessed what and when.
- **Contributor attribution:** co-contributor metadata fields formally attribute shared authorship at the record level, resolving inventorship questions before they become disputes.

The best time to deploy CERF is the first day your organization opens its doors, so that every idea, decision, and document is captured from the start. The second best time is now.

DUE DILIGENCE

Poor Documentation Kills Deals.

If your organization works in a field subject to auditing — or if you hope to be acquired, attract venture investment, or pursue an IPO — you will face due diligence. Ad hoc communication, missing or incomplete agreements, absent records of key decisions, and unresolvable questions about IP ownership make a devastating impression on investors, acquirers, and their legal teams.

Industry specialists report that approximately 60% of executives attribute deal failures to poor due diligence. The path to VC funding, mergers, acquisitions, and public listings can be blocked entirely by the avoidable inability to produce a complete, timestamped, unambiguous organizational history. Your inventions, IP agreements, investor arrangements, partner relationships, company ownership structure, legal provenance, and records of dispute resolution all need to be instantly accessible and beyond question.

CERF functions as a continuously maintained organizational data room. Every document your organization generates — from the first NDA to the latest board resolution — is versioned, attributed, signed, and searchable. When the due diligence team arrives, you produce everything they need in minutes, not weeks.

- **Controlled access for external reviewers:** grant due diligence teams time-limited, read-only access to specific workgroups. They see exactly what you authorize, nothing more.
- **Single-click audit exports:** produce complete, timestamped records of all activity, signatures, and document histories for regulatory or legal review.
- **Complete organizational history:** who decided what, when, with what authority, and on the basis of which version of which document.

-
- **IP ownership documentation:** inventor attribution, assignment records, and the complete creative lineage of every patent-pending asset.

Failure to produce complete records may kill your organization if the ownership of your IP is challenged, disputes lead to litigation, regulators issue warnings, or patent applications are denied on inventorship grounds.

COMPLIANCE

Built for Audits Before You Need One.

CERF is fully 21 CFR Part 11 compliant and purpose-built for regulated environments — superior to generic tools like SharePoint or Dropbox that require expensive, frequently failing customisation to achieve compliance. CERF enforces compliance automatically, as a structural feature of the system, not as an add-on.

Initially created for scientific research organizations and now recommended for use in biomedical, financial, legal, real estate, insurance, and engineering sectors, CERF has proven equally indispensable for any organization that needs to keep — and show that it kept — accurate records of events. The BEST time to deploy CERF is the first day your organization is activated, so that every file is stored safely from day one. The second best time is right now.

- **Immutable, computer-generated audit trail:** every user action captured with date/time, username, action taken, and previous record state. Cannot be modified or deleted from within CERF.
- **True PKI digital signatures:** built-in Public Key Infrastructure hashing via the U.S. government Digital Signature Algorithm. Every signed record carries a unique MD5 hash digest cryptographically linked to the record it protects.
- **Configurable signature workflows:** Submitter → Peer Reviewer → Manager → Legal/Regulatory. A record cannot be signed until all required workflow steps and SOP placeholders are satisfied.
- **GLP-compliant corrections:** errors corrected using the built-in Strike Out function. The original text remains legible in all views and printed copies, as required by GLP and ALCOA principles.
- **IQ/OQ validation support:** Lab-Ally and qualified validation partners provide Installation Qualification and Operational Qualification services for your specific deployment environment.
- **SOP lifecycle management:** controlled document module manages SOPs and required training records through creation, approval, acknowledgment, expiry, renewal, and archiving.

M&A; & INVESTMENT READINESS

The Documentation That Gets Deals Done.

When an acquirer, investor, or IPO underwriter conducts due diligence, they are not just evaluating your technology or your market — they are evaluating your organizational hygiene. Companies that can produce complete, credible, tamper-proof records of their decisions, their IP, their compliance history, and their ownership structure move through due diligence faster, negotiate from greater confidence, and close at better valuations.

CERF functions as a permanently maintained organizational data room. Rather than scrambling to assemble documentation when a deal materializes, organizations running CERF have been building that record since day one. Every agreement, board resolution, invention disclosure, and compliance sign-off is already versioned, signed, attributed, and searchable.

For organizations considering a future exit — through acquisition, private equity investment, or public listing — deploying CERF early is one of the highest-return investments in organizational infrastructure you can make.

- **Always-ready data room:** CERF is not a temporary virtual data room assembled under pressure. It is a continuously maintained organizational record always ready for external scrutiny.
- **Granular external access:** grant acquiring parties or investors access to precisely defined workgroups with full audit logging of everything they view.
- **IP portfolio documentation:** complete records of invention, assignment, licensing, and ownership for every asset in your IP portfolio.
- **Compliance posture evidence:** demonstrate to acquirers that your regulatory compliance is structural and validated, not a series of manual workarounds.
- **Litigation readiness:** CERF's immutable audit trail and cryptographic signatures produce court-admissible records that are far more defensible than email threads and shared drives.

CONTINUITY

Institutional Memory That Outlasts Your Staff.

CERF serves as your organization's corporate memory — maintaining an accurate, unambiguous record of events occurring over time, even as the people involved move on, retire, or forget. CERF knows what happened and who was responsible long after the original contributors have left your organization, long after the project has evolved into something quite different, and long after the details have faded from human memory.

This is especially critical for distributed organizations. CERF facilitates effortless collaboration between colleagues across offices, time zones, and continents — with the same granular access controls and audit trails regardless of where contributors are located. Remote and hybrid teams work seamlessly within the same system, with managers retaining full visibility of who is working on what.

When a key employee leaves, their entire contribution history stays — attributed, versioned, and accessible to their successors. When a long-running project is re-examined years later, CERF reconstructs the complete decision timeline without relying on anyone's recollection.

- **Permanent version history:** no version of any file is ever deleted. The complete creative and decision-making history of your organization is always retrievable.
- **Full contributor attribution:** every record carries the identity of every contributor, reviewer, and signatory — permanently associated with their specific contribution.
- **Cross-platform collaboration:** Windows, Mac, and Linux users collaborate seamlessly within the same system, on-site or remotely.
- **Email-to-CERF ingestion:** any user can send files and email attachments directly into CERF via email, attributed to the correct user, with automatic metadata extraction.
- **Find Experts search:** locate colleagues with specific expertise based on their documented contributions — a powerful capability for large or distributed teams.

CERF is specifically designed for ultra-long-term record storage using industry-standard, open-source components selected for technological longevity — not for a few years of use, but for decades.

LONG-TERM SUSTAINABILITY

Built to Run Dependably for Decades.

Most software-as-a-service products are designed to maximize recurring revenue — which means your data, your access, and your compliance posture are all contingent on an ongoing commercial relationship with a vendor whose priorities may change. CERF was designed around a fundamentally different philosophy: your data belongs to you, your system runs on your terms, and your access is permanent.

CERF has been in continuous production for more than 20 years. In that time, it has outlasted multiple generations of competing products and the kind of industry consolidation that has left customers of other systems scrambling for alternatives. The architecture is deliberately conservative — built on open-source industry stalwarts selected for longevity, not novelty.

Whether you choose an annual subscription or a perpetual license, your CERF installation will continue to operate independently, on your infrastructure, with your data in native formats, indefinitely — even on a sealed LAN with no internet access.

- **Perpetual license option:** a one-time purchase gives your organization permanent access to your CERF system and all your data, regardless of future payments or changes in your relationship with Lab-Ally.
- **Annual subscription option:** for organizations that prefer predictable operating expenditure, CERF is available as an annual subscription with all updates included.
- **Open-source components only:** CERF is built exclusively on open-source, industry-standard technologies. No component depends on proprietary or externally hosted services that could be deprecated or discontinued.
- **Native file storage:** data files are stored in their original native format in a secure file store, not compressed into a proprietary database. Your data is always extractable.
- **Unlimited storage capacity:** on-premise installs carry no per-gigabyte fees. Scale your storage infrastructure as your organization grows, with no vendor involvement required.
- **Fast bulk export:** the CERF Exporter returns your data in exactly the format it was submitted, organized hierarchically, with all metadata provided as open-standard XML files. Your data is never locked in.
- **Regular updates included:** all software updates (typically two per year) are included in the standard support package with no significant service interruption.

If Lab-Ally is ever discontinued, your perpetual-licensed system continues to run and your data remains fully accessible — stored in native formats on your own infrastructure, forever.

DEPLOYMENT OPTIONS

Flexible to Deploy — On Your Terms.

CERF runs as a client-server system. The CERF server holds all data; lightweight desktop clients connect from Windows, Mac, or Linux workstations on your network or remotely. Three deployment models are supported:

Cloud	Deploy on any cloud provider of your choice — AWS, Azure, GCP, or any VPS. Lab-Ally can also host and manage a private instance for you with no IT burden on your team.
On-Premise	Install CERF on your own physical or virtual server for maximum control over your data and infrastructure. The CERF server requires minimal ongoing IT maintenance.
Sealed LAN	For the most stringent security environments, CERF can operate on a completely air-gapped local area network with no internet connectivity whatsoever.

CERF is database-agnostic — compatible with MySQL (included by default), Microsoft SQL Server, or Oracle. Files are stored in native format; nothing is compressed into a proprietary container. Licensing is available as an annual subscription or perpetual: named-user seats belong to your organization permanently, regardless of your ongoing relationship with Lab-Ally.

DEPLOYMENT & SUPPORT

Lab-Ally Was Founded by Scientists.

Our implementation and support team brings deep familiarity with research workflows, regulatory requirements, and the practical challenges of deploying data management systems in active organizational environments.

- **Full deployment assistance:** server configuration, workgroup setup, workflow design, and user onboarding for organizations of any size.
- **IQ/OQ validation support:** in partnership with qualified third-party validation specialists, for organizations subject to 21 CFR Part 11 or equivalent requirements.
- **Cross-platform flexibility:** CERF excels in mixed environments — Mac, Windows, and Linux users working on-site or remotely.
- **Comprehensive training:** administrator and end-user training including live webcast sessions and formal user certification materials.
- **Responsive human support:** email, phone, and scheduled appointments. A live human being answers your support questions.
- **Free trial server access:** try CERF before you commit, on a fully functional hosted trial server.

Ready to see CERF in action?

Contact us for a live demonstration or to access a free trial server.

cerf-notebook.com · info@lab-ally.com · +1 (614) 407-4547