SECURITY STATEMENT

As a global leader in pre-employment screening and corporate due diligence services, SterlingBackcheck recognizes that data security is of paramount importance. In recognition of this, SterlingBackcheck has located its servers within a managed infrastructure provided by TELUS at their Calgary Internet Data Centre (CIDC). In doing so SterlingBackcheck benefits from a world class data security solution based on ISO 27001.
SterlingBackcheck benefits from a three-pronged approach to data security: physical, logical and informational.

Physical Security

- Highly secure environments – zoned photo ID and keycard authentication, biometric scanning technology and access master list verification.
- All TELUS employees receive Corporate Security clearance.
- Controls in place to ensure adherence to Corporate Security Policy.
- A 365 * 24 Security Officer presence to monitor and patrol all interior and exterior regions.
- Digitally archived CCTV images of all persons entering and leaving.
- Complete and comprehensive alarm, locking and fire detection systems.

Logical Security

- Stringent and comprehensive logical access controls in place.
- Front-end and back-end firewall isolation using Cisco and Check Point appliances with standard or customized rule sets, where appropriate.
- Network intrusion detection system to monitor and protect servers against malicious attacks.
- Wire-based backups to an offsite, physically secure and environmentally sound location – i.e. no physical transportation of tapes.
- Critical patching is carried out as needed; non-critical patching is performed in scheduled windows.

Informational Security

- All employee access is governed by the TELUS Ethics Policy to ensure privacy and confidentiality for all third party data in the CIDC.
- All client access is managed by authorized technical contacts only.
- All changes undertaken must be requested by authorized technical contacts.

SECURITY STATEMENT

SterlingBackcheck Applications and Employee Access

By employing the services of one of Canada's telecommunications and information technology leaders, SterlingBackcheck has transformed itself into a model of the paperless office. This significant investment has also provided a ready solution for remote working and excellent disaster recovery contingencies.

SterlingBackcheck's production systems are deployed to its users via Citrix and an MPLS network through a combination of VLANs and routing tables that ensure separation from all other traffic. The result is that data is secure on a dedicated network and encrypted at all times during transit.

In order to accomplish daily client requests, SterlingBackcheck gathers personal information about individuals. It can be demonstrated that SterlingBackcheck is compliant with Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). There are also a number of other provincial and federal acts and legislation that SterlingBackcheck adheres to. SterlingBackcheck provides ongoing IT security and privacy training to all employees throughout the year to ensure compliance.

Disaster Recovery

SterlingBackcheck has a continuity plan in case of interruption of service for any uncontrollable event that would render our primary operations centre ineffective. We are confident in the seamless continuity of operations in the event of any emergency situation. SterlingBackcheck's data is maintained by TELUS in a state-of-the-art facility that is designed to preserve and protect data in the event of any potential disaster. By harnessing industry leading technology, SterlingBackcheck ensures optimal privacy compliance and disaster recovery coordination.

Redundant Capacity through Geographical Separation

Harnessing the state-of-the-art technology that TELUS IDCs and the Citrix environment provide, SterlingBackcheck has the ability to transfer all operations between offices in Vancouver, Montreal, the United Kingdom, and Manila, Philippines. This will allow for optimal flexibility in workflow, ensuring 100% operational capacity.

Moreover, in the event of a pandemic or other disaster, SterlingBackcheck's state-of-the-art phone system and data security process would allow SterlingBackcheck to enable a seamless transition of workflow internally with clients experiencing no interruption in service and no change to procedure externally. SterlingBackcheck's team members can work from remote workstations, from the UK or Asia, or if need be, from a designated recovery site with the same operational environment and data integrity as performing work from SterlingBackcheck's global headquarters.

SterlingBackcheck has also taken the added precaution of employing geographically diverse police departments to provide assured continuity of SterlingBackcheck's Criminal Record Check service.

Citrix-based Environment

SterlingBackcheck operates exclusively in a Citrix-based platform environment. This allows employees of SterlingBackcheck to operate from any workstation with an internet connection while all necessary information is stored in Internet Data Centers at TELUS.
By utilizing Citrix technology, SterlingBackcheck's Disaster Recovery effort will ensure 100% continuous workflow within hours. SterlingBackcheck's business continuity plan makes several assumptions but will work for all failure situations. Assuming that SterlingBackcheck's primary location may be completely destroyed or inaccessible, Citrix technology allows SterlingBackcheck employees to work from any remote location on independent workstations. Moreover, because remote workstations use the Citrix platform exclusively, ongoing privacy compliance is ensured since all data remains stored in IDCs and not the workstation.