Cyber Security Procedure

Risk Management:

Schumacher Cargo Logistics maintains limited access to all company related data & systems. Limited access to all platforms is based on management level security access systems wide. 2-Step verification authentication is activated via Authentication APP is implanted on all systems & platforms.

Secure configuration
Company has multiple lawyers of cyber security monitoring features including but not limited to:

- Innovative IT monitoring Software on all company computers
- 2-step WVD access via authenticator application
- Limited access at all security levels 1 – 4

Home & mobile working
Employees can access company data & telephone exchange via remote application cloud-based access systems, mentioned in secure configuration. Same security access protocols are in place for in-office or remote based workforce.

Incident management
All incidents are first reported to direct mangers for analyzation purposes.
manager either resolves issue or reports to branch manager. Branch manager either resolves incident or reports to CEO for escalation purposes. Company has Emergency contact list for all incidents.

Malware prevention:
All company computers are monitored by SentinelOne software. SentinelOne is monitored by 3rd party monitoring company who notifies I.T support company Innovative of all threats. Innovative notifies SCL for escalation purposes.

Email systems are monitored by Proofpoint monitoring software. Any threats are immediately quarantined and isolated.

Managing user access
Company has 4 security access levels, with each with own unique data access.

Security Level 1 - Top Management - Access to full company data/drive resources
Security Level 2 - Mid Management – Access to company documents
Security Level 3 – Employees – Access to limited company documents and customer data
Security Level 4 – Customers & Suppliers – Access to own data only.

Monitoring
Windows Virtual Desktop (WVD) Cloud Computers, Microsoft Azure.
SCL Company servers & computers are cloud based. Each employee is provided with unique User ID and Password. 2-Step verification authentication is activated via Authentication APP.

Cyber Security Procedure

Programs Daily Used by employees

- Email – Microsoft Outlook, is used for customer and supplier communications.
- WORD, EXCEL
- Paychex – Employees access payroll data via secured portal access with unique User ID and Password.

Telephone System – Webex by Cisco

SCL Company telephone systems is cloud based. Employees download Mobile or Desktop APP to devise for usage. Each employee is provided with unique User ID and Password.

Industry Software - Moveware

Employees have direct user access to company & customers data via unique Username & Password that can only be accessed inside our WVD environment.

Customer can access limited Move details via our website tracking portal - Login (moveconnect.com)
Each customer is provided Username & Password to access information pertaining to individual move.

Customers are directed to upload documents and to pay invoices via secured web links, not to send data via email/text or other means.

Network security
Employees must only access internet while logged into our WVD secured work environment.
All access computers & devices must have monitoring software installed.

Removable media controls
Employees must never input portable devices into any company related computer, it is NOT required or needed in our work environment
Employees must never copy any customer or company data to a portable device for any reason.

Accountability, user education and awareness
All company employees are committed to protecting customer and company data by adhering to Code of Conduct written and clearly identified in employee handbook.

All employees have mandatory annual training where newly implements or updated cyber security measures are discussed, analyzed, explained to ensure systemwide successful implementation.

General
* Customer data is retained till no governess level requitements ends.
* Employee passwords are periodically set to renew by our IT system controller.
* Company encourages Supplier and Customer to submit and transfer data via secured web links such as: API/Stripe/Web Portal.