COLLABRANCE®
A GREATAMERICA COMPANY

Collabrance Co-Managed IT Support for Financial Institutions:

Security Policies & Practices

We recognize the unique security implications specific to many financial institutions and the concerns that may come with evaluating a third-party partnership for IT services. In this document, we've aimed to address those considerations and outline the security measures Collabrance takes in delivering co-managed IT support and service to our customers, including:

- Your top concerns related to systems access and connectivity
- The technical and procedural requirements of working with Collabrance
- Frequently asked questions, including security incident response and business continuity plans
- Information about security controls and technical training

Collabrance is a wholly owned subsidiary of GreatAmerica Financial Services, the leading provider of equipment financing in the U.S. We have firsthand familiarity with the security concerns associated with financial institutions, because we are rooted in one. Both Collabrance and GreatAmerica are 100% U.S.-based and operate only in the U.S.

There are a number of procedures we've put in place to navigate the perceived risks of entrusting an outsourced provider with access to your internal systems. We're confident in our ability to provide safe and secure IT services to your company and companies like yours – it's something we do every day.

TOP CUSTOMER SECURITY CONCERNS OF OUTSOURCED IT

1. Access to company systems

Collabrance uses N-able remote management software. The easiest way for our support team to help an end user is to have the N-able Essential License installed on each computer. The Essential agent permits Collabrance to connect to a device only with the end user's approval. Our remote management tools do not have the ability to run scripts, access or change the file system, or most other administrative tasks. Administrative access to systems and tools should be granted to us only as needed.

Even with these accessibility restrictions, we recognize installing software may present issues in many environments. As an alternative, we are always willing to evaluate what tools you may have in place to give Collabrance remote control within the bounds of your company's requirements.

2. Data documentation

Any connection to any device on your network is logged by Collabrance and can be audited at any time. Additionally, all calls into and out of the Collabrance service desk are recorded and saved for 30 days and can be provided at your request. If concerns ever arise around the sharing of protected data or improper use by anyone on our team, we can quickly locate and address the issue with transparent information.

Any data we have for your system is stored in our documentation tool, IT Glue. This tool is only accessible by our service desk technicians and requires multi-factor user authentication. All accesses and changes made in IT Glue are logged and can be audited as needed.

3. Connectivity to company network
Collabrance will not have direct connectivity to your company's network. No virtual private network (VPN) will be established.

4. Administrative access
Rest assured, Collabrance will not have – nor do we want – administrative access to your banking systems. Our co-managed service is limited to triage and tier 1 technical support. Granular delegated administrative privileges (GDAP) should allow us to assist with password resets, unlocking accounts, resetting print spoolers, and other basic issues. You control the level of access given to our technical team, and we work to accommodate your business's needs and requirements.

5. Remote monitoring and management (RMM) and professional services automation (PSA) systems
Each Collabrance service desk technician uses individual account credentials to access our RMM and PSA platforms, both of which require multi-factor authentication for login. User-level access information is available for either system at any time.

6. Technical talent and competency
Collabrance is 100% U.S.-based, with most of our technical team working from our headquarters in Cedar Rapids, Iowa, and others within surrounding U.S. states.

Our team of 30+ technicians range in experience and skill level, from triage support to ensure requests are prioritized and resolved efficiently, up to tier 3 product engineers. The team dedicated to supporting our remote management software alone boasts a combined 32 years of experience.

While our co-managed IT support is limited to triage and tier 1 user issues, our higher-level technicians are always available as a resource to the greater service desk team, and technicians of all levels are responsible for answering user support calls during high-volume periods.

TECHNICAL REQUIREMENTS FOR COLLABRANCE CUSTOMERS

Installation of N-able Essential License on supported devices
Additionally, if your company uses virtual technology throughout your environment – like desktop virtualization for offline or remote access, for example – we'll need a virtual solution or physical device that provides access to the virtual system when we receive support requests. This could be a Citrix host or a standalone device or server. Generally, whatever tool is being used by your entry-level technicians for remote access to answer basic support requests is where we would first look to determine a solution.

For more information about the N-able Essential License software, see item 1 above, Access to company systems.

A detailed knowledge base outlining the 10 to 15 most common user support issues Collabrance will focus on
The most common user support requests typically include password resets, user verification, account unlocks, basic hardware troubleshooting, reboots, and printer issues, to name a few. If necessary, we can manage more specific user issues unique to your institution.

Collabrance needs only the administrative access necessary to do the tasks you would like us to focus on.
As the customer, you decide what access allowances Collabrance has, and you control any adjustments made to that level of access.

COLLABRANCE SERVICE ACTIVATION REQUIREMENTS

1. Primary contacts: The people on your team we can work with to escalate issues and assist with requests we can't resolve. We will work together to define the escalation flow, so we are helping users in the most efficient way.
2. Vendor access information: We only need vendor access information for the business applications you want us to support, and you decide what those applications are.
3. Workstation information including number of workstations and operating system.
4. Domain controller/active directory server: Access level dependent on support issues Collabrance will handle.

INCIDENT RESPONSE AND BUSINESS CONTINUITY

Collabrance maintains a documented incident response plan. We conduct annual discussion-based exercises to review roles and responsibilities in the event of an emergency. Quarterly security incident reviews are held to assess real activity and evaluate our processes.

What if a security incident occurs within Collabrance?
Collabrance has a muti-tiered response plan for internal IT security. If a security event is detected within our environment, our endpoint detection and response (EDR) software and other security tools will automatically mitigate the threat and alert appropriate staff. Depending on severity and impact, the event will be escalated to the Collabrance and GreatAmerica IT and leadership teams, as directed by procedure.

In the event a suspected security breach is confirmed, Collabrance legal counsel will contact customers within 72 hours. Critical incidents are reported and managed with executive oversight and communication. Forensic analysis will be conducted by qualified third-party investigators.

Collabrance supports mitigation and investigation through log collection and analysis, validation of restored systems, communication to stakeholders, and documentation for compliance. Other events – such as password sharing or unauthorized disclosure – will be investigated and reported as required by procedure.

What if a security incident occurs within your company?
Collabrance uses ITIL incident management to assess the urgency and impact of security events. Based on the incident specifics, our team will determine if there is a use-case – such as credential or email compromise – and apply an appropriate runbook procedure to ensure consistent and timely action.

Collabrance can support your specific incident response needs including communication, escalation, evidence collection, and validation.

What if a security incident occurs with another Collabrance customer?
A security event affecting another Collabrance customer would not be shared unless a determination is made by general counsel that there is impact to your company, and your security incident response plan would be executed as necessary. Likewise, a security event affecting your company would not be shared with any other party.

SECURITY CONTROLS AND COMPLIANCE SUPPORT

Collabrance is insured under a general liability policy with a cyber insurance rider from TrueNorth. If both parties – Collabrance and your company – are insured, there should be mutual protection.

In addition, Collabrance is SOC 2 accredited and certified to have the highest operational standards to meet the core trust principles of security, availability, processing integrity, confidentiality, and privacy. We maintain information security policies framed in NIST 800 and references provided by the FFIEC. We can share evidence of our controls with a mutual NDA relationship upon request.

TECHNICAL TRAINING

Training is continuous and ongoing at Collabrance. Our technicians are trained in skills and security awareness, which requires formal training on an annual basis. If there is a particular training or skillset you'd like our technical team to have, we're happy to discuss our records and training history.

BUSINESS CONTINUITY

Our services and data are protected by backup and recovery procedures. Additionally, all key Collabrance suppliers are SOC accredited to meet best practices for disaster recovery and business continuity planning.

Outside of scheduled training and exercises, Collabrance has successfully executed continuity strategies in critical real-life incidents, including a widespread weather event in August 2020 that downed over 950,000 trees and left hundreds of thousands of residents in eastern Iowa and the surrounding region without power – some for up to two weeks.

Thank you for considering Collabrance for your co-managed IT solution. If there are additional questions we can answer, please don't hesitate to get in touch with a member of our sales or service team.

COLLABRANCE®
A GREATAMERICA COMPANY