

BalaBoss

BalaBoss Service Security

BalaBoss is committed to the highest levels of security and ensures that the architecture, policies, processes, and tools are in place to ensure maximum security.

Hosting and Hardware Security

- BalaBoss hosts client data in two secure bunker type facilities in Montreal. These facilities are Canadian owned and operated – two locations are utilized – one for production servers and a second location for backup servers.
- The access control system on-site is composed of a biometric reader to authenticate fingerprints, access card readers, and a series of surveillance cameras
- Each facility includes a 300KVA UPS and a 500KVA diesel generator
- Hydro-Quebec's electricity powers the UPS (Uninterruptible Power Supplies) in case of power loss, and a diesel generator is automatically started in less than fifteen (15) seconds via an ATS (Automatic Transfer Switch).
- The generator is used to supply energy to the data centre for fifteen (15) minutes every Monday morning, to ensure full functionality of the system.
- Air conditioning is supplied by completely redundant 22 ton Liebert units that are linked to independent compressors. These units are used to regularize the temperature and humidity within the data centre.
- The disaster recovery plan is available to clients for review.

Software Security

- Each server is configured to only support HTTP and HTTPS no other services have been enabled on each server and all **other ports** are permanently disabled to improve security.
- All servers are supported by individual Firewall software.
- Vulnerability testing is performed on a regular basis to ensure that system is secure this includes; Network Vulnerability Tests and results are available to customers.
- **ICMP (Internet Control Message Protocol)** is disabled to reduce the possibility of Denial of Service (DoS) attacks.
- SSL 128 bit encryption is used for all data transmission.
- Passwords are encrypted using SHA1.

Data Security

- Client defined password and intruder detection policies are used to monitor usage.
- Client data is only accessible through client controlled usernames and passwords. Clients control visibility of their data to their staff right down to the individual field level.
- All user sessions are logged in addition to value changes to fields and the viewing history for each project.
- All documents produced in BalaBoss offices are security shredded and a certificate of destruction supplied.
- All Client data is removed and purged if the service is cancelled and a certificate of destruction is supplied.

People Security

BalaBoss

- BalaBoss employees are not allowed to access client information with the exception of troubleshooting technical issues.
- All employees have signed PIPEDA compliant non-disclosure agreements.
- All staff must pass criminal background and credit checks.