PRIVACY & CONFIDENTIALITY

In the course of serving its customers, Cityspan acquires, stores and transmits personally identifiable information about persons that may be regarded as confidential. Cityspan does not, except for reasons stated below, disclose to third parties the contents of personal information that it stores or transmits. Personal information is never sold or otherwise transferred for commercial purposes.

Cityspan will only disclose personal information if it has reason to believe that disclosing such information is necessary to identify, make contact with, or bring legal action against someone who may be causing harm or interfering with the rights or property of Cityspan or its customers, or if Cityspan has a good belief that the law requires such disclosure. The circumstances under which Cityspan will disclose such personal information are when:

- it is required to cooperate with interception orders, warrants, or other legal processes that Cityspan determines to be valid and enforceable; and
- it is necessary to provide to a law enforcement agency when information obtained by Cityspan appears to pertain to the commission of a crime.

Cityspan disclaims any intention to censor, edit or engage in ongoing review or surveillance of information stored on or transmitted through its facilities. Cityspan will, however, review, delete or block access to information that may harm Cityspan, its customers or third parties.

SECURITY

Cityspan implements and maintains comprehensive security controls to protect its networks, servers, and applications from the threat of hacking and ransomware attacks. Cityspan security complies with standards published by the National Institute of Standards and Technology (NIST). In 2020, NIST compliance was verified by a third-party auditor, resulting in the issuance of a SOC 2 Type 1 report. The SOC 2 describes all aspects of Cityspan's security infrastructure, including security devices, application controls, backup systems, employee policies, and disaster recovery. In addition to SOC 2 compliance, Cityspan maintains 24/7 security monitoring and real-time reporting by implementing AlienVault - Unified Security Management software and Qualys application scanning services.

Physical Security

Cityspan hosts all operations at a secure datacenter co-located at CenturyLink Communications in Santa Clara, California. The system is guarded by layered security protocols, with each layer addressing a particular threat, including biometric access points, video surveillance, smoke detectors, fire suppression systems and intrusion alarms.

Transmission Security

Transmission security guards against the interception of data as it passes between an end-user (client) and server (host). Cityspan's browser-based communications are secured by a VeriSign 256-bit digital certificate.

Network and Host Security

Network and host security prevents unauthorized persons from accessing the system from a remote network location. Cityspan servers are guarded by Cisco ASA firewalls, which are the industry standard for

network protection. In addition to firewall defense, Cityspan maintains security protocols consistent with recommendations from CERT (www.cert.org) and Microsoft.

System Maintenance

Cityspan routinely schedules maintenance updates. In the instance that an update is expected to affect a user's access to their site, a 72-hour notice is posted to the login page. Updates are scheduled to occur during non-peak user hours.

Cityspan Staff Access to Data

Cityspan employees follow company protocols for accessing and modifying data. All work is performed at the Cityspan's office or at remote U.S. locations were Cityspan's staff connects to the data center using a secure VPN.

LEGISLATIVE REQUIREMENTS

Cityspan maintains the integrity and accuracy of its information to meet its business goals and obligations. To ensure this, it is essential that information is secured in line with professional best practices as well as statutory, regulatory, and contractual requirements that maintain confidentiality, integrity, and availability of all information assets. Cityspan's Information Security Team maintains awareness of applicable requirements, implements appropriate guidelines and procedures to meet compliance requirements, and ensures Cityspan staff are trained on all related obligations. Review of requirements are performed on an annual basis.

Family Educational Rights and Privacy Act (FERPA)

Cityspan complies with requirements for managing student education records as set forth in the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99).