Security and Availability Information

Physical Security, Backups and Redundancies

- LabArchives servers are kept in a secure, primary data center with a separate disaster recovery data center installation
- Customer data is continuously synced between the primary and disaster recovery data centers with regular backups of customer data kept in multiple locations using multiple backup technologies
- Customer data is optimized and checked for integrity regularly
- LabArchives servers are completely isolated from other corporate machines, servers, email systems, networks, etc.
- Primary and secondary data centers provide redundancies for power, HVAC and network connectivity

Network Security

- LabArchives servers are protected by redundant, industry standard firewalls and security devices
- All network traffic is logged and monitored for any suspicious activity regularly

Data and Application Security

- LabArchives is a secure application written in Ruby and runs on Linux servers
- SSL certificates provide full-time HTTPS security and identity verification to every connection made to the LabArchives application.
- All code is written by LabArchives' developers with decades of experience writing secure, data driven, web applications
- Each customer’s data is stored in its own database, isolated from other customer data
- LabArchives accounts are secured with a login/password and all access to LabArchives is logged

High Availability

- Critical server statistics and accessibility are monitored from multiple locations worldwide continuously
- Systems staff are standing by to respond when monitoring thresholds for availability and performance are reached
- Procedures to failover to secondary data centers have been documented and are tested regularly

Local Installations

- We can arrange to install servers at your location to give you complete control over the security, backups and availability of your own LabArchives system
- Contact sales@labarchives.com for more information about this option.