



## About Security

Security at ABACUS Backups is obviously a serious matter. This document details some of the procedures and safeguards which we have implemented to protect our clients' data.

### **Introduction:**

As an introduction, manual backups (to tape or CD) are insecure and error prone. This is because manual backups depend on human beings to remember to do the backup, to change the tapes, to verify the tapes, and to store them offsite.

Even with all the effort involved, manual backups are subject to considerable risk – in terms of fire, theft or flood. They usually have no password protection, decay over time, and are unreliable to restore data. In a survey from "Storage Magazine" (published November, 2005), 77% responded that their own tape backup device failed to restore all of their data more than 50% of the time.

With ABACUS, data is stored in a way which can be considered secure, even by the most critical of standards. Important elements of this security strategy include:

- Replication to multiple servers across N. America
- Transmission and storage using 128 Bit Encryption
- IP Address Restriction
- Secure physical premises
- Automatic, daily email reports
- Two levels of password protection

More details on each of the above:

### **Replication**

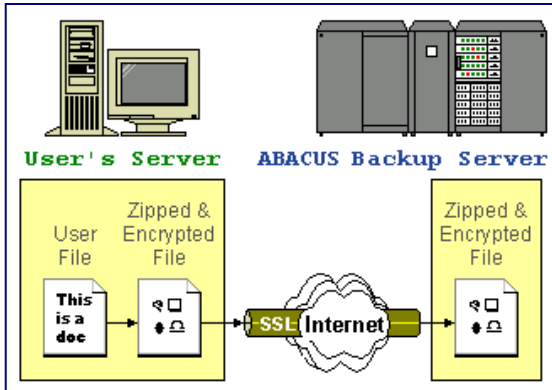
With every backup performed by ABACUS, client data is automatically and simultaneously replicated to multiple servers across N. America. We do not advertise the locations of these servers (with the exception of one), and the premises are physically secure. See below "Secure Physical Premises".

The minimum distance between any two servers is 300 miles. That means in the event of a natural disaster, theft or hardware failure, our clients' data remains uncompromised.

## 128 Bit Encryption:

Why our security is *better than the Bank*:

To compare, when we do our banking online, we trust the security because our connection is encrypted at 128 bits. 128 Bit encryption is subjected to frequent public review, and no (zero) known attacks have been successful against it.



But...did you realize that the bank stores our data as clear text? The proof is that when we call them with a question, the bank employee can always answer us because he/she can see all our sensitive information.

At ABACUS however, both the client's connection and his/her data storage is done via 128 bit encryption. That means even if someone were able to hack the connection to our servers, the data would

be useless to them. Moreover, it would take more than  $8 \times 10^{17}$  years to crack the code using the world's most sophisticated CPU.<sup>1</sup>

Currently, ABACUS employs the 128-bit Twofish algorithm. It is a block cipher designed by Counterpane Labs. It was also one of the five Advanced Encryption Standard (AES) finalists chosen by National Institute of Standard and Technology (NIST).

No one, not even our employees, can access clients' data. Only the holder of the "decryption key" can download and decrypt the data.

## IP Address Restriction:

Access to our clients' backup files can be restricted by the range of IP addresses you have defined. If someone tries to access your data from an IP address not on your defined list, their access will be denied.

This additional security ensures backup files can not be restored outside company premises, even when the username and password are known.

---

<sup>1</sup> Here's the math: A 128-bit key size has 2128 or around  $3.4 \times 10^{38}$  possible combination. The ASCI White Supercomputer manufactured by IBM has a CPU of 375 Mhz, and has 8192 processors. This totals a capability of 12.3 teraflops (trillions of operations/second). As such, it would take  $8.77 \times 10^{17}$  years to test all combinations. To use brute force attack (checking all combinations) on this encryption algorithm, it would take:  $(3.4 \times 10^{38}) / (12.3 \times 10^{12})$  seconds  $\sim 2.76 \times 10^{25}$ sec (i.e. 876,530,835,323,573,935 years or)  $8.77 \times 10^{17}$  years

## **Government Authorization:**

Our company is authorized by the Canadian Federal Government to store **PROTECTED** information up to and including the PROTECTED "B" level at its site. Our Canadian and International Industrial Security Directorate (CIISD) file number is 95365389-0000451338.

Infrastructure:

ABACUS has implemented a high-availability Internet Transit network infrastructure, available within secure facilities. This has been accomplished by the following:

- » Connection uses Cisco's HSRP (hot standby router protocol)
- » Multiple upstream providers
- » Fully redundant OCn internal backbone network
- » All network devices have onsite spares
- » All key network components are monitored 24x7
- » Physical access to premises is restricted to authorized personnel only.
- » Multiple mirror locations throughout North America.
- » We guarantee 99.9% uninterrupted transit to the servers.

## **Secure Physical Premises:**

**The Building** - Toronto Star Building in downtown Toronto, Canada

**Year built** - 1972

**Ceiling height** - 12 feet

**Construction** - Reinforced cast in place concrete

**Building security** - 24/7 building security guard, monitored closed circuit cameras, 24/7 facility access with photo ID card

**Elevators/Loading facilities** - Freight elevator available for booking upon request

**Parking** - Pay parking available. 3 independent pay parking facilities within a 1 block radius

**Directions** - The facility is located in the Toronto Star building at the corner of Yonge and Queens Quay

**NOC/support** - 24/7 NOC in Toronto, on-site support available, 24/7 engineer on call.

**Facility security** - 24/7 photo ID and access card, monitored closed circuit camera system

**Backup power** - UPS and dedicated generator

**Environmental design** - Redundant climate control system