CORPORATE TRAVELLER | Powered by melon

Information Security (InfoSec) Canada Fact Sheet

Information Protection

- Shared infrastructure
  - Compliant with PCI-DSS and GDPR standards
- System development life cycle (SDLC) designed based on these standards and frameworks:
  - GDPR
  - Adherence to Flight Centre Travel Group (FCTG, parent company of Corporate Traveller) Security and Privacy by Design framework
  - Open Web Application Security Project (OWASP)
  - ISO 27001
- Minimum security baselines defined using CIS and NIST and reviewed annually
- All data encrypted at rest using AES356 and in transport using TLS 1.2
- Client data restricted from being stored on employee equipment
- McAfee ePO and Microsoft Defender utilized for anti-malware and anti-virus across all endpoints and servers
- Vulnerability management provided by Tenable, malicious activity protection through full SIEM and SOC 24x7x365 and penetration tests by Trustwave Dvuln or Bugcrowd
- All developers utilize Snyk and resolve vulnerabilities as found in code

IT System Audits

- External vulnerability scans performed monthly
  - Trustwave for network and externally facing (Internet) websites
  - Verizon (QSA) conducts regular third-party security assessments
- Results reviewed and remedial action led internally by senior IT and Security management, in accordance with internal security policies

Access Controls

- Corporate Traveller has a process for authorizing, provisioning, and de-provisioning client employee access
- Ability to integrate with your HR system through routine data feed, including termination notices
- The Corporate Traveller Melon Platform offers Single Sign On access in which Corporate Traveller can integrate with Clients' existing SAML 2.0 compliant authentication to remove the need for Corporate Traveller to save user passwords or login information
- Corporate Traveller employees authenticate over secure connections, including two factor certificate-based VPN for multi-factor (MFA) approved access, SSL-based connections and Windows-based authentication
- Quarterly user access entitlement reviews

Passwords

- First-time passwords for new users and reset passwords for existing users are set to a unique value for each user and changed after first use
- Passwords are stored as a bcrypt hash in postgres text
- Passwords for User accounts are required to have the following minimum standards (may be increased based on Client specifications):
  - a password length of no less than 7 for user accounts, with the policy stating 12
  - complexity requirements in line with PCI-DSS standards
  - Passwords must be changed on a regular schedule – 90 days
  - Passwords cannot be the same as the last password
  - Account access is temporarily suspended after 5 attempts in 30 minutes
- Desktop session idle time out features have been set to 15 minutes or less. Processor session inactivity times out after 30 minutes
- All remote access protected by MFA

Data Storage, Physical Controls & Disaster Recovery

- FCTG Data Centres are on Microsoft Azure cloud-based platform that are physically located in Virginia, USA. Microsoft Azure is compliant with industry standards such as ISO 27001, ISO 27018, ISO 9001, ISO 22301, HIPAA, FedRAMP, PCI DSS, SSAE-18 SOC 1 and SOC 2 for logical and physical security, processing integrity and availability. Also Concur and Sabre are SOC 2 compliant.
- Microsoft Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services. Each facility is designed to run 24x7x365 and employs various measures to help protect operations from power failure, physical intrusion and network outages. Backups are performed on a regular basis to prevent loss of client data by Azure.
- Reporting data uploaded to ClientBank, Corporate Traveller's PowerBI environment, where data is fully encrypted and managed by FCTG.

Human Resources

- Background checks performed in Canada, including:
  - SIN number verification and trace
  - Provincial records
  - Education verification
- Security awareness training program required for all new employees and repeated annually

Incident Management

- Security monitoring is conducted through a Global SIEM solution which monitors key servers and network infrastructure. Incidents can be tracked to specific users, files changes and server changes. Incident managers, Information Security analysts, and the Security Operations Centre will assess security events to determine severity and appropriate escalation route, and perform appropriate forensics and root cause analyses to identify, track, and resolve security incidents.