Committed to Security, Accessibility & Operational Excellence

Our Data Center is dedicated to upholding the highest industry standards for compliance, security and continuous improvement, evidenced by our achievement and attainment of numerous data center and service certifications outlined below. In keeping with our commitment to ensuring the safety and security of customer data, the agility of our solutions, and the continued excellence of our customer service, we are always evaluating and considering new certifications and standards based on the needs of our customers. Our Data Center also employs a Compliance Specialist who is instrumental in working side-by-side with customers and our engineers to help plan and architect technical solutions that comply with various certification and security requirements, such as HIPAA.

SSAE18 SOC 2 Type 2 certification

SSAE18 SOC 2 Type 2 certification was established by the American Institute of Certified Public Accountants (AICPA) in May 2017, superseding the globally-recognized control and services reporting standard, SSAE16. To achieve certification, data centers must undergo an independent examination of control objectives and activities supporting their solutions performed by an independent, third-party service auditor. Recent changes to the standard require companies to take additional control and ownership of internal controls surrounding the identification and classification of risk and appropriate management of third-party vendor relationships.

SSAE18 SOC 2 Type 2 is a critical designation for serving Our Data Center's healthcare, financial services, eCommerce and government customers. The certification demonstrates Our Data Center's ability to effectively support these global customers' business environments and offer critical protection for sensitive company information. SOC 2 Type 2 audits offer an unbiased assessment of Our Data Center's data center infrastructure, systems, processes and services, evidencing the company's ability to provide the highest levels of security and reliability across all of its certified data centers.

The HIPAA Act of 1996

The HIPAA Act of 1996 is a federal mandate that requires specific security and privacy protections for Protected Health Information (PHI). HIPAA was expanded in 2009 to include Health Information Technology for Economic and Clinical Health Act (HITECH) to promote the adoption and meaningful use of health information technology in the U.S. In 2013, the final HIPAA Omnibus Rule set further statutory requirements, which greatly enhanced a patient's privacy rights and protections, including holding all custodians of PHI — including HIPAA Business Associates (BA) — subject to the same security and privacy rules as covered entities under HIPAA.

While there are no specific industry certifications for HIPAA compliance, SSAE16 SOC 1 TYPE II audits include a HIPAA Matrix attesting that companies' administrative actions, policies and procedures properly conform to HIPAA regulations. Yearly audits are performed and evaluated by an independent, third-party auditor who issues an evaluation report that details the controls Our Data Center has in place to meet HIPAA requirements in regards to data privacy and security.

Healthcare and enterprise customers require proper storage and security of their electronic Protected Health Information (ePHI) in order to remain compliant with HIPAA / HITECH mandates.

Our Data Center's hosting services feature a number of safeguards to ensure maximum data protection, fast accessibility and safe transmission of ePHI, including customer segmentation, dedicated VLANs, restricted physical access to production servers, default firewalls for all managed services, audit logs and reporting, 99.9 uptime SLA, and more.

Our Data Center also signs HIPAA Business Associate Agreements (BAAs) with customers.

Open-IX OIX-2 data center certification

The Open-IX OIX-2 data center certification defines the standards for data centers to offer an "open" and cost-effective Internet exchange and interconnection platform.

The designation ensures that the certified data center's infrastructure reduces the complexity that restricts interconnection and enables the implementation of business-critical environments, international IP core networks or content platforms.

Our Data Center is committed to improving the landscape of Internet peering and interconnection. The certification demonstrates that Our Data Center holds the highest physical and operational standards throughout its data centers in order to facilitate greater interconnection.

The certification upholds Our Data Center's mission to provide customers with advanced, open and neutral technical and human ecosystems along with fully managed solutions that allow them to focus on their core business. Our Data Center's NY1 facility is the only OIX-certified data center on Long Island and East of Manhattan offering fully managed Hybrid Cloud and technical and human ecosystems.

Our Data Center CTO Sagi Brody is also a Committee Member of the Open-IX Data Standards Committee.

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act (FISMA) requires federal agencies to implement and support standardized IT security controls. These controls, defined by the National Institute of Standards and Technology (NIST), allow agencies to safely and confidently outsource critical applications to FISMA-compliant clouds, managed hosting environments and SaaS providers.

Our Data Center implements and deploys the appropriate FISMA, NIST and Federal Information Processing Standard (FIPS) for managed security controls, auditing, and documentation. This allows federal agencies that must adhere to these regulations to outsource ownership and accountability of critical infrastructure to Our Data Center in a compliant manor.

Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS), administered by the Payment Card Industry Security Standards Council, is a mandatory designation for any provider or organization that stores, processed or transmits cardholder data and / or sensitive authentication data. Setting forth proper controls and best practices, PCI DSS helps to alleviate merchant-based security vulnerabilities and protect cardholder data.

Our Data Center's team manages, monitors and scales PCI-compliant infrastructure for a variety of eCommerce customers and platforms. Our Data Center provides physical, environmental, network and infrastructure security to ensure sensitive cardholder data remains sage and secure.

CJIS Security Policy

The CJIS Security Policy is a set of standards developed by the FBI's Criminal Justice Information Services Division (CJIS) in 2011 to better protect the data it delivers to federal, state and local law enforcement agencies. or organizations that access criminal justice information

While there are no specific industry certifications for CJIS compliance, SSAE16 SOC 1 TYPE II audits include a matrix attesting that companies' administrative actions, policies and procedures properly conform to CJIS regulations. Yearly audits are performed and evaluated by an independent, third-party auditor who issues an evaluation report that details the controls Our Data Center has in place to meet CJIS requirements in regards to data privacy and security.

Our Data Center provides a secure environment and redundant technical infrastructure to safely handle the storage, exchange and recovery of critical information belonging to state, local and federal law enforcement, justice and public safety agencies.

Our Data Center operates a private, secure and DDoS-monitored network. Its data centers are also monitored by CCTV 24x7.

Our Data Center's NY1 facility features an on-site Security Operations Center (SOC). Card access, a mantrap and 24x7 on-site personnel ensure customer identity is verified before access is granted to the data center.

In addition to completing extensive pre-employment background checks on employees, Our Data Center also signs CJIS security agreements with customers.

IRS 1075

Internal Revenue Service Publication 1075 (IRS 1075) provides guidance for > US government agencies and their agents to protect Federal Tax Information (FTI). IRS 1075 specifically references NIST 800-53 security controls.

While there is no official certification for 1075, Our Data Center supports organizations to protect FTI by taking ownership of encryption at rest and in transit. Additionally, Our Data Center can provide direct and secure connectivity between customer networks and hosted infrastructure, completely segmenting the FTI information from the public internet.

EU–US Privacy Shield

The EU–US Privacy Shield is a framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States. One of its purposes is to enable US companies to more easily receive personal data from EU entities under EU privacy laws meant to protect European Union citizens.

Our Data Center completed its compliance assessment and filed the Privacy Shield application with the U.S. Department of Commerce in 2018. Our Data Center has certified that it adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) establishes a legal framework that sets policies for the collection, storage and processing of the personal data of individuals in the European Union (EU). The GDPR takes effect on May 25, 2018, and affects all companies that interact with the digital information of data subjects in the EU.

Most services that Our Data Center provides are content-neutral - Our Data Center does not know, and has no way of knowing, whether customer content contains the personal data of EU residents. As such, it is the customer, not Our Data Center, who has primary responsibility for GDPR compliance.

Our Data Center assists customers in achieving GDPR compliance as required by Article 28 of the GDPR, including cooperating with security audits and providing contractual assurances where necessary.

LOCATION OF DATA:

GDPR requirements apply to the personal data of EU residents, wherever in the world that data is collected or stored, and cannot be avoided by moving data to a different jurisdiction or registering a website in a different country.

Our Data Center ensures security of physical data, data at rest, and data in transit via industry accepted best practices. Our Data Center's security controls are audited via 3rd party through the aforementioned SSAE18 SOC2 audits.