

● ● ● An Overview of Labrador Data Security Measures



At Labrador, complete protection of our clients' confidential information underpins our regulated financial documents production processes. We invest 9% of revenues each year in technologies and infrastructure that manage and protect customer data. Our online tools make it easy to communicate with production team members and to access documents. Labrador's systems and processes described below guarantee that sensitive financial information remains secure at all times.

LABRADOR SERVERS

All production data is secured in an Orange Business Services datacenter (ISO 9002 and SAS 70 certifications). Orange Business Services is a wholly owned subsidiary of Orange, the world's third largest telecommunications company.

Specifications:

- Three different uninterruptible power supplies provide the datacenter with electricity. The datacenter also has an emergency diesel generator that can provide power for up to five days;
- Orange Business Services benefits from a preferential relationship with its electricity provider: private direct power supply with no interference by other grid users;
- Dual fiber routes service the datacenter and ensure zero downtime;
- Data is securely and permanently saved on our servers throughout the project;
- Fire safety is assured by dual, automatic fire detection and extinguishing systems (using neutral gas);
- The datacenter is under 24/7/365 video surveillance and monitoring;
- Access control via cards and access codes ensure that only qualified, authorized individuals have access to the datacenter;
- Intrusion alarms sound in the case of any unauthorized access, averting security staff;
- Air conditioning and controlled ventilation provide for an in-room temperature of 70°F and 50% humidity (+/- 5%).

LABRADOR'S EXCHANGE PLATFORM

Labrador never uses email to communicate confidential files or attachments. We have developed a dedicated platform that is as easy to use as a classic FTP platform and as secure as the most high-security websites. This platform is a simple and proven method to easily communicate confidential files between Labrador and its clients.

- Extremely high-level authentication (2048 bits – 256 bit encryption key) and real-time data encryption (256 bits - real-time encryption);
- Secure https:// connection;
- Unique confidential username and password;
- ISO/IEC 27001:2005 hosting;
- Destruction of files by multiple writing of random data at the end of the subscription period.

Internal security procedures:

Every Labrador employee signs a non-disclosure agreement, and we maintain a list of the employees who work with client data; this list is communicated to our clients on request. Every person working at or visiting any of our facilities is electronically "badged" into and out of the location.

In the course of project management, each Labrador team member respects strict security instructions. Our project management processes and performance are regularly audited in order to further reinforce our data protection measures.

Materials printed on behalf of our clients are systematically shredded and stored in locked bins. The bins are then emptied and processed by a service provider specialized in the recycling of highly confidential information.

Our security certificates are provided by Thawte, which accounts for 40% of the global SSL market. Thawte has issued more than 945,000 SSL and code signing certificates since 1995, protecting identities and transactions in over 240 countries.

Please contact a Labrador representative for further information about our security technology and internal security procedures:

ATLANTA

Kimberly Salter
salter.k@labrador-company.com
(404) 419-1317

NEW YORK

Nancy Schueneman
schueneman.n@labrador-company.com
(212) 792-4066