2600Hz

2600Hz's servers for "Hosted" and "Private Cloud" are located in Equinix around the United States. These data centers are certified in the following:

SOC1 TYPE 1

SOC1 is an American Institute of Certified Public Accountants (AICPA) report used to document controls relevant to an organization's Internal Controls over Financial Reporting (ICFR). The report focuses on an organization's services provided, along with supporting processes, policies, procedures, personnel and operational activities that constitute the core activities relevant to users. The auditing standards for an SOC1 report include SSAE 16 and ISAE 3402.

SOC2 TYPE 2

A standard designed for technology companies, including: data centers, IT managed services, SaaS vendors, cloud-computing based businesses and other technology. SOC2 criteria is based on the Trust Services Principles (TSP) of security, availability, processing integrity, confidentiality and privacy as well as controls outside of financial reporting.

ISO 27001

An internationally recognized best practice framework that specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS). ISMS is a systematic approach to managing sensitive company information including people, processes and IT systems.

ISO 27001

NIST 800-53 is published by the National Institute of Standards and Technology, which creates and promotes the standards used by federal agencies to implement the Federal Information Security Management Act (FISMA) and manage other programs designed to protect information and promote information security. Agencies are expected to meet NIST guidelines and standards within one year of publication. National security is not included in these standards.

NIST 800-53/FISMA

NIST 800-53 is published by the National Institute of Standards and Technology, which creates and promotes the standards used by federal agencies to implement the Federal Information Security Management Act (FISMA) and manage other programs designed to protect information and promote information security. Agencies are expected to meet NIST guidelines and standards within one year of publication. National security is not included in these standards.

PCI DSS

The PCI Security Standards Council offers comprehensive standards and supporting materials to enhance data security for payment cards. They include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process, including prevention, detection and appropriate reaction to security incidents.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Any company that deals with protected health information (PHI) must ensure that all the required physical, network, and process security measures are in place and followed. This includes: covered entities (CE); all treatment providers; healthcare payment and operations; business associates; personnel with access to patient information to provide support in treatment, payment or operations. Subcontractors and business associates must also follow HIPAA compliance.

HDA/HADS

Hosting of health data is regulated under French law and aimed at protecting the confidentiality, integrity and availability of patients' data. Such hosting activity can only be implemented by a hosting service provider ("HSP") previously approved by the French Ministry of Health's Shared Healthcare Information Systems Agency (ASIP) via a Health Data Agreement (HDA).

OHSAS 18001/ISO 18001

OHSAS 18001, also referred to as ISO 18001, is the internationally accepted and recognized management standard for occupational health and safety. The standard is used as a method of assessing and auditing occupational health and safety management systems.

ISO 9001

ISO 9001 is a certified quality management system (QMS) for organizations who want to demonstrate their ability to consistently provide products and services that meet the needs of their customers and other relevant stakeholders.

ISO 22301

An international standard for Business Continuity Management (BCM), ISO 22301 replaces British standard (BS) 25999. It specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to prepare for, respond to and recover from disruptive events such as natural disasters, environmental accidents, technology mishaps and man-made crises.

SS 564

SS 564 helps organizations in Singapore establish systems and processes to improve the energy efficiency of their data centers. The standard, modeled after the global ISO 50001 certification system, outlines a detailed framework for data center energy and environmental management that's tailored to conditions in Singapore.

ISO 14001

ISO 14001, the most current version being ISO1400:2015, specifies the requirements for an environmental management system that an organization can use to enhance its environmental performance in a systematic manner that contributes to the environmental pillar of sustainability.

ISO 50001

ISO 50001, the most current version being ISO 50001:2011, specifies requirements for establishing, implementing, maintaining and improving an energy management system, whose purpose is to enable an organization to follow a systematic approach in achieving continual improvement of energy performance, including efficiency, use and consumption. It has been designed to be used independently, but it can be aligned or integrated with other management systems.

UpTime Institute

As an independent advisory organization, Uptime Institute is focused on improving the performance, efficiency, and reliability of the business critical infrastructure that underlies today's global information economy. Uptime Institute is recognized worldwide for the creation and administration of the Tier Standards & Certifications for Data Center Design, Construction (Facility) and Operational Sustainability.

FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that will save cost, time, and staff required to conduct redundant agency security assessments.

TSI

Trusted Site Infrastructure, introduced from TÜV-IT, is a catalogue of requirements on ten different areas of a data center including areas such as environment, construction, firehandling, security, cabling, energy, air, organization and documentation.